15. Symposium des

Bundesamtes für Verfassungsschutz

14. Mai 2018, Berlin

„Hybride Bedrohungen – Vernetzte Antworten“

Dr. Hans-Georg Maaßen

Präsident

Bundesamt für Verfassungsschutz

Es gilt das gesprochene Wort!

[Begrüßung]

Meine sehr geehrten Damen und Herren,

ich möchte Sie herzlich willkommen heißen zum 15. Symposium des Bundesverfassungsschutzes.

„Hybride Bedrohungen – Vernetzte Antworten“ – so lautet dieses Jahr unsere Überschrift.

Mit Blick auf die anwesenden Gäste stelle ich mit Freude fest, dass es uns auch dieses Jahr gelungen ist, viele kompetente Partner aus dem In- und Ausland zu versammeln. Die Vielfalt unserer Gästeliste spiegelt damit die Vernetzung wider, die es braucht, um die richtigen Antworten auf die Bedrohungen für unsere Sicherheit zu finden.

Und so begrüße ich herzlich *Sir Julian King*: Als EU-Kommissar für die Sicherheitsunion bemühen Sie sich um die europäische Vernetzung nationaler Sicherheitsstrategien. Die Europäische Kommission hat in den vergangenen Jahren zahlreiche Schritte

unternommen, um hybriden Bedrohungen zu begegnen. Ich möchte insbesondere das Maßnahmenpaket aus dem Jahr 2016 erwähnen, mit dem die Europäische Kommission und die Vertreterin der Union für Außen- und Sicherheitspolitik 22 konkrete Vorschläge zur Abwehr hybrider Bedrohungen unterbreiteten. Ich danke Ihnen, lieber *Julian King*, für Ihr Kommen.

Die Streitkräfte sind enge Partner bei der Abwehr hybrider Bedrohungen. Die NATO hat sich dieses Themas im Zusammenhang mit der Ukraine-Krise angenommen und auf ihrem Gipfel in Warschau im Juli 2016 wichtige Maßnahmen zur Abwehr hybrider Bedrohungen vereinbart. Zugleich ist bei diesem Gipfel eine Erklärung über eine engere Zusammenarbeit mit der EU in diesem Themenbereich unterzeichnet worden. Ich freue mich, den NATO Assistant Secretary General for Intelligence and Security, Herrn *Arndt Freiherr Freytag von Loringhoven*, hier zu begrüßen. Herzlich willkommen!

Der Direktor des M I 5, *Andrew Parker*, wollte im vergangenen Jahr bereits auf unserem Symposium zu uns sprechen, er musste aber leider kurzfristig absagen. Wir erinnern uns: wenige Tage vor dem letztjährigen Symposium, am 22. Mai 2017, hatte ein islamistischer Terrorist in Manchester nach einem Popkonzert bei einem Selbstmordanschlag 22 Menschen getötet und über 500 Menschen verletzt. Es war der schwerste Terroranschlag im Vereinigten Königreich seit Juli 2005. Andrew Parker sagte mir, nein, er versprach mir, dass er auf jeden Fall in diesem Jahr zu unserem Symposium kommen wolle. Er hat sein Versprechen eingehalten und ich freue mich besonders, Dich hier begrüßen zu dürfen. Deine Anwesenheit möchte ich ausdrücklich als Beleg für die vertrauensvolle Zusammenarbeit der europäischen Nachrichtendienste verstanden wissen, die auch vom Brexit unberührt bleiben soll.

Ausdruck der vertrauensvollen europäischen Zusammenarbeit ist auch die Tatsache, dass viele Leiter, stellvertretenden Leiter und Mitarbeiter sowie Verbindungsbeamten unserer europäischen

Partnerdienste, der Direktor für Sicherheit der Europäischen Kommission, Herr *Ilkka Salmi*, sowie der Direktor des EU-Zentrums für Informationsgewinnung und -analyse des Europäischen Auswärtigen Dienstes (kurz: IntCen), Herr *Gerhard Conrad*, zu uns gekommen sind. Ich freue mich, dass Sie heute dabei sind. Ich mchte an dieser Stelle nicht unerwähnt lassen, dass die EU eine Analyseeinheit für hybride Bedrohungen geschaffen hat (die sog. „EU Hybrid Fusion Cell“) die Teil des von Herrn Conrad geleiteten IntCen ist.

