Cyber Defence (Teil 2)

Cyber Defence - eine nationale Herausforderung (Teil 2)

Walter J. Unger[1)],[2)]/Sigmar Stadlmeier/Andreas Troll

Nach der Skizzierung des Bedrohungsbildes im Cyberraum und der Darstellung der geplanten Reaktionsmöglichkeiten Österreichs befasst sich der zweite und abschließende Teil mit der gegebenen Rechtslage und den Vorbereitungen des ÖBH - milCERT und Cyber Defence.

Zur Rechts- und Befugnislage nach österreichischem Recht

Verfassungsrechtslage

Im gegenständlichen Zusammenhang sind in erster Linie die Kompetenztatbestände „Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“[3)] und „Militärische Angelegenheiten“[4)] betroffen. Ersteres legt die Verfassung in die Hand des BMI,[5)] Letzteres obliegt dem BMLVS und dem Bundesheer.[6)]

Dazu kommen hinsichtlich des Bundesheeres Auslandsaufgaben[7)] sowie Aufgaben in fremder Kompetenz (sicherheitspolizeiliche Assistenz, Katastrophenassistenz).

Einfachgesetzliche Rechtslage

a) Öffentliche Ruhe, Ordnung und Sicherheit

Das Sicherheitspolizeigesetz (SPG) definiert den „harten Kern“ der Sicherheitspolizei[8)] als Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit (ausgenommen örtliche Sicherheitspolizei) und erste allgemeine Hilfeleistungspflicht. Die Kommentarliteratur versteht unter „öffentliche Sicherheit“ die Sicherheit des Staates sowie der Person (Leben, Gesundheit, Freiheit) sowie des Eigentums und unter „öffentlicher Ordnung“ den durch die Rechtsordnung geprägten „Sollzustand“ in der Öffentlichkeit.[9)] Die Hauptbedrohung, der sich die Sicherheitspolizei widmen soll, ist die „allgemeine Gefahr“, die entweder in einem „gefährlichen Angriff“ (= Straftat nach StGB, VerbotsG oder SuchtmittelG einschließlich unmittelbarer Vorbereitungshandlungen) oder in einer kriminellen Verbindung besteht.[10)] In Zusammenhang mit der allgemeinen Gefahr beruft das SPG die Sicherheitspolizei auch zur Gefahrenerforschung (= Feststellung der Gefahrenquelle und des sonst für die Abwehr maßgeblichen Sachverhalts).[11)] Anders als das MBG (dazu unten, b)) nennt das SPG die von ihm geschützten Rechtsgüter nicht ausdrücklich; diese müssen vielmehr aus den Justizstraftatbeständen des StGB, VerbotsG und SMG ermittelt werden. Dies bedeutet aber auch, dass mit der (Neu-)Festlegung eines geeigneten Straftatbestandes im StGB das darin geschützte Rechtsgut ex lege zu einem Rechtsgut wird, zu dessen Schutz das SPG die Sicherheitspolizei beruft.

Im gegenständlichen Zusammenhang ist dies deswegen von Bedeutung, weil Österreich (schon vor dem Inkrafttreten der Cybercrime Convention des Europarats[12)]) etliche cybersicherheitsrelevante Straftatbestände im StGB verankert hat (§ 118a, Widerrechtlicher Zugriff auf ein Computersystem; § 119a, Missbräuchliches Abfangen von Daten, § 126a, Datenbeschädigung; § 126b, Störung der Funktionsfähigkeit eines Computersystems; § 126c, Missbrauch von Computerprogrammen oder Zugangsdaten). Dadurch - nicht erst durch die programmatische Erklärung in der Cyber-Sicherheitsstrategie - ist Cybersicherheit zum Rechtsgut geworden, das von der Sicherheitspolizei im Rahmen des § 16 SPG zu schützen ist.

b) Militärische Angelegenheiten

Die zentralen einfachgesetzlichen Regelungen finden sich hier im Wehrgesetz (WG) sowie im Militärbefugnisgesetz (MBG).

Das Wehrgesetz regelt primär die innere Organisation des Bundesheeres und konkretisiert im § 2 die auf Verfassungsebene festgelegten Zwecke der militärischen Landesverteidigung, der sicherheitspolizeilichen Assistenz, der Katastrophenassistenz und des Auslandseinsatzes.[13)] In diesem Zusammenhang wird klargestellt, dass die Kernaufgabe „militärische Landesverteidigung“ auch die allgemeine Einsatzvorbereitung, die unmittelbare Einsatzvorbereitung und Abschlussmaßnahmen nach einem Einsatz umfassen.

Die allgemeine Einsatzvorbereitung dient dabei der Sicherstellung der ständigen Einsatzbereitschaft durch Schaffung aller Einsatzvoraussetzungen, insbesondere personeller und materieller Natur.[14)] Die bloß demonstrative Aufzählung („insbesondere“) schließt weitere Vorkehrungen (etwa immaterieller Natur) nicht aus und erlaubt auch einsatzbezogene Vorkehrungen in Sachen Cybersicherheit.

Die unmittelbare Einsatzvorbereitung dient der Verstärkung und Erhöhung der Einsatzbereitschaft des Bundesheeres, sofern aufgrund der ständigen Beobachtung der militärischen und sicherheitspolitischen Lage Gefahren für die Unabhängigkeit nach außen oder für die Unverletzlichkeit oder Einheit des Bundesgebietes vorherzusehen sind.[15)] Die „ständige Beobachtung“ wird in dieser Bestimmung vorausgesetzt; liefert doch erst diese die Anhaltspunkte für einschlägige Gefahren; in diesem Kontext ist auch die Lageentwicklung im Cyberspace mit zu beobachten, um Anhaltspunkte für massive Bedrohungen, die sich gegen die staatliche Unabhängigkeit (= Handlungsfreiheit ohne politischen Druck von außen) richten,[16)] zu erkennen.

