Beitrag zum Sammelband über die 53. Sicherheitspolitische Informationstagung 2019

Minister Holger Stahlknecht

Sehr geehrter Herr HERRMANN sehr geehrter Herr KOHL, *sehr geehrte(r) namentliche Ehrengäste),* meine sehr geehrten Damen und Herren im Auditorium.

Ich danke Ihnen recht herzlich für die Einladung zu der heutigen Veranstaltung und die Gelegenheit, Ihnen aus der Sicht eines verantwortlichen Innenpolitikers einige ausgewählte aktuelle Herausforderungen im Bereich der Inneren Sicherheit in Deutschland näher zu bringen.

Als Minister für Inneres und Sport des Landes Sachsen-Anhalt UND als Offizier der Reserve der Bundeswehr ist es mir eine besondere Herzensangelegenheit, die Kommunikation zwischen unseren überwiegend im Inneren tätigen Behörden und Organisationen mit Sicherheitsaufgaben einerseits und der Bundeswehr andererseits zu stärken. Dies gilt insbesondere für aktuelle und künftige schwierige Aufgaben, die noch vor uns liegen.

Meine Damen und Herren, in der Vorbereitung auf meinen Vortrag bin ich auf ein Zitat gestoßen, das dem einen oder anderen von Ihnen bekannt vorkommen wird und das ich gerne als übergeordnetes Leitthema für meine Ausführungen nutzen möchte:

„Unvorhergesehene Gelegenheiten sind unverzüglich zu nutzen, und auf unvorhergesehene Schwierigkeiten ist sofort zu reagieren.“ (Carl von Clausewitz)

Unabhängig von der Natur oder dem geographischen Auftreten einer sicherheitspolitischen Herausforderung sind wir uns, denke ich, alle im Klaren darüber, dass unverzüglichem Handeln eine überragende Bedeutung zukommt. Dies bedeutet keinesfalls, dass die Handlung vor einer genauen Situationsanalyse liegen soll. Aber ein koordiniertes und auf intensiver Ursachenbetrachtung beruhendes schnelles Agieren birgt die besten Chancen, Herausforderungen nicht in Probleme ausufern zu lassen, möglichst schon in einem frühen Stadium wieder abzustellen oder zumindest die Folgewirkungen deutlich zu minimieren. Welches sind nun aber aktuelle Herausforderungen im Bereich der inneren Sicherheit in Deutschland und wie begegnen wir diesen im Moment? Dafür möchte ich im Folgenden vier ausgewählte Beispiele kurz thematisieren:

- Cyberkriminalität;
- Extremistische Gewalttaten/ Politisch
    - motivierte Kriminalität;
- die sogenannte „Clankriminalität“ sowie
- die europäische Zusammenarbeit im Bereich
    - der Inneren Sicherheit.

Bereits in der Einladung zu dieser 53. Sicherheitspolitischen Informationstagung 2019 der Clausewitz Gesellschaft e.V. wird festgestellt: Zitat „im digitalen Zeitalter vor allem

Verwundbarkeiten im Cyber- und Informationsraum und hybriden Angriffen unterhalb der Schwelle klassischer, traditioneller Kriegsformen besondere Aufmerksamkeit zu widmen“ ist.

Wenn wir in Deutschland polizeilich von Cyberkriminalität sprechen, so betrachten wir hier im engeren Sinne Straftaten, die sich gegen