Besonders begrüßen möchte ich auch Herrn Parlamentarischer Staatssekretär *Mayer*, die zahlreich erschienen Abgeordneten aus dem Deutschen Bundestag, die Kollegen aus den anderen Bundessicherheitsbehörden sowie die zahlreich erschienenen Leiter und stellvertretenden Leiter der Landesämter für Verfassungsschutz. Und schließlich möchte ich mit einem ganz besonderen Dank für ihr Kommen die weiteren Teilnehmer unseres Symposiums begrüßen.

Ich freue mich, dass Sie alle durch Ihre Präsenz und Ihre Expertise unser Symposium bereichern werden – herzlich willkommen in Berlin!

Meine sehr geehrten Damen und Herren,
ich bin in den vergangenen Wochen wiederholt danach gefragt worden, warum das BfV erstmals nach mehreren Jahren kein Symposium zum Thema „Islamistischer Terrorismus“ durchführt. Man fragte mich, ob man daraus schlussfolgern könne, dass die Bedrohung durch den islamistischen Terrorismus nachgelassen habe. Auf diese Frage habe ich folgendes geantwortet: die Bedrohung durch den islamistischen Terrorismus hat nicht nachgelassen, sie ist weiterhin hoch, und wir müssen weiterhin jederzeit mit terroristischen Anschlägen rechnen. Ob in Manchester, in Brüssel, in Berlin oder anderswo.

Am vergangenen Samstag war anderswo in Paris. Dieser Anschlag führte uns deutlich vor Augen, dass Anschläge jederzeit in Westeuropa stattfinden können. Und er machte wieder einmal

deutlich, dass auch das Ende des IS in Syrien und im Irak nicht das Ende des islamistischen Terrorismus ist. Der IS existiert in anderen Regionen weiter, ebenso Al-Qaida, die extremistischen Salafisten sind mitten unter uns und die islamistisch-jihadistische Ideologie wird weiterverbreitet und trifft nach wie vor auf Menschen, die für diese Ideologie empfänglich sind. Die islamistischen Anschläge der letzten drei Jahre in Europa machen deutlich, dass die europäischen Sicherheitsbehörden mit aller Kraft versuchen müssen, die potentiellen Einzelattentäter, die in unseren Städten leben und sich radikalisieren, zu identifizieren und rechtzeitig zu verhindern, dass es zu einem Terroranschlag kommt. Aber die Sicherheitsbehörden können es nicht alleine. Das Entstehen von islamistischem Extremismus in der Gesellschaft muss verhindert werden, und das ist eine politische und gesamtgesellschaftliche Aufgabe. Um Anschläge verhindern zu können müssen die Sicherheitsbehörden in Europa die notwendigen Mittel und Werkzeuge erhalten, um extremistische Personen frühzeitig zu identifizieren und von ihrem terroristischen Handeln abzuhalten. Ich weiß, dass ich mich mit solchen

Wünschen wiederhole, dass das bei manchem Unbehagen hervorruft, aber in meiner Funktion muss ich das sagen.

Meine sehr geehrten Damen und Herren,

ein Terroranschlag mit Toten und Verletzten führt mit drastischen Bildern die Vulnerabilität unserer freiheitlichen Demokratien vor Augen. Er macht aber auch deutlich, wie wichtig es ist, gemeinsam dagegen zu kämpfen. Gemeinsam als Gesellschaft, aber auch gemeinsam mit unseren Freunden und Partnern. Aber, und jetzt nähere ich mich dem Thema, es gibt auch andere gefährliche Bedrohungen für unsere freiheitlichen Demokratien, ich würde sogar so weit gehen zu sagen: existenzgefährdende Bedrohungen für unsere Demokratien und für die Europäische Union als Ganzes. Bedrohungen, die nicht mit so drastischen Bildern einhergehen, Bedrohungen, die wir als solche nicht wahrnehmen, weil wir sie nicht kennen oder weil wir nicht wissen, dass es sie gibt. Wir sehen nicht den unmittelbaren Zusammenhang zwischen der Bedrohung und dem Tod von Menschen. Es gibt keine Bekennerschreiben. Es soll keine Bekennerschreiben geben. Es soll niemand wissen, dass

es diese Angriffe überhaupt gibt und es soll niemand wissen, wer hinter diesen Angriffen auf unsere freiheitliche Demokratie steht.