Das Militärbefugnisgesetz benennt - anders als das SPG, s.o. - ausdrücklich die mittels der darin vorgesehenen Befugnisse zu schützenden Rechtsgüter, nämlich

- Leben und Gesundheit von Personen, die mit der Vollziehung militärischer Angelegenheiten betraut sind, während ihrer Dienstausübung;

- Leben und Gesundheit von Organwaltern und verfassungsmäßigen Einrichtungen sowie Vertretern anderer Staaten oder internationaler Organisationen, sofern deren Schutz jeweils im Rahmen der militärischen Landesverteidigung zu gewährleisten ist;

- militärische Bereiche, Heeresgut, militärische Geheimnisse.[17)]

Der „Angriff" auf diese Rechtsgüter ist § 16 Abs. 2 SPG nachgebildet (Verwirklichung eines gerichtlich strafbaren Offizialdeliktes einschließlich Vorbereitungshandlungen), allerdings sind im Rahmen der durch das WG abgesteckten Zuständigkeitsgrenzen, also bereits im Rahmen der allgemeinen Einsatzvorbereitung, nur diese abschließend aufgezählten militärischen Rechtsgüter zu schützen.[18)]

Der militärische Eigenschutz umfasst zum einen den Wachdienst zum Schutz vor drohenden und zur Abwehr gegenwärtiger Angriffe oder vergleichbarer Handlungen[19)] gegen militärische Rechtsgüter, zum anderen die nachrichtendienstliche Abwehr. Der militärische Eigenschutz ist allerdings insofern subsidiär zum Schutz der öffentlichen Ordnung und Sicherheit durch die Sicherheitsbehörden, als Angriffe gegen militärische Rechtsgüter, die eine allgemeine Gefahr im Sinne des § 16 SPG darstellen, nur dann zum Handeln nach MBG Anlass geben, wenn und solange nicht Sicherheitsbehörden dagegen einschreiten.

Für den Cyberbereich bedeutet dies, dass Angriffe mit Cybermitteln

- die Straftatbestände (z.B. die oben genannten §§ 118a, 119a, 126a-c StGB) oder vergleichbare Verwaltungsübertretungen verwirklichen

- und so geartet sind, dass sie entweder Leben und Gesundheit von Personen gefährden, die mit der Vollziehung militärischer Angelegenheiten befasst sind,

- oder sich direkt gegen militärische Hardware aller Art richten (diese ist als „Heeresgut", nämlich bewegliche Sache, die militärischen Organen zur Aufgabenerfüllung zur Verfügung steht,[20)] anzusehen),

- oder sich gegen militärische Geheimnisse[21)] richten,

im Rahmen des militärischen Eigenschutzes in die militärische Zuständigkeit fallen.

Stellen solche Angriffe darüber hinaus auch eine allgemeine Gefahr im Sinne des SPG dar, gilt diese Zuständigkeit subsidiär zu jener der Sicherheitsbehörden. Ob ein Angriff auf ein militärisches Rechtsgut auf dieses beschränkt ist oder auch Rechtsgüter der Allgemeinheit bedroht, ist im Einzelfall zu beurteilen.

Beispiele:

- Ein Cyberangriff, der auf interne militärische (d.h. nicht-öffentliche) Netze beschränkt ist, wird Rechtsgüter der Allgemeinheit kaum berühren.

- Ein Cyberangriff auf die militärische Luftraumüberwachung wird trotz ihres militärischen Charakters auch Rechtsgüter der Allgemeinheit gefährden, weil die Militärflugleitung in militärisch reservierten Bereichen (z.B. military training areas, MTA) auch zivilen Luftverkehr führt.[22)] Das Rechtsgut sichere Luftfahrt wird vom § 186 StGB (Vorsätzliche Gefährdung der Sicherheit der Luftfahrt) geschützt. Daher liegt in einem solchen Fall (auch) eine allgemeine Gefahr vor, die zur Zuständigkeit der Sicherheitsbehörden führt.

Auch in Fällen einer bloß subsidiären militärischen Zuständigkeit besteht diese, wenn und solange die Sicherheitsbehörden nicht einschreiten. Reagieren also militärische Organe im obigen LRÜ-Szenario zuerst, dann ist ihr Handeln jedenfalls so lange rechtmäßig, als die Sicherheitsbehörden (noch) nicht einschreiten.

c) Strafrecht

Im Hinblick auf Cyberabwehr sind insbesondere die strafrechtlichen Delikte, die in Umsetzung der Cybercrime Convention ins StGB eingefügt wurden, von Bedeutung. Diese sind § 118a, Widerrechtlicher Zugriff auf ein Computersystem; § 119a, Missbräuchliches Abfangen von Daten, § 126a, Datenbeschädigung; § 126b, Störung der Funktionsfähigkeit eines Computersystems; § 126c, Missbrauch von Computerprogrammen oder Zugangsdaten. Ohne dass hier eine detaillierte Analyse dieser Tatbestände vorgenommen werden kann,[23)] ist doch davon auszugehen, dass alle diese Delikte Cyberabwehr-relevant sind: Im diesem Kontext ist - im Gegensatz zum „bloßen" Hacken als Fähigkeitsdemonstration - auch der erforderliche erweiterte Schädigungsvorsatz beim widerrechtlichen Zugriff nach § 118a oder beim missbräuchlichen Abfangen von Daten nach § 119a wohl gegeben; werden im Zuge von Cyberabwehr Daten beschädigt, greift § 126a; selbst wenn keine Daten beschädigt werden, wird Cyberabwehr ihrer Natur nach darauf abzielen, die (unerwünschte) Funktion der IKT-Einrichtungen, gegen die sie sich richten, zu stören, was dem Tatbestand von § 126b entspricht; schließlich kriminalisiert § 126c bereits Herstellung, Einfuhr, Vertrieb, Besitz etc. der dafür nötigen Software-Werkzeuge, sofern diese zur Tatverwirklichung der o.a. Delikte verwendet werden sollen.

d) Telekommunikationsrecht

Das Telekommunikationsgesetz[24)] gilt nicht für „Kommunikationseinrichtungen (wie insbesondere Funkanlagen und Telekommunikationsendeinrichtungen)", die ausschließlich für Zwecke der Landesverteidigung betrieben werden;[25)] nur die Frequenznutzung ist mit dem BMVIT im Einvernehmen festzusetzen. Als Funkanlagen gelten gem. § 3 Z 6 TKG auch elektrische Einrichtungen, deren Zweck es ist, mittels Funkwellen Funkkommunikation zu verhindern (solche dürfen aber nur von Behörden betrieben werden, die mit Aufgaben der Landesverteidigung, der öffentlichen Sicherheit oder der Strafrechtspflege betraut sind[26)]). Eine ähnliche Ausnahme besteht für die Fernmeldebehörden. Soweit das TKG Schutzvorschriften für Nutzer enthält, beziehen sie sich - aufgrund der Definition der „Nutzer" in § 3 Z 14 TKG - nur auf Nutzer öffentlich zugänglicher Kommunikationsdienste (und wohl nicht auf das ÖBH als Nutzer der 3. VE, solange diese nicht wenigstens teilweise geöffnet wird).

Unter dem Titel „Kommunikationsgeheimnis“ untersagt das TKG das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer.[27)] Die Ermittlung und Verarbeitung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten darf nur für Zwecke eines Kommunikationsdienstes erfolgen,[28)] gem. StPO und SPG zulässige Erfassungen und Übermittlungen von Verkehrsdaten, Standortdaten und Stammdaten, einschließlich Vorratsdaten, sind detailliert geregelt;[29)] insbesondere nimmt das TKG hier keinen Bezug auf das MBG, das wiederum nur rudimentäre Auskunftspflichten der Betreiber von Kommunikationsdiensten kennt (s.u.).