- das Internet,
- weitere Datennetze,
- informationstechnische Systeme

oder damit übermittelte, gespeicherte und verarbeitete Daten richten. Mit der zunehmenden Nutzung von IT, aber auch z.B. durch die unzureichende Absicherung noch verwendeter älterer Technik ergeben sich weitere Möglichkeiten des Missbrauchs und der Begehung von Straftaten. Deutschland stellt dabei, aufgrund seines hohen Entwicklungsstands und Know-hows (insbesondere der Wirtschaft) weltweit ein attraktives Ziel für Cyberkriminelle dar. Bei einer Forsa-Befragung im Frühjahr 2018 zum Thema „Cyberrisiken und der deutsche Mittelstand“ (repräsentative Befragung von 300 Entscheidern bei kleinen und mittleren Unternehmen) gaben 30% der Befragten an, durch Attacken von Cyberkriminellen bereits wirtschaftliche Schäden erlitten zu haben. Die Gesamtzahl der festgestellten Schadprogrammvarianten hat sich von 2014 bis 2017 mehr als verdoppelt. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge sollen 2018 mehr als 800 Millionen Schadprogramme im Umlauf gewesen sein (Vergleich 2017: >600 Millionen).

Die bedrohlichsten Phänomene der Cyberkriminalität sind heute:

a) Botnetze / DDos-Angriffe: Hierbei wird zum einen oft unbemerkt Schadsoftware auf Opfer-IT-Systemen zwecks gebündelten Missbrauch zu kriminellen Zwecken installiert und ferngesteuert. Zum anderen werden durch massive Datenanfragen durch Botnetze an ausgewählte Server diese überlastet.

b) Ransomware: Eine „Erpressungs-Schadsoftware“ verschlüsselt ungewollt Daten eines digitalen Systems, was in den meisten Fällen jedoch auch nach Zahlung eines „Lösegeldes“ nicht wieder zur Entschlüsselung bzw. Entsperrung des infizierten Systems führt.

c) Diebstahl digitaler Identitäten

Die digitale Identität als Ganzes oder zumindest Teile davon sind begehrtes „Diebesgut“ von Cyberkriminellen, sei es, um die erlangten Informationen für die eigenen kriminellen Zwecke einzusetzen oder um die gestohlenen Daten über illegale Verkaufsplattformen weiter zu veräußern.

d) Tatmittel Internet

Nahezu sämtliche Kriminalitätsphänomene werden zwischenzeitlich auch über das Internet begangen. Durch sich permanent weiter entwickelnde Modi Operandi werden klassische Deliktsbereiche, wie z. B. Erpressungen und Betrugsdelikte sowie der Handel mit inkriminierten Gütern unter der Nutzung von internetverbundenen IT-Systemen abgewickelt.

e) Kritische Infrastrukturen (KRITIS)

> In den vergangenen drei Jahren waren in Deutschland diverse beeinträchtigende Cyberangriffe auf Unternehmen der KRITIS-Sektoren wie z. B. Gesundheit, Transport und Verkehr sowie Energie zu verzeichnen. Von einer weiteren Zunahme derartiger Angriffsversuche auf Kritische Infrastrukturen und damit verbundener gefährdungsrelevanter Auswirkungen ist auszugehen.

Meine Damen und Herren, wie agieren die Strafverfolgungsbehörden heute, um diesen Bedrohungen zu begegnen? Die Bekämpfung von Cybercrime ist ein herausragender deliktischer Schwerpunkt bei allen Polizeien des Bundes und der Länder. Aus diesem Grund wurde zur Erarbeitung einer Bekämpfungsstrategie im Jahr 2015 eine Bund-Länder-Projektgruppe (BLPG) eingerichtet. Sie informiert über maßgebliche aktuelle Trends, geht auf zunehmende bzw. zukünftige Gefährdungspotenziale ein und spricht konkrete Handlungsempfehlungen aus. Maßgebliche Ziele sind eine flexible und ganzheitliche Bekämpfung von Cybercrime auf nationaler und internationaler Ebene, optimierte, risikoorientierte Ressourcensteuerung sowie der Aufbau einer hinreichenden Cyber-Grundkompetenz auch in klassischen Ermittlungsbereichen.

Im Kontext Darknetermittlungen wurde beim BKA eine Zentrale Informations- und Koordinierungsstelle Darknet (ZIK) eingerichtet.
Zur Vernetzung und zum regelmäßigen Informationsaustausch zwischen staatlichen Institutionen und der Wirtschaft wurden die Zentralen Ansprechstellen Cybercrime (ZAC) des Bundes und der Länder geschaffen.