[Was sind hybride Bedrohungen]

Und damit bin ich bei „Hybriden Bedrohungen“. Den Begriff könnte ich von den Zielen, von der verwendeten Methodik, den Techniken und Instrumenten her definieren. Weil ich aber nicht in einer universitären Vorlesung bin, möchte ich einmal untechnisch formulieren, nämlich dass wir bei hybriden Bedrohungen

- von der gezielten Einflussnahme auf einen anderen Staat
- unterhalb eines offenen militärischen Konflikts oder in Ergänzung militärischer Maßnahmen
- durch eine Mischung von offenen und verdeckten geheimdienstlichen, militärischen und nicht-militärischen Handlungsweisen sprechen.

Methodisch kombinieren hybride Bedrohungen mehrere Bausteine, die einzeln betrachtet vergleichsweise harmlos erscheinen, in ihrer Summe aber beträchtliche Schäden anrichten können. Der

Aggressor möchte nicht als klar erkennbare Konfliktpartei in Erscheinung treten – Stichwort *„Abstreitbarkeit“.* Durch die Kombination von zivilen und militärischen Mitteln operiert er mit Tarnkappe, um gezielt seine Verantwortlichkeit zu vernebeln und Gegenmaßnahmen zu unterlaufen. Seine Motive sollen – wenn überhaupt – erst dann deutlich werden, wenn es zu spät ist!

Dabei müssen wir uns darüber im Klaren sein, dass derartige Einflussnahmen keinen Selbstzweck haben. Es geht letztlich um das Verändern von politischen Machtverhältnissen zwischen Staaten.

Zur Erreichung eines bestimmten politischen oder militärischen Ziels, nämlich einen anderen Staat zu einem bestimmten Verhalten zu veranlassen, und sei es nur, dass er z. B. wegen Bürgerkriegs als außenpolitischer Akteur ausfällt, kann eine Vielzahl von Methoden, Techniken und Instrumenten von unterschiedlichen Akteuren konzertiert eingesetzt werden. Teilweise sind die Techniken getarnt, teilweise offen, ohne dass der Urheber in Erscheinung tritt, teilweise auch gewalttätig, wie bei der Aufwiegelung zu gewalttätigen Demonstrationen oder der

Durchführung von Attentaten. Nicht immer werden die Maßnahmen von staatlichen Stellen selbst durchgeführt oder initiiert. Operateure können neben staatlichen Stellen, also vor allem ausländischen Geheimdiensten, auch Gruppierungen sein, die ermutigt, angestiftet oder unterstützt werden, um bestimmte Operationen durchzuführen; z. B. fanatisierte politische Unterstützer, Kriminelle oder Hacker, die sich in den Dienst einer hybriden Operation stellen. In diesen Fällen könnte man von einer hybriden Guerilla sprechen.

Es gibt unterschiedliche Methoden und Techniken, um die Politik eines anderen Staates subtil zu beeinflussen: z. B.

- die direkte Einflussnahme auf politische Entscheider, durch Bestechung, Erpressung oder durch die Diskreditierung von Personen oder sogar durch Attentate auf Führungspersonen.
- die Destabilisierung eines Staates, die Demoralisierung von Verwaltung und Militär, die Verunsicherung der Bevölkerung und das Untergraben des Vertrauens der Bevölkerung in Staat und Regierung. Hierzu werden als Techniken Propaganda,

Desinformation und psychologische Operationen, das Verbreiten von Verschwörungstheorien, die Unterstützung bzw. Finanzierung von Terroristen, Extremisten, von Separatisten oder Unzufriedenen oder die Sabotage an kritischer Infrastruktur eingesetzt. Die Platzierung von Einflussagenten in Politik, Medien, gesellschaftlichen Gruppen ist dazu ein wirkungsvolles Instrument.

[Hybride Bedrohungen gestern und heute]

Meine sehr geehrten Damen und Herren,

vielleicht denken Sie bei meiner kurzen Aufzählung der möglichen Methoden und Techniken zur Einflussnahme, dass manches altbekannt ist. Ich persönlich bin ja der Meinung, dass nicht alles, was mit einem neuen Namen versehen wird, wirklich neu sein muss. Oftmals ist die Kernidee alt oder von jemand anderem vorgedacht, es ist vielleicht wiederentdeckt oder es kommt mit einer neuen Verpackung daher. Und so ist es auch hier: Viele Elemente der hybriden Bedrohungen sind nicht wirklich neu.