Befugnisse

Zur Wahrnehmung der in der Rechtsordnung festgelegten Zuständigkeiten müssen den jeweiligen Organen Befugnisse zugewiesen sein; diese folgen nicht etwa schon aus der Zuständigkeit. Dies ist auch im völkerrechtlichen Kontext von Bedeutung, daher ist abschließend die nationale Rechtslage auf einschlägige Befugnisse zu überprüfen. Dabei erfolgt eine Beschränkung auf solche Befugnisse, die im Cyberabwehrbereich einschlägig sein können.

Beispiel:

Die Cybercrime Convention des Europarats richtet sich ausschließlich an ihre Signatarstaaten, verpflichtet sie, bestimmte Delikte festzulegen und unter Strafe zu stellen, wobei autorisiertes Vorgehen von Staatsorganen nicht tatbildlich sein soll. Diese Autorisierung muss aber im nationalen Recht durch Zuweisung von Befugnissen erfolgen.

a) Befugnisse nach SPG

Die zentralen Befugnisse finden sich in den §§ 32-50 SPG und sehen zunächst die allgemeine Befugnis zur Beendigung eines gefährlichen Angriffs durch die Ausübung von unmittelbarer Befehls- und Zwangsgewalt vor.[30)] Die Kommentarliteratur betont, dass diese Bestimmung zumindest die Rechtsgüter, in die dabei eingegriffen werden kann, nicht einschränkt, womit auch Rechtsgüter aus dem Bereich der Telekommunikation in Frage kommen. Dabei darf - nach einer im Schrifttum verbreiteten, aber nicht unumstrittenen Auffassung - nicht nur in Rechtsgüter der Täter, sondern (mangels Einschränkung in der Befugnisnorm) auch in Rechtsgüter Dritter im erforderlichen Ausmaß eingegriffen werden.[31)] Ein gefährlicher Angriff im Netz kann also mit dieser Befugnis unter Einsatz von Cybermaßnahmen beendet werden, wenn diese das zweckdienliche Mittel hierfür sind.

Dabei kommt die Befugnis zum Sicherstellen von Sachen in Betracht, wenn dies dazu dient, bei gefährlichen Angriffen eine weitere Bedrohung von Leben, Gesundheit, Freiheit oder Eigentum von Menschen zu verhindern.[32)] Dies ist zwar keine Cyberbefugnis, aber - je nach Lage der Umstände - eine „Alternativbefugnis“, die, wenn sinnvoll, in Erwägung gezogen werden muss.

Fraglich erscheint, ob im Falle der Durchführung von Cyberabwehr die Befugnis zur Inanspruchnahme fremder Sachen[33)] aktiviert werden muss. Eine solche Inanspruchnahme ist zulässig, wenn sie zur Abwehr eines gefährlichen Angriffs unerlässlich ist, d.h. es keine vernünftige Alternative gibt. Ist etwa eine Cybermaßnahme das einzig sinnvolle Mittel zur Beendigung eines gefährlichen Angriffs, kann den Sicherheitsorganen zumindest nicht entgegengehalten werden, sie hätten sich der dabei benutzten fremden Einrichtungen (Server, Router etc.) nicht bedienen dürfen. Die Formulierung des Gesetzestexts, insbesondere die dort vorgesehene Rückstellung nach Gebrauch, sowie die in der Kommentarliteratur gegebenen Beispiele[34)] lassen annehmen, dass es sich dabei um körperliche Sachen handeln muss.

Sicherheitsorgane dürfen zur Durchsetzung ihrer Befugnisse auch Zwangsgewalt anwenden, wobei dies anzudrohen und anzukündigen ist; allerdings kann bei der Beendigung gefährlicher Angriffe davon abgesehen werden, wenn dies zur Verteidigung des angegriffenen Rechtsgutes unerlässlich erscheint.[35)] Die Kommentarliteratur betont, dass „Zwangsgewalt“ nicht auf körperliche Gewalt beschränkt ist, sondern „technische Hilfsmittel im weitesten Sinn“ beinhalten kann.[36)] Dies lässt - insbesondere zur Beendigung gefährlicher Angriffe - auch Cybermaßnahmen als Mittel der Zwangsgewalt tauglich erscheinen.

Unter den Ermittlungsbefugnissen der Sicherheitsbehörden sticht schließlich § 53 (Zulässigkeit der Datenverarbeitung) ins Auge, der ausdrückliche Befugnisse zu Auskunftsverlangen über IP-Adressen zu bestimmten Nachrichten und Nutzern enthält,[37)] wenn sie diese Daten zur Abwehr gefährlicher Angriffe oder einer kriminellen Verbindung oder einer konkreten Gefahr für Leben, Gesundheit oder Freiheit eines Menschen benötigen. Die IP-Adresse ist ein wesentlicher Anhaltspunkt zur Rückverfolgung von Aktivitäten im Netz und als Grundlage für gezielte Cybermaßnahmen erforderlich. Von Seiten der Sicherheitsbehörden gesehen passt diese Befugnis auch zur Schnittstelle zwischen sicherheitsbehördlichen und militärischen Befugnissen, weil sie entweder einen gefährlichen Angriff oder (bereits) konkrete Gefahr für Menschen verlangt.

b) Nach MBG

Aufgaben und Befugnisse des Wachdienstes finden sich in den §§ 6-19 MBG, Aufgaben und Befugnisse der nachrichtendienstlichen Aufklärung und Abwehr in den §§ 20-25 MBG. Zu beachten ist, dass im Einsatzfall allen eingesetzten militärischen Organen die Wachbefugnisse zur Erfüllung ihrer Einsatzaufgaben zukommen.[38)]

Militärische Organe im Wachdienst dürfen - analog den Sicherheitsorganen - Angriffe gegen militärische Rechtsgüter beenden und dabei auch unmittelbare Zwangsgewalt ausüben.[39)] Auch diese Bestimmung schränkt die Eingriffsbefugnis nicht auf Rechtsgüter des Angreifers ein, sodass im erforderlichen Ausmaß auch in Rechtsgüter Dritter eingegriffen werden darf. Sie dürfen Fahrzeuge und Räume betreten (aber nicht durchsuchen[40)]) und Behältnisse öffnen[41)] sowie Sachen sicherstellen, wenn dies (u.a.) für Zwecke des militärischen Eigenschutzes erforderlich ist oder wenn von diesen Sachen eine sonstige Gefahr für militärische Rechtsgüter ausgeht oder wenn dies zur Erfüllung von Einsatzaufgaben erforderlich ist.[42)] Dies ist zwar keine unmittelbare Cyberbefugnis, kann aber als „Alternativbefugnis“ oder ergänzend eingesetzt werden, ermöglicht sie doch den physischen Zugriff auf im Inland befindliche IKT-Einrichtungen, die für Cyberangriffe gegen militärische Rechtsgüter eingesetzt werden.