Im internationalen Rahmen, da oftmals ausländische IT-Infrastrukturen zur Durchführung von Angriffen genutzt werden oder die Täterstrukturen international zusammengesetzt sind, arbeiten Strafverfolgungsbehörden in Kooperation mit überstaatlichen Institutionen wie Europol und Interpol koordiniert zusammen:
2013 nahm das Europäische Zentrum zur Bekämpfung der Cyberkriminalität unter dem Dach von EUROPOL seine Arbeit auf und koordiniert die grenzübergreifende Strafverfolgung der Cybercrime in der EU. 2015 eröffnete Interpol den Global Complex for Innovation (IGCI) in Singapur, um IKPO-Interpol Mitgliedsstaaten bei der Bekämpfung grenzüberschreitender Cybercrime zu unterstützen.

In Deutschland sind darüber hinaus neben dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) die Verfassungsschutzbehörden des Bundes und der Länder mit der Abwehr von Cyberspionage betraut. BKA, BfV, BSI und weitere Bundesbehörden wirken im Nationalen Cyberabwehrzentrum (NCAZ) zusammen und stimmen sich bei größeren Angriffswellen ab.

Meine Damen und Herren, schauen wir uns nun ein weiteres, leider sehr aktuelles Kriminalitätsphänomen an: die Politisch motivierte Kriminalität. Insbesondere die in den zurückliegenden Wochen bekanntgewordenen sogenannten Feindeslisten und das Tötungsdelikt zum Nachteil des Kasseler Regierungspräsidenten haben uns allen vor Augen geführt, dass das Phänomen des Rechtsextremismus seinen Schrecken nicht verloren hat. Die im Zuge des NSU-Prozesses erkennbar gewordenen Defizite bei der frühzeitigen Erkennung haben verdeutlicht, dass es der gemeinsamen Anstrengung aller politischen und gesamtgesellschaftlichen Akteure bedarf: Die Bekämpfung des politischen Extremismus, und hier ist der Extremismus jeden Lagers gemeint, ist ständiges Thema der Befassung der Politik in den Ländern und auf Bundesebene.

Die Entwicklung des Rechtsextremismus ist auf Bundesebene in den letzten Jahren zwar leicht rückläufig. Allerdings bewegen sich die Fallzahlen mit rund 20.000 Delikten auf einem hohen Niveau. Strukturen des traditionellen Rechtsextremismus sind nach wie vor aktiv, jedoch ist ein Wandel in der Szene feststellbar, der im Wesentlichen von der Digitalisierung und internetbasierter Kommunikation beeinflusst wird. Die mit Hilfe der modernen Medien ohne großen Aufwand zu erreichenden Personenpotentiale lassen sich insbesondere nach Ereignissen wie Chemnitz und Köthen kaum noch trennscharf in Anhänger der Szene und bloße Sympathisanten unterscheiden.

Im Bereich des Linksextremismus ist die Fallzahlenentwicklung in erfreulichen Größenordnungen rückläufig. Wies die Statistik PMK-links für das Jahr 2017 noch 9.752 Delikte aus, waren es im Jahr 2018 noch 7.961 Straftaten. Die positive Entwicklung der Fallzahlen sollte indes nicht dazu verleiten, die aus dem Lager des Linksextremismus drohende Gefahr zu unterschätzen, wie die unfriedlichen Proteste anlässlich des G20-Gipfels oder die gewalttätigen Aktionen im Zusammenhang mit der Räumung des Hambacher Forstes zeigen. Auch in diesem Phänomenbereich führt die schnellere Kommunikation singulärer Ereignisse zu einem nicht mehr vorhersehbaren Mobilisierungspotential. Bei den G20-Protesten und auch bei den Räumungsaktionen im Hambacher Forst sind zahlreiche Störer festgestellt worden, die überregional und international agierten.