Weil unsere britischen Freunde heute anwesend sind, erlaube ich mir in diesem Zusammenhang an unsere gemeinsame Geschichte zu erinnern. Im Ersten Weltkrieg waren hybride Maßnahmen zur Flankierung der militärischen Operationen ein Schwerpunkt der geheimdienstlichen Operationen auf beiden Seiten. Der deutsche Geheimdienst hatte ab 1916 irische Separatisten und indische Nationalisten unterstützt. Wie ich dem Buch von *Christopher Andrew* über die Geschichte des M I 5 entnommen habe, war die Bekämpfung der deutschen Subversion ein Schwerpunkt der damaligen Arbeit des M I 5. Vielleicht haben in dieser Zeit die deutschen Nachrichtendienste sogar die größte und erfolgreichste oder - vorsichtiger formuliert - folgenreichste hybride Operation aller Zeiten durchgeführt: Nämlich die von der Abteilung IIIb des Großen Generalstabs der deutschen Armee (das war damals der Nachrichtendienst) und vom Auswärtigen Amt eingefädelte Rückkehr *Lenins* in einem verplombten Zug nach Russland, um das zaristische Russland aus der Allianz mit den Westmächten herauszubrechen und um zu einem Separatfrieden mit den

Bolschiwiki zu kommen. Beides gelang schließlich mit dem Friedensvertrag von Brest-Litowsk im März 1918. Aber es half nicht wirklich. Die Briten hatten den Krieg trotzdem gewonnen. Ich glaube, wenn ich an die britischen Propagandamaßnahmen aus der Zeit denke, wir hatten uns damals wenig geschenkt.

Auch die Verwendung von Einflussagenten in Politik und Medien ist nicht neu. In Erinnerung zu rufen sind die sog. Aktiven Maßnahmen der Abteilung X der HV A der DDR-Staatssicherheit. Zu diesen Maßnahmen zählte z. B. das Anwerben, Bestechen oder Diskreditieren von Politikern und Journalisten.

Was ist also neu an den hybriden Bedrohungen?

Aus meiner Sicht sind drei Punkte neu. Und jeder dieser Punkte rechtfertigt es, dass wir uns besonders dieser Bedrohung widmen:

1. Wir sind geprägt durch die Zeit nach Ende des Kalten Krieges. Bedrohungen, die wir heute hybrid nennen, waren – wie soeben erwähnt – in Kriegszeiten und in der Zeit des Kalten Krieges im Wesentlichen bekannt und die Menschen waren

sensibilisiert. Nach 1990 ist man in Europa vielfach davon ausgegangen, die schlimmsten Kapitel der europäischen Geschichte hinter sich gelassen zu haben und eine Zukunft von Frieden und Partnerschaft vor sich zu haben. Wir müssen zur Kenntnis nehmen, dass sich diese idealistischen Vorstellungen so nicht realisiert haben. Wir sind in Teilen überrascht, dass andere Staaten, die Methoden hybrider Operationen oder sog. aktiver Maßnahmen, die sie zur Zeit des Kalten Krieges anwandten, auch heute noch beherrschen und anwenden. Die Sicherheitslage hat sich in den letzten Jahren insoweit deutlich verändert. Es bedarf deshalb ein Mehr an Sensibilisierung der Öffentlichkeit und ein Mehr an eigenem Schutz vor diesen Maßnahmen.

2. Mit dem Cyberraum ist neben die Realwelt ein neuer Aktionsraum hinzugetreten. All die Maßnahmen, die in der Realwelt als hybride Operationen durchgeführt werden können, können noch einfacher und, ggf. auch ohne Spuren zu hinterlassen, im Cyberraum durchgeführt werden. Anders als früher, muss man heute nicht mehr Propagandaflugblätter

hinter den feindlichen Linien abwerfen oder Einflussagenten in Redaktionen platzieren, weil es möglich ist, z. B. über soziale Netzwerke gezielte Falschinformationen zu streuen und durch APT-Angriffe gegnerische Netze lahmzulegen. Nahezu jeder einzelne Bürger kann durch den Cyberraum als Opfer von Propaganda und Desinformation erreicht werden und viele Bereiche kritischer Infrastruktur können sabotiert werden.