Militärische Organe im Wachdienst dürfen in Ausübung ihrer Wachdienstbefugnisse auch (personenbezogene) Daten verarbeiten,[43)] wobei die Kommentarliteratur klarstellt, dass es sich dabei auch um elektronische Daten (etwa aus Zugangskontrollsystemen) handeln kann.[44)] Daher können wohl auch Daten aus Zugriffskontrollsystemen militärischer Netze darunter subsumiert werden. Diese Daten können Anhaltspunkte für Cyberangriffe liefern und Grundlagen für die Zielauswahl bei Cybermaßnahmen sein.

Militärische Organe im Wachdienst dürfen die ihnen eingeräumten Befugnisse (insbesondere jene, Angriffe gegen militärische Rechtsgüter zu beenden) als Ultima Ratio („unerlässlich“) auch mit unmittelbarer Zwangsgewalt gegen Personen und Sachen durchsetzen. Der Einsatz ist - analog zu sicherheitspolizeilichen Bestimmungen - anzukündigen bzw. anzudrohen; dies kann entfallen, wenn dadurch der Zweck der Befugnisausübung vereitelt wird.[45)] Während das SPG hinsichtlich des Waffeneinsatzes auf das Waffengebrauchsgesetz verweist, regelt das MBG alle Einsatzmittel der unmittelbaren Zwangsgewalt und nennt dabei nicht nur die dienstlichen Waffen, sondern auch „sonstige Waffen“ und „Mittel, deren Wirkung der einer Waffe gleichkommt“.[46)] Der Einsatz von Cybermaßnahmen als waffengleiches Mittel gegen IKT, die für Cyberangriffe verwendet wird (Zwangsgewalt gegen Sachen), kann darunter subsumiert werden, wobei die allgemeinen Regeln des MBG für den Waffengebrauch[47)] zu beachten sind.

Ermittlungsbefugnisse im Vorfeld von Cyberangriffen sind hingegen der nachrichtendienstlichen Abwehr zuzuordnen. Diese umfasst die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten lassen.[48)] Dabei sticht eine Inkongruenz der Befugnisse im Vergleich zur Sicherheitspolizei ins Auge, indem unter den Datenermittlungs- und Verarbeitungsbefugnissen nur Auskunftsverlangen hinsichtlich der Telefonanschlüsse bestimmter Nutzer, aber keine vergleichbaren Bestimmungen zu IP-Adressen (wie im SPG) vorgesehen sind. Zwar zieht die Kommentarliteratur Analogien zwischen althergebrachter Kommunikation per Telefon und zeitgemäßer Kommunikation per E-Mail, allerdings im Zusammenhang mit Datenschutzvorschriften (Telekommunikationsgeheimnis);[49)] eine analoge Ausdehnung einer Eingriffsbefugnis unter rechtsstaatlichen Gesichtspunkten[50)] ist nur in speziellen staatsgefährdenden Lagen vertretbar. Daher besteht im Vorfeld von Cyberangriffen eine empfindliche Lücke, weil erst im Angriffsfall oder bei konkreter Gefahr einschlägige Befugnisse zu Auskunftsverlangen seitens der Sicherheitsbehörden bestehen, im Vorfeld bei zwar erwartbaren, aber noch nicht konkreten Gefahren für militärische Rechtsgüter hingegen für die Organe der nachrichtendienstlichen Abwehr nicht. Diese ist auf die Nutzung offener (Internet-)Quellen angewiesen.

c) Anwendung der Befugnisse im Cyberspace

Der Aufgabenbereich des Abwehramtes umfasst u.a. die Angelegenheiten der klassischen nachrichtendienstlichen Abwehr[51)] und erstreckt sich über die physische Anwendung hinaus auch auf den Bereich der Cyberabwehr.[52)] Die durch den Gesetzgeber im MBG normierten Befugnisse geben somit auch den Rahmen für die Ermittlung im Cyberraum sowie für alle Maßnahmen der Cyberabwehr vor.

Für die Anwendung dieser Befugnisse wird aber nicht unterschieden, ob diese auf Bedrohungen in der realen Welt - also auf physische Gefahren - oder auf Bedrohungen aus der virtuellen Welt, dem Cyberspace, angewendet werden können und angewendet werden dürfen.

Demnach liegt der Schluss nahe, dass die im Gesetz normierten Befugnisse vorerst ausreichen müssen, um mögliche Angriffe auch aus der Cyberwelt zu erkennen, aufzuklären und letztlich entsprechend abzuwehren bzw. beenden zu können.

Der Befugniskatalog reicht dabei vom freiwilligen Auskunftsverlangen[53)] für militärische Organe zur Ermittlung sachdienlicher Hinweise über die Verarbeitung von Daten[54)] bis hin zur Observation[55)] und verdeckten Ermittlung,[56)] auch unter der Verwendung von Legenden.[57)]

§ 3 MBG normiert das Recht zur Informationsbeschaffung und zum Sammeln von Daten, die nicht in die Rechte von Personen eingreifen. Demnach können also Informationen und Daten, die nicht unter den Schutzmaßstab des DSG fallen, erhoben werden. Ein Eingriff in die personenbezogenen Rechte, insbesondere in den Grundrechtsschutz von Betroffenen, liegt nicht vor, Daten im Open Source-Bereich können daher verarbeitet werden.