Für erwähnenswert halte ich auch, dass linksextremistische Strukturen z.B. die türkische Militäroffensive im Norden Syriens und die öffentliche Diskussion um innenpolitische Entwicklungen in der Türkei nutzen, um ihre Vernetzungen zum türkischen und kurdischen extremistischen Spektrum auszubauen.

Für den Bereich des Islamistischen Terrorismus ist zu konstatieren, dass die Bedrohungslage, auch in Deutschland, weiter anhält. Es ist lediglich der akribischen Arbeit unserer Sicherheitsbehörden zu verdanken, dass eine Reihe von aufgedeckten Anschlagsplanungen in unterschiedlichen Vorbereitungsstadien nicht in einem terroristischen Ereignis ihren Abschluss fand. Deutschland gilt nach wie vor als Ziel jihadistischer Organisationen. Zurückliegend sind die Anschläge vermehrt mittels leicht zu beschaffender und einzusetzender Tatmittel ausgeführt worden. Langfristig fürchtet bspw. Europol, dass die Nutzung von Drohnen, wie sie durch den „Islamischen Staat“ in Syrien und im Irak bereits üblich ist, auch Terroristen für Anschläge in Europa inspirieren könnte. Vorrangig wird zudem mit Anschlägen auf leicht zugängliche „weiche“ Anschlagsziele zu rechnen sein. Bisherige Taten wurden meist von angeleiteten Einzeltätern oder Kleinstgruppen, teilweise unterstützt von Angehörigen der verschiedenen, weltweit operierenden Terrororganisationen wie DAESH oder Al Qaida, verübt.

Meine Damen und Herren, um den Bedrohungen des Extremismus und Terrorismus wirksam begegnen zu können, verfolgen die deutschen Strafverfolgungsbehörden Strategien, die auf gesetzgebende und präventive Maßnahmen sowie eine effektive Strafverfolgung setzen. Zudem sind bei Polizei und Verfassungsschutz verstärkt Personal zugeführt, Organisationsstrukturen angepasst und ist erheblich in die materielle Ausstattung investiert worden.

Auch die Zusammenarbeit mit und in der EU sowie mit unseren ausländischen Verbündeten und Partnern wurde forciert, so wurde u.a. 2016 bei Europol das Europäische Zentrum zur Terrorismusbekämpfung (ECTC) eingerichtet, das den Mitgliedstaaten eine Plattform für den Informationsaustausch und die verstärkte operative Zusammenarbeit bietet.

Ein weiteres, sehr aktuelles Thema in Deutschland ist die sogenannte „Clankriminalität". Zurückliegend ist das Verhalten von Mitgliedern türkisch-arabischer Großfamilien (sog. „Clans") in der Öffentlichkeit und die ihnen mutmaßlich zuzurechnenden Straftaten Gegenstand einer hefigen medialen Diskussion gewesen. Dabei wurden unter anderem die Problembereiche Ablehnung der deutschen Rechtsordnung durch Clanangehörige und Entstehung sog. rechtsfreier Räume thematisiert.

In der polizeilichen Wahrnehmung sind „Clans" durch ethnische Geschlossenheit und abgeschottete, auf Familienzugehörigkeit reduzierte Strukturen gekennzeichnet. Die ethnische Geschlossenheit spielt bei der Begehung von Straftaten eine herausragende Rolle. Bei der Identifizierung von Personen, welche als Angehörige von „Clans" handeln, stellten verschiedene Landespolizeien fest, dass die „Clans" auch bundeslandübergreifend und international, in einer Vielzahl von legalen und illegalen Geschäftsfeldern agieren. Der Handel mit illegalen Betäubungsmitteln (Kokain und Cannabis) spielt eine zentrale Rolle. Der Betrieb von Shisha Bars, Glücksspielstätten und Wettbüros , aber auch das Angebot von Security-Dienstleistungen, welche z. B. bei der sog. Türsteherszene in Bars oder Diskotheken auch den Vertrieb von Drogen begünstigt, gehören dazu. Die Erlöse aus den kriminellen Aktivitäten werden dann häufig, zur Geldanlage aber auch zur Geldwäsche, in Immobilien angelegt.