3. Wir sind verwundbarer. Unsere Angriffsfläche ist größer geworden. Zum einen durch den Cyberraum, der alles mit allem vernetzt, und wodurch die Risiken des Cyberraums auch zu Risiken der Realwelt werden, ob beim Schutz kritischer Infrastrukturen oder bei Wahlen. Der Bürger in freiheitlichen Demokratien braucht verlässliche Informationen, um Wahlentscheidungen zu treffen. Er braucht eine zutreffende und breite Tatsachengrundlage. Auf Grund dieser Tatsachen kann man zu unterschiedlichen Bewertungen und politischen Meinungen kommen. Es kann alternative Meinungen und Bewertungen geben, aber nur eine Realität und es können neben ihr keine alternativen Realitäten oder Tatsachen

existieren. Wenn aber durch hybride Aktionen falsche Tatsachen verbreitet, Tatsachen manipuliert, Tatsachen unterdrückt oder aus bloßen Meinungen Tatsachen und aus Tatsachen Meinungen konstruiert werden, verliert der Bürger die verlässliche Grundlage auf der er seine politischen Entscheidungen treffen kann. Eine Demokratie ist darauf angewiesen, dass der Bürger Zugang zu vollständigen und wahren Tatsachen erhält, damit er hieraus für sich eine politische Entscheidung treffen kann.

Desinformation mag im Einzelfall plump daherkommen – aber auf Dauer vergiftet sie den freiheitlichen Diskurs der pluralistischen Demokratie. Offene Gesellschaften vertragen viele Meinungen, aber nicht viele Wahrheiten! Diesen Umstand machen sich hybride Kampagnen zunutze, denn sie wollen die Wahrnehmung des Opfers paralysieren, seine Willensstärke unterminieren und am Ende seine Wehrhaftigkeit zersetzen.

Bekanntlich braucht die offene, demokratische Gesellschaft Raum für die gleichberechtigte Diskussion. Und sie braucht Zeit zur

Prüfung aller Sachverhalte, Fakten und Standpunkte. Genau dieses Zeitfenster will hybride Aggression nutzen, um im Nebel der Desinformation Fakten zu schaffen.

Hybride Bedrohungen sind deshalb heute anders als sie es vor Jahrzehnten waren; sowohl qualitativ als auch hinsichtlich der schieren quantitativen Möglichkeiten.

[Aktuelle Bedrohungssituation]

Meine sehr geehrten Damen und Herren,
als Realisten müssen wir einfach zur Kenntnis nehmen, dass es für andere Staaten attraktiv ist, die Möglichkeiten der hybriden Angriffe jetzt und jederzeit zu nutzen, um eigene Interessen durchzusetzen und um deutschen und europäischen Interessen zu schaden. Die Möglichkeiten und Gelegenheiten sind einfach zu günstig. Und es wäre auch naiv zu glauben, dass der Staat der die Möglichkeiten und die entsprechenden politischen Interessen hat, darauf verzichtet.

Hybride Maßnahmen haben sich nicht in den Cyberraum verlagert. Sie erfolgen sowohl in der Realwelt als auch in der Cyberwelt. Der Cyberraum ist hinzugetreten, er ergänzt nicht die bisherigen Möglichkeiten unseres Gegenübers in der Realwelt, aber er ersetzt sie nicht.

Ziel von Hybriden Bedrohungen sind nicht nur Nationalstaaten, sondern auch die Europäische Union als Global Player. Mit Blick auf die Europäische Union müssen wir auch mögliche Interessenlagen anderer Mächte berücksichtigen, wonach z. B. eine schwache und zerstrittene Europäische Union aus dortiger Sicht vorteilhafter sein könnte als eine starke EU. Eine schwache EU, die auf sich selbst fixiert ist und mit vielen inneren Problemen zu kämpfen hat, kann im Zweifel nicht mehr die weltpolitische Rolle einnehmen, die sie einnehmen sollte. Dies dürfte für manche Mächte durchaus wünschenswert sein. Wir dürfen uns hier nichts vormachen.