Auskünfte über Betreiber öffentlicher Telekommunikationsdienste

Darüber hinaus können militärische Organe auch von den Betreibern öffentlicher Kommunikationsdienste Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses verlangen.[58)] Diese Bestimmung ist gegenwärtig jedoch nur auf Telefonverbindungen anwendbar und für den IT-Verkehr ausgeschlossen. Im Rahmen dieser Abfragemöglichkeit sind ausschließlich Stammdaten[59)] von Personen umfasst.[60)]

Kritisch zu hinterfragen ist, ob vom Auskunftsumfang dieser Norm auch die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht sowie der Zeitpunkt ihrer Übermittlung umfasst sind. Telefonnummern sowie IP-Adressen dienen der Übertragung von Informationen und sind Endkunden bzw. Teilnehmern von Telekommunikationsdiensteanbietern zugeordnet. Dabei macht es für die Abfrage der Stammdaten keinen Unterschied, dass bei dynamischen IP-Adressen die Zuordnung der Teilnehmerkennung nur temporär erfolgt, hingegen eine Telefonnummer auf die gesamte Vertragsdauer besteht.[61)]

Obwohl die Daten unzähliger IP-Adressen bereits im Internet öffentlich zugänglich sind und elektronisch im Open Source-Bereich ermittelt werden können, sind Anfragen bei Telekommunikationsunternehmen bezüglich der Zuordnung von IP-Adressen nicht vom Umfang der Befugnis des § 22 Abs. 2a MBG erfasst, während für die Sicherheitsbehörde jedoch eine entsprechende Rechtsgrundlage im SPG besteht.[62)] Standortdaten und die IMSI-Kennung (Internationale Teilnehmerkennung) dürfen zur Lokalisierung von Endgeräten durch die Sicherheitsbehörde ebenso erhoben werden.[63)]

Ermittlung von Bewegungsprofilen und Standortdaten

Zu einer der wesentlichsten Befugnisse im MBG zählt die Ermittlung von Bewegungsprofilen im Rahmen von Observationen.[64)] Die Ermittlung der Daten von Betroffenen ist demnach durch physische Beobachtung zur Erstellung von Bewegungsprofilen gesetzlich im MBG verankert. Solche Bewegungsprofile könnten ebenso unter Zuhilfenahme technischer Hilfsmittel erfolgen. So wäre einerseits die Beobachtung von Personen mittels Peilsender denkbar, andererseits aber auch durch Standortbestimmung eines Telekommunikationsgerätes, sofern eine zu observierende Zielperson ein entsprechendes Endgerät bei sich trägt.

Wenn auch im Sicherheitspolizeigesetz der Einsatz von Peilsendern rechtlich verankert ist[65)] und unter bestimmten gesetzlich normierten Voraussetzungen die Standortbestimmung in der Strafprozessordnung[66)] geregelt ist, besteht im Militärbefugnisgesetz keinerlei vergleichbare befugnisrechtliche Norm.

Die Herausforderung, Bewegungen von Personen vergleichbar mit einem Einsatz eines Peilsenders bei der physischen Beobachtung auch bei der Verfolgbarkeit im Internet zur Erstellung von digitalen Bewegungsprofilen zu gewährleisten, stellt eine Anforderung für die Zukunft unter Beachtung der raschen Entwicklung der IT dar, die gegenwärtig auch an die Grenzen des § 118a StGB gebunden ist. Mangels der entsprechenden Befugnis im MBG ist eine derartige Ermittlung jedenfalls aus rechtlichen Gründen ausgeschlossen und bleibt den militärischen Organen verwehrt.

Militärische Organe können unter bestimmten, im Gesetz geregelten Voraussetzungen und nach Prüfung und Genehmigung des Rechtschutzbeauftragten auch verdeckt ermitteln.[67)] Diese Befugnis findet ihren Handlungsspielraum ebenso im realen Anwendungsbereich von betroffenen Personen.

Vor einem Cyberangriff kann diese Methode eine durchaus wichtige Form der Datengewinnung aus dem Internet sein und zur Verteidigung bzw. Abwehr von Angriffen auf militärische Netze dienen.

Auch in diesem Zusammenhang bieten die Rechtsgrundlagen keinen Spielraum für eine verdeckte Ermittlung im Internet bzw. bei einem Cyberangriff zum vorbeugenden Schutz der militärischen IT. Für eine verdeckte Ermittlung im Internet bilden rein passive Ermittlungsmethoden innerhalb der Grenzen und Möglichkeiten via NIC-Name und unter Beachtung der rechtlichen Schranken des widerrechtlichen Zugriffes auf ein Computersystem[68)] die absolute Grenze der geltenden Rechtsordnung und stehen den militärischen Organen bei der Datengewinnung entgegen.

Das Militärbefugnisgesetz[69)] regelt ebenso die Zulässigkeit der Datenermittlung mit Bild- und Tonaufzeichnungsgeräten. Vor einem Cyberangriff könnten als Bilder gespeicherte Daten von Dokumenten in einem vernetzten Datenträger, die verdeckt aufgezeichnet werden, als Ermittlungsmethode zur Informationsgewinnung über mögliche Angriffsvektoren wichtige Hinweise liefern.[70)] Voraussetzung hierfür ist die Installation geeigneter Software auf diesen vernetzten Systemen, dem allerdings ein von der derzeitigen Rechtsordnung nicht gedecktes Eindringen in ein Computersystem für militärische Organe unter Umgehung von Sicherheitsschranken vorangehen müsste, wofür gegenwärtig keine befugnisrechtliche Norm besteht.

Informationen über ein System durch Anpingen zu beschaffen, ist als Methode zur Feststellung des Zustandes des Systems hingegen nicht auszuschließen, da die Sicherheitsschranken nicht umgangen werden; somit ist der Tatbestand des § 118 StGB in diesem Fall nicht erfüllt.

Zusammenfassung

Aus dem Verfassungsrecht abgeleitet, beschränkt sich die Tätigkeit des Österreichischen Bundesheeres auf militärische Angelegenheiten, die auf einfachgesetzlicher Basis im Wehrgesetz und im Militärbefugnisgesetz ihre Verankerung finden. Der Fokus ist dabei auf militärische Rechtsgüter sowie auf die Sicherstellung der Einsatzbereitschaft des Bundesheeres gerichtet. Die im MBG normierten Befugnisse sind in erster Linie zur physischen Abwehr von Bedrohungen und Angriffen aus der realen Welt gerichtet, müssen aber ebenso für die Cyberabwehr herangezogen werden.

Eine absolute Grenze für den Handlungsspielraum der militärischen Organe im Cyberspace sind die Cybercrime-Delikte im Strafrecht. Ergänzt werden diese Tatbestände mit den Normen des Telekommunikationsrechts, das u.a. den Rechtsrahmen für die Übermittlung von Daten und Inhalten in den Netzen der Telekommunikation festlegt.

Eindeutig festzustellen ist, dass Organe nur im Rahmen ihrer durch Gesetz eingeräumten Befugnisse handeln dürfen. Wenn auch den Sicherheitsbehörden ein weiter reichender Befugniskatalog zur Verfügung steht, so bleiben die im MBG verankerten Befugnisse für militärische Organe bindend.

Demnach sind für eine zielorientierte Cyberabwehr und den Schutz der militärischen IKT vorwiegend die nachrichtendienstlichen Befugnisse maßgeblich. Diese erstrecken sich von der allgemeinen Datenermittlung ohne Grundrechtseingriff über Auskunftsverlangen und Observationen bis hin zur verdeckten Ermittlung und geben auch bei der elektronischen Datenermittlung in der digitalen Welt den Anwendungsspielraum zur Informationsbeschaffung vor.