Wie ist diesem Kriminalitätsphänomen nun zu begegnen? Ein Schwerpunkt polizeilichen Handelns ist es, in betroffenen Räumen eine starke sichtbare Polizeipräsenz sowie eine Null-Toleranz-Strategie zu praktizieren. Dieses Einschreiten muss sich auf alle Lebensbereiche beziehen und bedarf des Zusammenwirkens aller staatlichen Behörden, natürlich in erster Linie der Polizei, aber auch der Ordnungs- und Ausländerämter, Gewerbe- und Gaststättenaufsicht, Straßenverkehrsbehörden, Sozialämter, Zoll- und Steuerbehörden etc. Die interbehördliche Zusammenarbeit aller Partner in der öffentlichen Verwaltung hat sich als entscheidender Faktor für eine effektive Bekämpfung der „Clankriminalität" herausgestellt. Vermehrt finden z. B. gemeinsam geplante und durchgeführte Aktions- und Kontrolltage statt. Auch die Identifizierung kriminell erlangter Vermögenswerte steht weiter im Fokus des staatlichen Handelns: Verbrechen darf sich nicht lohnen, eine effektive Gewinnabschöpfung ist zu gewährleisten. Und da es auch hinreichende Erkenntnisse gibt, dass die „Clans" nicht nur im Bundesgebiet, sondern auch im europäischen Ausland und darüber hinaus vernetzt sind, wird die Einbindung insbesondere europäischer Behörden wie Europol oder Nutzung von Verfahren wie z.B. des europäischen Informationsaustauschsystems SIENA durch die deutschen Polizeien forciert.

Meine Damen und Herren, lassen Sie mich im Weiteren näher auf die bereits mehrfach angesprochene europäische Zusammenarbeit im Bereich der Inneren Sicherheit eingehen:

Neben der Bedrohung durch den Terrorismus sind in dem von Europol herausgegebenem aktuellen Bericht zur Bewertung der schweren und organisierten Kriminalität SOCTA[1] 2017 folgende fünf prioritäre Bereiche mit einer „großen Gefahr" für Europa beschrieben: Cybercrime, Drogenproduktion und -handel, Menschenhandel, Schleusung von Migranten sowie organisierte Eigentumskriminalität. Auch diese Kriminalitätsfelder stellen Herausforderungen für die Zukunft dar. Europol steht hier im Zentrum der europäischen Sicherheitsarchitektur. Es bietet eine einzigartige Palette von Dienstleistungen (u. a. den

[1] SOCTA - Serious and Organised Crime Threat Assessment; Lagebericht erscheint alle 2 Jahre; letztmalig erschienen 2017, nächster SOCTA erscheint voraussichtlich im Jahr 2019.

größten Pool analytischer Kompetenz in der EU, EU-weite Informationssysteme) für die Strafverfolgungsbehörden der Mitgliedstaaten der EU bei der Bekämpfung der internationalen schweren Kriminalität und des Terrorismus.

Ein weiterer Punkt der Zusammenarbeit betrifft die finanziellen Vorteile aus Straftaten: Schätzungen zufolge werden in der EU jährlich 110 Milliarden Euro aus kriminellen Aktivitäten generiert. Allerdings werden nur 1,1 Prozent der Erlöse aus Straftaten effektiv eingezogen. Um das Einfrieren und Beschlagnahmen von kriminellen Vermögen in der gesamten EU zu erleichtern, wurden im Oktober 2018 neue Regeln vereinbart und die Anti-Geldwäsche-Richtlinie aktualisiert.