In Deutschland haben wir in den vergangenen Jahren wiederholt hybride Angriffe anderer Staaten feststellen müssen. Im Mittelpunkt standen Propaganda und Desinformationen,

Einflussnahmeversuche, aber auch der Einsatz von Cyberwaffen zur möglichen Vorbereitung von Sabotageakten. Der Verfassungsschutz hat wiederholt festgestellt, dass Mitarbeiter von Politikern, von Parteien oder von politischen Stiftungen von ausländischen Nachrichtendiensten angesprochen wurden, um über diese Personen Einfluss auf Entscheidungsträger auszuüben. Ebenso konnten wir Ausspähungen durch ausländische Nachrichtendienste oder Diskreditierungsversuche feststellen. Da wir es bei hybriden Maßnahmen regelmäßig mit geheimen Operationen zu tun haben, ist uns naturgemäß vieles unbekannt und kann von uns als solche nicht aufgeklärt werden. Dies gilt insbesondere für die mir immer wieder gestellte Frage nach der finanziellen Unterstützung radikaler politischer Gruppierungen in Deutschland durch ausländische Stellen. Wir müssen jedenfalls realistischerweise von einer sehr aktiven hybriden Bedrohungssituation für Deutschland ausgehen.

Ein Informationsaustausch mit europäischen Partnern macht deutlich, dass dort ähnliche Erfahrungen gemacht werden, dass

insbesondere von Russland versucht wird, durch geheime Operationen Einfluss zu nehmen auf die öffentliche Meinungsbildung, dass radikale oder extremistische Organisationen insbesondere durch Finanzzuwendungen gestärkt werden oder dass – wie auch berichtet wird – im Falle der katalanischen Separatisten deren Position durch Propagandamaßnahmen unterstützt wird.

Meine sehr geehrten Damen und Herren,

eine zentrale Rolle stellen bei hybriden Maßnahmen Cyberoperationen, insbesondere Cyberangriffe dar. Cyberangriffe sind zum Standardwerkzeug zahlreicher Nachrichtendienste geworden – wodurch sich eine fatale Aufrüstungsspirale ergeben kann. Dieser kostengünstige, asymmetrische Hebel ist für Herausforderer der gegenwärtigen Weltordnung sowie für Staaten mit geringen Kapazitäten gleichermaßen attraktiv.

Dass gerade Cyberspionage nicht nur attraktiv, sondern auch lukrativ ist, belegt der hohe Aufwand, der sich hinter den oftmals hochkomplexen Kampagnen verbirgt. Dies hat zwei Gründe: Zum einen hat Cyberspionage durch die informationstechnologische Vernetzung eine internationale Dimension. Dadurch kann Cyberspionage im Idealfall viele Opfersysteme abschöpfen – weil es nun die eine, digitale Weltsprache gibt.

Zum anderen können die ausgespähten Daten – auch für hybride Kampagnen – multifunktionale Verwendung finden: Sie können zum Ausforschen von Zielpersonen (z: B. um eine Diskreditierungskampagne mit Kompromaten vorzubereiten) nutzbar gemacht werden, aber auch zur Sabotage oder zur politischen Einflussnahme.

Ein Musterbeispiel dafür ist die Cyberangriffskampagne *APT 28*: Sie stellt einen Arbeitsschwerpunkt der Cyberabwehr des Bundesamtes für Verfassungsschutz dar, weil sie als langjährige, internationale Angriffsoperation auch gegen deutsche Ziele aktiv ist. Aufgrund der bisherigen Opferauswahl, dem dahinter

stehenden Aufklärungsinteresse, durch Analysen der technischen Parameter und durch Aufklärung im *Humint*-Bereich gehen wir von einer Steuerung durch russische staatliche Stellen aus.

Wir schreiben ihr den Cyberangriff auf den Deutschen Bundestag im Frühjahr 2015 sowie erneute Spear-Phishing-Angriffswellen auf das Parlament und politische Parteien im Frühjahr und Sommer 2016 zu. Auch 2017 erlangten wir Kenntnis von Angriffen auf politische Parteien und Stiftungen in Deutschland, die technische Rückschlüsse auf *APT 28* zuließen.

APT 28 wird nicht nur für Spionage-, sondern auch für Einflussoperationen eingesetzt – wie zum Beispiel im Rahmen einer *False-Flag*-Operation im April 2015 gegen den französischen Fernsehsender *TV5 Monde*, bei der nur scheinbar islamistische Hacker dem Sender einen Millionenschaden zufügten und IS-Propaganda verbreiteten. Die nachträgliche Analyse verwies jedoch auf *APT 28* als Urheber.