So ist die Abfrage von personenbezogenen Daten - insbesondere Telefonnummern bei den Telekommunikationsbetreibern - von der Rechtsordnung umfasst, nicht aber die Abfrage von IP-Adressen und der Einsatz von Peilsendern zur Erstellung von Bewegungsprofilen sowie die verdeckte Ermittlung bei infrage kommenden Plattformen und Foren im Internet.

Unter Beachtung der raschen Fortentwicklung der Technologie im Cyberbereich wären auch die Rechtsgrundlagen in Hinblick einer umfassenderen Ermittlungsmethodik zu forcieren. Die Informationsbeschaffung auch außerhalb des Open Source-Bereiches ist für militärische Nachrichtendienste ein wesentliches Erfordernis und sollte, wenn auch unter der rechtsstaatlichen Kontrolle des Rechtsschutzbeauftragten, eine Verankerung in der Rechtsordnung finden und den militärischen Organen für eine erfolgreiche Cyberabwehr zur Verfügung stehen.

Abschließend kann festgestellt werden, dass es derzeit keine rechtliche Grundlage für das heimliche Eindringen in ein Computersystem durch militärische Nachrichtendienste gibt. Wie bereits näher erwähnt, besteht nur die Befugnis zur Erhebung von Stammdaten im MBG. Verkehrsdaten und Inhaltsdaten dürfen auf keinen Fall erhoben werden.

Das Fernmeldegeheimnis[71)] steht dem Abhören von Telefongesprächen, dem Abfangen und Lesen von E-Mails oder sonstigen Kommunikationsmethoden entgegen. Die rechtskonforme Anwendung der Befugnisse ist insofern gewährleistet, als eine Überschreitung der Befugnisse durch militärische Organe den Tatbestand des Missbrauches der Amtsgewalt[72)] erfüllen und somit strafbar sein kann.

Ein Nachrichtendienst muss auch schon im Frieden die Informationen beschaffen können und über entsprechende Maßnahmen und Befugnisse verfügen, um Informationen über vermeintliche Gegner und potenzielle Angreifer sammeln zu können. Demnach wäre zu überdenken, ob die erforderlichen rechtlichen Rahmenbedingungen für die Identifizierungsmöglichkeiten geschaffen werden sollten.

Die Ermittlung von Daten sowohl bei Software- als auch Hardwarekomponenten, aber auch von klassifizierter Information, die für den Einsatz und die militärische Landesverteidigung im Inland und Ausland erforderlich sind, ist zwingend notwendig. Das Wissen und Kennen der Gegner, der Methoden und sämtlicher Angriffsvektoren auch von fremden IT-Systemen, also die Information selbst, ist der Weg zur erfolgreichen Cyberabwehr.

Vorbereitungen des ÖBH - milCERT und Cyber Defence

Die Verteidigung des Cyberraumes (Cyber Defence) ist definitionsgemäß ein integriertes System und besteht in seiner Gesamtheit aus der Umsetzung der Maßnahmen zur IKT-Sicherheit und der Informationssicherheit, aus den Fähigkeiten des milCERT, der CNO (Computer Network Operations) und der Unterstützung durch die physischen Fähigkeiten der Streitkräfte.

Die Maßnahmen zur IKT- und Informationssicherheit sind für die Cyber Defence von wesentlich höherer Bedeutung als die Maßnahmen der militärischen Sicherheit für die klassische Verteidigung. Da Cyberangriffe ohne Vorwarnung erfolgen können und sehr rasch ablaufen, müssen die einsatzwichtigen IKT-Systeme auch im tiefsten Frieden einen sehr hohen Schutzzustand aufweisen. Konzeptiv sind die besonders wichtigen Systeme im gesamten Lebenszyklus einem lückenlosen Risikomanagement zu unterziehen. Schon in der Planungs- und Entwicklungsphase sind Analysen der Bedrohungen und Schwachstellen durchzuführen und ein Sicherheitskonzept zu entwickeln. IKT-Systeme sind zu akkreditieren und in gut geschützten Objekten zu betreiben sowie regelmäßig zu auditieren. Sicherheitsvorfälle sind zu untersuchen und sollten zur Überführung von Tätern führen. Die Ergebnisse der Audits und der untersuchten Vorfälle müssen zur Abstellung von Mängeln und Schwachstellen führen. Eine gut aufgestellte Sicherheitsorganisation mit laufend fortgebildetem verlässlichem Personal und der Einsatz von am neuesten Stand befindlicher Sicherheitstechnik (FW, IDS, IPS, Sandboxing u.a.) haben ein hohes Sicherheitsniveau zu gewährleisten. Damit sollten Bedrohungen mit geringem bis mittlerem Gefährdungsgrad abgehalten werden.

Für groß angelegte Angriffe sind erhebliche, zusätzliche Vorkehrungen zu treffen. Dazu ist der Aufbau der Fähigkeiten des Militärischen Cyber Emergency Readiness Teams (milCERT) von zentraler Bedeutung. Das milCERT hat, abgestützt auf eine umfangreiche und ständig zu erweiternde Wissensbasis, die Darstellung eines konsolidierten permanent aktuellen Cyber Defence-Lagebildes für den militärischen und als Beitrag für den gesamtstaatlichen Bedarf sicherzustellen. Das milCERT-Lagebild sollte die globale Cyberbedrohungslage, die Situation der militärischen IKT-Systeme, die Ergebnisse der Schnittstellenüberwachungssysteme, nachrichtendienstliche und Erkenntnisse aus der Analyse von Malware und Angriffsmethoden umfassen. Eine Erweiterung um die Systeme anderer Behörden sowie der sonstigen strategischen Infrastruktur sollte möglich sein. Aus dem Lagebild sind permanent Empfehlungen und Vorgaben für die Optimierung der IKT-Sicherheit abzuleiten. Lageinformationen haben laufend zu ergehen, und der Alarm- und Warndienst schafft die Voraussetzung für ein rasches Hochfahren der Verteidigungsmaßnahmen. Für den Fall von groß angelegten Cyberangriffen muss das milCERT technisch und personell so ausgestattet sein, dass es in der Lage ist, auf Vorfälle rasch zu reagieren, Unterbrechungen des ordnungsgemäßen Betriebes auf ein Minimum zu reduzieren sowie die Koordination des Incident Management durchzuführen. Die Fähigkeit zur Unterstützung der Erhebung der Angreifer /Täter durch die Strafverfolgungsbehörden und Nachrichtendienste sollte vorhanden sein.