Bezüglich der Praxis, dass Kriminelle und Terroristen oft mehrere falsche Identitäten verwenden, um sich den Grenz- und Strafverfolgungsbehörden zu entziehen spielt das Schengener Informationssystem (sog. SIS) eine große Rolle. Es handelt sich hierbei um die größte europäische Polizeidatenbank mit mehr als 76 Millionen ausgeschriebenen Personen und Sachen. 2018 wurden neue Regeln zur Stärkung des Schengener Informationssystems vereinbart. Die Datenbank ermöglicht es nationalen Polizei- und Grenzschutzbeamten, Meldungen über gesuchte oder vermisste Personen sowie verlorene oder gestohlene Gegenstände einzugeben und in der täglichen Polizeiarbeit abzufragen.

Weitere, hier nur zu nennende neue EU-weite Datenbanken zur Verstärkung des Informationsaustauschs der Strafverfolgungsbehörden sind

(1) VISA-Informationssystem,
(2) Eurodac[2],
(3) (zukünftig) Entry-/Exit-System (sog. EES) und das
(4) (zukünftig) ETIAS[3].

Und, meine Damen und Herren, nicht unerwähnt lassen möchte ich schließlich eine der vermutlich größten Herausforderungen in unserer nahen Zukunft: ein Austritt des Vereinten Königreiches ohne Austrittsabkommen – der „Brexit“. Großbritannien ist für Europol und die EU-Mitgliedstaaten der größte Datenanlieferer im Bereich Terrorismus. Der Brexit ohne Austrittsabkommen bedeutet den Verlust von Informationen, die für die gesamte EU von Bedeutung sind. Sollte Großbritannien -möglicherweise ab 31. Oktober 2019- Drittstaat werden, bestünde bei einem Austritt ohne Austrittsabkommen kein Zugriff mehr auf die EU-Systeme (u. a. nicht auf Europol- und Schengener Informationssystem), erfolgt keine Einspeisung von operativen Daten in EU-Datensysteme und keine Zusammenarbeit mehr mit Europol. Das akute Problem: Großbritannien will kein Schengen-Assoziierungsabkommen abschließen, so dass lediglich der INTERPOL-Kanal verbleibt, der jedoch den bisherigen Informationsaustausch nicht abdecken wird.

Meine Damen und Herren, ich möchte zum Schluss meines Vortrages, basierend auf den vorangegangenen Ausführungen, einige Thesen, auch für die nachfolgende Diskussion aufstellen:

1. Die Gewährleistung der Inneren Sicherheit Deutschlands ist und bleibt die vorrangige Aufgabe der deutschen Sicherheitsbehörden.

[2] Eurodac - ist ein Fingerabdruck-Identifizierungssystem für den Abgleich der Fingerabdruckdaten aller Asylbewerber sowie von bestimmten Drittstaatsangehörigen und Staatenlosen, wenn die betreffenden Personen älter als 14 Jahre sind.
[3] ETIAS - EU Travel Information and Authorisation System; EU-weites Reiseinformations- und Genehmigungssystem.

2. Bedrohungen der Inneren Sicherheit Deutschlands sind stärker als jemals zuvor durch äußere Einflüsse generiert oder verstärkt (internationalisiert).

3. Die Bekämpfung der Bedrohungen der Inneren Sicherheit Deutschlands erfordert zunehmende und insbesondere zeitnahe Kooperationen verantwortlicher Stellen deutschlandweit und vor allem international.

In diesem Sinne sollte es uns möglich sein, auf die aktuellen und künftigen Herausforderungen im Bereich der Inneren Sicherheit effektiv und kurzfristig zu reagieren und nach Möglichkeit schwerwiegende negative Auswirkungen zu minimieren. Es gilt also auch hier der Ausspruch des Carl von Clausewitz:

„Unvorhergesehene Gelegenheiten sind unverzüglich zu nutzen, und auf unvorhergesehene Schwierigkeiten ist sofort zu reagieren."

Ich danke für Ihre Aufmerksamkeit.

Zum Referenten:

Minister Holger Stahlknecht ist Minister für Inneres und Sport des Landes Sachsen-Anhalt