Ebenso beim Mitte Juni 2016 bekannt gewordenen erfolgreichen Cyberangriff auf das Netzwerk des Democratic National Committee (DNC) in den Vereinigten Staaten. Dieser Angriff erzielte unter dem Aspekt der Einflussnahme auf den US-amerikanischen Präsidentschaftswahlkampf große Bedeutung, denn er ist ein Beispiel für sogenannte *Hack-and-Leak-Operationen*: Nach dem Hack erfolgten Veröffentlichungen von über 19.000 internen E-Mails aus dem DNC, die große Kontroversen auslösten und nicht nur die damalige Präsidentschaftskandidatin der Demokraten unter Druck setzten, sondern die US-Administration bis heute beschäftigten.

Auch der Wahlkampf des französischen Präsidentschaftskandidaten Emmanuel Macron ist bekanntlich 2017 von einer *Hack-and-Leak-Operation* überschattet worden.

Vor diesem Hintergrund setzte das Bundesamt für Verfassungsschutz vor der Bundestagswahl 2017 eine speziell eingerichtete Taskforce ein. Wir mussten davon ausgehen, dass

auch der erkannte Datenabfluss von 16 Gigabyte aus dem Bundestag als potentielles Mittel zur unlauteren Einflussnahme genutzt werden könnte. Wir intensivierten die Beobachtung relevanter Cyberoperationen sowie das Monitoring deutschsprachiger Kanäle russischer Medien in der Real- und Cyberwelt.

Es wäre nicht das erste Mal gewesen, dass wir zur Zielscheibe von Desinformationskampagnen geworden wären: Erinnern Sie sich an das Beispiel der angeblichen Entführung und Vergewaltigung einer 13-Jährigen – dem sogenannten „Fall Lisa“ aus dem Jahr 2016.

[Maßnahmen]

Meine sehr geehrten Damen und Herren,

was ist zu tun? Ich denke nicht, dass wir diesen Bedrohungen schutzlos ausgeliefert sind.

Prävention beginnt dem Bewusstmachen der Bedrohung. Mit Blick auf Desinformation und Propaganda stehen Maßnahmen der Sensibilisierung, der Öffentlichkeitsarbeit und der Erarbeitung von

Gegenbotschaften im Vordergrund. Desinformation kann nur Erfolg haben, wenn sie nicht als solche erkannt wird und wenn man sich von ihr irreführen und verunsichern lässt. Den Medien kommt in der Abwehr von Desinformation eine herausragende Rolle zu. Die Menschen brauchen verlässliche Informationen. Sie müssen sich darauf verlassen, dass das, was sie in Zeitungen lesen und im Fernsehen sehen und hören, verlässlich ist, und dass es sorgfältig geprüft ist. Dies ist in Zeiten, in denen Redaktionen verkleinert werden und die Medienlandschaft im Umbruch ist, mehr als eine Selbstverständlichkeit. Es ist eine Herausforderung. Prävention bedeutet auch, dass der Konsument von Informationen, also jeder Bürger wachsamer und kritischer sein muss.

Im Vorfeld der Bundestagswahl gab es in Deutschland eine breite öffentliche Diskussion darüber, ob es vergleichbar der russischen Einflusskampagne bei den amerikanischen Präsidentschaftswahlen eine derartige Kampagne auch bei der Bundestagswahl geben könne. Ich denke, dass allein diese öffentliche Diskussion schon hilfreich war, nicht nur um die notwendige Sensibilität in der Gesellschaft herzustellen, sondern

auch um unserem Gegenüber deutlich zu machen, dass wir wachsam sind.

[Vernetzung]

In Zeiten hybrider Konflikte funktioniert Sicherheit nicht mehr als strenge Arbeitsteilung monolithischer Blöcke – mit dem Militär und den Sicherheitsbehörden auf der einen und der Zivilgesellschaft auf der anderen Seite. In einer vernetzten Gesellschaft tragen alle Verantwortung. Politik, Wirtschaft, Forschung und Verwaltung sind jetzt auch Sensoren des einen vernetzten Sicherheitssystems. Sie können als Plattform kommunizieren und gemeinsam mit den Sicherheitsbehörden interagieren.

In diesem tiefgestaffelten Netzwerk spielen Nachrichtendienste eine wichtige Rolle. Wir sind es gewohnt, nationale wie internationale Sicherheitsallianzen zu knüpfen und sensible Informationen zu vernetzen.

Unser Auftrag ist die Gewinnung und Auswertung von Informationen, um Bedrohungen frühzeitig zu erkennen und um

Lagebilder zu schaffen. In Zeiten hybrider Bedrohungen ist diese Arbeit mehr denn je notwendig.