Das milCERT sollte Trendanalysen, einen Warn- und Informationsdienst und Beratungsleistungen für die strategische und operative Ebene bereitstellen sowie Sensibilisierungsmaßnahmen anbieten. Mit einem Frühwarnsystem sollten Angriffe frühzeitig detektiert und eine koordinierte Reaktion ausgelöst werden können. Dabei sind die unverzügliche Lageinformation an die strategische Ebene, die Alarmierung möglicher Betroffener und die Veranlassung forensischer Maßnahmen zu berücksichtigen. Eine 24/7 Netzwerk-Überwachungsfähigkeit sowie die Fähigkeit, Verteidigungsmaßnahmen sehr rasch hochzufahren, sind bei den IKT-Betreibern zu etablieren und durch das milCERT zu steuern.

Das milCERT muss in der Lage sein, Vorfallmanagement zu betreiben und zu koordinieren sowie die nationale Zusammenarbeit der CERTs und die internationale Zusammenarbeit zu gewährleisten. Erforderliche abhörsichere, redundante Kommunikationsverbindungen für Lagemeldungen und Reaktionskoordinierung sind einzurichten. Forensische Fähigkeiten, um Angriffe eindeutig konkreten Angreifern zuordnen zu können, müssen vorhanden sein. Hierfür müssen leistungsfähige technische Mittel zur Analyse und Speicherung riesiger Datenmengen vorgehalten werden. milCERT sollte in der Lage sein, mobile Cyber Defence Teams („Cyber-Feuerwehr“) für den Fall einzusetzen, dass Remote-Maßnahmen oder im Einsatzgebiet verfügbare Expertise nicht ausreichen. Damit sollte ein wesentlicher Beitrag für die rasche Widerherstellung normaler Betriebsbedingungen und Unterstützung für die Aufrechterhaltung kritischer Dienste und Prozesse geleistet werden.

Weiters sind Elemente zur aktiven Verteidigung aufzubauen. Diese haben Fähigkeiten zum Scannen und Blocken von Schadprogrammen/-routinen des Netzwerkverkehrs an den Schnittstellen zu nationalen, für die Verteidigung bedeutsamen Netzwerken zu entwickeln.

Notfallpläne, das Bereithalten redundanter Systeme wie Ausweichrechenzentren, USV und anderer Maßnahmen sollten eine sehr hohe Verfügbarkeit der militärischen IKT sicherstellen. Bei den Streitkräften könnten nach einer vorausschauenden Erhebung und adäquater Ressourcenzuordnung redundante Systeme für die Regierungs- und allgemeine Kommunikation aufgebaut und im Krisenfall betrieben werden. Darüber hinaus sind Fähigkeiten zum elektronischen Kampf und für CNO in Einsatzräumen aufzubauen und bereitzuhalten. Alle aufzustellenden Elemente sind so zu strukturieren, dass eine sehr rasche Verstärkung auf der Basis aktueller und erprobter Alarm- und Notfallpläne erfolgen kann.

Die volle Einsatzbereitschaft der die milCERT-Fähigkeit liefernden Organisationselemente des Abwehramtes und des Führungsunterstützungszentrums liefern damit die Hauptfähigkeiten für die Cyber Defence des ÖBH. In einem Evaluierungsschritt ist die Weiterentwicklung zu einem Cyber Defence-Zentrum zu analysieren. Dieses Zentrum bildet gemeinsam mit dem Cyber Security-Zentrum beim Bundesamt für Verfassungsschutz im Bundesministerium für Inneres die operative Basis für den Schutz bzw. die Verteidigung des Cyberraumes. Die Koordination dieser operativen Struktur ist bereits im Frieden einzurichten. Diese Koordinierungsstruktur muss sich am Bedarf der potenziellen Einsatzszenarien orientieren und könnte sehr ressourcenschonend durch die Leiter der beiden Zentren abgedeckt werden. Eine enge Zusammenarbeit mit den govCERT und allen anderen österreichischen CERTs sowie den Sicherheitsverantwortlichen der kritischen Unternehmen ist aufzubauen. Für die Cyber Defence und das Funktionieren der kritischen Infrastruktur ÖBH ist die Versorgung mit elektrischer Energie und Kommunikationsdienstleistungen von herausragender Bedeutung und daher bei der Einsatzvorbereitung besonders zu berücksichtigen. Der Aufbau weiterer Ebenen zwischen der strategischen und operativen widerspricht dem Bedarf und sollte vermieden werden.

Ausblick

General Naumann meint, dass neutrale Staaten des 21. Jahrhunderts die Bewältigung der überwiegend globalen Gefahren „nur noch durch Bündnisse oder internationale Organisationen“ erreichen werden.[73)] Verteidigung im 21. Jahrhundert umfasst nicht nur die drei herkömmlichen Dimensionen (Land, Luft, See), sondern zusätzlich auch den Weltraum und den Cyberraum.[74)] Verteidigung ist keine Aufgabe der Streitkräfte alleine mehr, sondern „erfordert den Verbund aller Sicherheitskräfte, eine verzugsarm handelnde, interministerielle und die Gesamtheit des Staates erfassende Führung, und sie reicht vom Schutz in humanitären Notfällen und Naturkatastrophen über den Kampf gegen organisierte Kriminalität bis hin zur Abwehr von und zum Schutz gegen die Wirkung von ABC-Waffen, von Luftangriffsmitteln und von Cyberangriffen.“[75)]

Naumanns Ausführungen bestätigen den Weg, den Österreich eingeschlagen hat, und sollten Ansporn sein, die Konzeptentwicklung zügig abzuschließen und den Auf- und Ausbau der geplanten Instrumente zum Schutz des Cyberraumes voranzutreiben. Im nationalen Verbund aller Cybersicherheits- und -verteidigungskräfte, eingebettet in der EU und partnerschaftlich mit der NATO, sollte ein hinreichender und resilienter Schutz des Cyberraumes erreichbar sein.