Als nationale Spionagewehrbehörde ist es seit jeher Aufgabe des Bundesverfassungsschutzes, in der Realwelt wie im Cyberraum Angriffe nachrichtendienstlicher Strukturen frühzeitig zu erkennen, deren Gefährdungspotenzial zu bewerten und gezielte Abwehr- und Sensibilisierungsmaßnahmen zu initiieren.

Mit einer 360-Grad-Perspektive stellen wir uns dem verstärkten Aufkommen von gesteuerten und hochkomplexen Angriffen, investieren Ressourcen und Personal, konzentrieren Know-how an den neuralgischen Stellen und arbeiten mit nationalen wie internationalen Partnern zusammen. Dadurch gelingt es uns, die fachliche und technische Expertise zur Abwehr staatlich gesteuerter Cyberangriffe stetig zu erweitern.

Wir sind täglich bestrebt, die Gefahren „digitaler Proliferation“ auf dem Radar zu halten! Die Entwendung und anschließende Verbreitung von „waffenfähigem IT-Wissen“ wird in Zukunft eine große Herausforderung für unsere Abwehrdienste darstellen. Wir geben unsere Erkenntnisse über erkannte Schadcodes an die

Öffentlichkeit weiter und sensibilisieren Wirtschaft und Wissenschaft über feindliche Spionagetechniken oder Proliferationsversuche. Und wir beobachten und analysieren verfassungsfeindliche, extremistische Strömungen – auch dadurch können wir unlauteren Mobilisierungsversuchen durch externe Akteure besser begegnen!

Der Bundesnachrichtendienst und die Bundeswehr, dort vor allem das Kommando Cyber- und Informationsraum, sind in dieser nationalen Abwehr gegen hybride Bedrohungen wichtige Partner.
Aber auch eine enge europäische Zusammenarbeit ist wichtig. Ich hatte bereits gesagt, dass es auch um die Stabilität der Europäischen Union und um ihre Rolle als Global Player geht. Es bedarf auf europäischer Ebene einerseits eines engen Informationsaustauschs über Bedrohungen und andererseits auch gemeinsamer Maßnahmen zur Abwehr hybrider Bedrohungen. Die Europäische Union hat im Jahr 2016 ein 22 Punkte umfassendes Maßnahmenpaket zur Abwehr von hybriden Bedrohungen verabschiedet. Aus unserer Sicht ein wichtiger Schritt. Hierzu

zählte auch die Einrichtung des European Center of Excellence for Countering Hybrid Threats in Helsinki, das eine Art Forschungseinrichtung zur Aufklärung hybrider Bedrohungen ist. Diese Stelle, in der Deutschland auch vertreten ist, hat inzwischen ihren Arbeitsbetrieb aufgenommen. Eine weitere Einheit, die den innereuropäischen Informationsaustausch erleichtern soll, ist die beim IntCen eingerichtete EU-Analyseeinheit für hybride Bedrohungen.

[Schluss]

Meine sehr geehrten Damen und Herren,
ich möchte zum Schluss kommen und feststellen:

- Hybride Angriffskampagnen zielen auf die Schwachstellen und Bruchlinien offener Gesellschaften.

- Sie bedienen sich heute mit Vorliebe den Möglichkeiten digitaler Technologien, um ihre Opfer zu überrumpeln, ohne dass aber die hybriden Bedrohungen in der Realwelt abnehmen. Hackerangriffe werden leider immer häufiger Teil der Außenpolitik.

- Sie profitieren dabei von technischen Schlupflöchern und dem freiheitlichen Pluralismus der Demokratie, die sich zur Wehr setzen muss, ohne ihre Rechtsstaatlichkeit und Meinungsfreiheit zu gefährden.

Am Ende konfrontieren uns hybride Bedrohungen mit zwei grundsätzlichen Fragen: Wie abwehrbereit ist der Staat? Und wie demokratisch ist der Cyberraum?

Diese Fragen sind heute die Überschriften unserer beiden Diskussionsforen. Ich freue ich mich sehr auf Ihre Beiträge, denn sie sind die demokratischen Antworten einer vernetzten

Gesellschaft, die ihre Freiheit schätzt und gewillt ist, sie zu verteidigen.

Ich danke Ihnen für Ihre Aufmerksamkeit.