ANMERKUNGEN:

1) Der Autor dankt Frau Ella-Maria Moritz für ihre wertvolle Unterstützung.
2) Der Artikel folgt im ersten Teil weitgehend folgendem Aufsatz: Walter J. Unger: Cyber Defence - eine nationale Herausforderung. In: Michael Brzoska, et al. (Hrsg.): S+F Sicherheit und Frieden. Security and Peace. 32/1 (2014), S.8-16.
3) Art. 10 Abs. 1 Z 7 B-VG.
4) Art. 10 Abs. 1 Z 15 B-VG.
5) Art. 78a B-VG.
6) Art. 79 B-VG.
7) § 1 iVm § 4 Abs. 1 Z 1 KSE-BVG.
8) Der Begriff „Polizei“ ist hier inhaltlich (nicht organisatorisch) zu verstehen.
9) Keplinger, SPG (Polizeiausgabe), 12. Aufl. 2012.
10) § 16 Abs. 1 und 2 SPG.
11) § 16 Abs. 4 SPG.
12) Für Österreich in Kraft getreten mit 1.1. 2012.
13) § 2 Abs. 1 lit a-d WG.
14) § 2 Abs. 3 WG.
15) § 2 Abs. 4 WG.
16) Art. 2 Z 4 UN-Charta schützt die zentralen Rechtsgüter der Staaten im Völkerrecht, soveriegnty, territorial integrity und political idependence, vor rechtswidrigem Zwang durch Androhung oder Anwendung von Gewalt (threat or use of force).
17) § 1 Abs. 7 MBG.
18) § 1 Abs. 8 MBG. - Insoweit irreführend Keplinger/Kreutner/Sauer: MBG Praxiskommentar, 2. Aufl. Linz 2009: Zwar weisen sie zutreffend darauf hin, dass das MBG pauschal auf Straftatbestände verweist, wohingegen § 16 SPG nur auf jene des StGB, des VerbotsG und des Suchtmittelgesetzes zeigt, doch schützt das SPG alle in diesen Strafgesetzen normierten Rechtsgüter, wohingegen hinsichtlich des MBG nur jene Delikte in Frage kommen, die sich gegen die im MBG selbst genannten Rechtsgüter richten. Im Ergebnis ist die sachliche Reichweite des MBG also wesentlich geringer als jene des SPG. Die EB der RV zur Novelle 2003 („Beschränkung des Militärbefugnisgesetzes auf unmittelbar militärrelevante Umstände“) bestätigen diese Auffassung.
19) Nicht gerichtlich strafbare bloße Verwaltungsübertretungen, die gegen militärische Rechtsgüter gerichtet sind.
20) § 1 Abs. 4 MBG.
21) § 1 Abs. 5 MBG.
22) Vgl. § 73 Abs. 2 iVm Anhang G LVR 2010.
23) Für eine solche vgl. etwa Reindl, Computerstrafrecht im Überblick, Wien 2004.
24) BGBl I 70/2003 idF zuletzt BGBl I 96/2013.
25) § 2 Abs. 1 TKG.
26) § 74 Abs. 2 TKG.
27) § 93 Abs. 3 TKG.
28) § 96 Abs. 1 TKG.
29) § 94 Abs. 4 iVm § 99 und § 102a TKG.
30) § 33 SPG.
31) Vgl. Keplinger (Anm. 15), 100, und Hauer/Keplinger, SPG-Kommentar, zu § 33 SPG.
32) § 42 Abs. 1 Z 1 SPG.
33) § 44 SPG.
34) Vgl. Keplinger (Anm. 15) und Hauer/Keplinger (Anm. 70).
35) § 50 SPG.
36) Keplinger (Anm. 15), Keplinger/Hauer (Anm. 70).
37) Art. 53 Abs. 3a Z 2 und 3 SPG.
38) § 6 Abs. 3 MBG.
39) § 6a iVm 16 MBG. Vgl. Keplinger/Kreutner/Sauer: MBG-Praxiskommentar, 2. Aufl. 2009, 91.
40) Keplinger u.a. (Anm. 76), 129.
41) § 13 MBG.
42) § 14 Abs. 1 MBG.
43) § 15 iVm § 1 Abs. 6 MBG.
44) Keplinger u.a. (Anm. 76), 138.
45) § 16 MBG.
46) § 17 MBG.
47) §§ 18 und 19 MBG.
48) § 20 MBG.
49) Keplinger u.a. (Anm. 76), 183.
50) Art. 18 B-VG.
51) Darunter versteht man die Abwehr von Spionage, Sabotage und sonstigen kriminellen Handlungen gegen militärische Rechtsgüter.
52) Bezogen auf den Schutz von militärischen Rechtsgütern, die Schnittstelle zwischen MBG und SPG ist in § 2 MBG nach den Vorgaben der Subsidiarität geregelt.

Vgl. § 16 Abs. 1bis 3 SPG und VwGH vom 23 01 2004 (G363/02).
53) § 21 MBG.
54) § 22 MBG.
55) § 22 Abs. 3 MBG.
56) § 22 Abs. 4 MBG.
57) § 22 a MBG.
58) § 22 Abs. 2a MBG.
59) Vgl. Jahnel, Mader, Staudegger: IT Recht 3. Auflage, 716.
60) § 93 Abs. 3 Z 3 TKG umfasst.
61) Vgl. Platzer: Die Befugnisse der Nachrichtendienste in Österreich, Deutschland und der Schweiz im Bereich der Informationstechnologie, Eigenverlag; im Besitz des Verfassers.
62) § 53 Abs. 3a SPG.
63) Diese Befugnis dient nicht dem nachrichtendienstlichen Ermittlungszweck, sondern dient dem Selbstschutz einer gefährdeten Person bei einer gegenwärtigen Gefahr für Leib und Leben.
64) Die Datenermittlung durch Beobachten (Observation) ist zulässig. 1. zur Abwehr gegenwärtiger vorsätzlicher Angriffe gegen militärische Rechtsgüter unter Bedachtnahme auf die militärische Zuständigkeit nach § 2 Abs. 2. 2. zum vorbeugenden Schutz militärischer Rechtsgüter, sofern aufgrund bestimmter Tatsachen mit vorsätzlichen Angriffen gegen militärische Rechtsgüter zu rechnen ist. 3. für Zwecke der nachrichtendienstlichen Aufklärung, wenn sonst die Aufgabenerfüllung der Aufklärung verhindert oder erheblich behindert wäre. Eine Observation erfolgt ausschließlich nach den Regeln der Verhältnismäßigkeit und nach Genehmigung des Rechtsschutzbeauftragten. Dabei wird in das Grundrecht iSd Art. 8 EMRK (VfSlg 17102/2004) eingegriffen. Vgl. Raschauer/Wessely, Militärbefugnisgesetz, Kommentar, S.106ff.
65) § 54 Abs. 2a SPG, Zur Unterstützung der Observation gemäß § 54 Abs. 2 ist der Einsatz technischer Mittel, die im Wege der Übertragung von Signalen die Feststellung des räumlichen Bereichs ermöglichen, in dem sich die beobachtete Person oder der beobachtete Gegenstand befindet, zulässig, wenn die Observation sonst aussichtslos oder erheblich erschwert wäre.
66) § 135 StPO.
67) § 22 MBG.

68) § 118 StGB.
69) § 22 Abs. 5 MBG.
70) § 22 Abs. 5 iVm mit Abs. 4 MBG.
71) Art. 10a StGG.
72) § 302 StGB.
73) Naumann, S.143f.
74) Naumann, S.145.
75) Naumann, S.145.