Deutscher Bundestag **Drucksache 18/4286**

18. Wahlperiode 11.03.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/4074 –

Kooperationen zur „Cybersicherheit“ mit der Europäischen Union und den Vereinigten Staaten

Vorbemerkung der Fragesteller

Trotz der Enthüllungen über die Spionage von britischen und US-Geheimdiensten in Mitgliedstaaten der Europäischen Union (EU) existieren weiterhin eine Reihe von Kooperationen zur „Cybersicherheit“ zwischen der Bundesregierung, der Europäischen Union und den Vereinigten Staaten (Bundestagsdrucksache 18/164). Schon länger existieren Zusammenarbeitsformen, wie die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ oder ein „EU-/US-Senior-Officials-Treffen“. Zu ihren Aufgaben gehört die Planung gemeinsamer ziviler oder militärischer „Cyberübungen“, in denen „cyberterroristische Anschläge“, über das Internet ausgeführte Angriffe auf kritische Infrastrukturen, „DDoS-Attacken“ sowie „politisch motivierte Cyberangriffe“ simuliert und beantwortet werden. Eine dieser US-Übungen war „Cyberstorm IV“ mit allen US-Behörden des Innern und des Militärs. Ähnliche Manöver werden von der NATO abgehalten, zuletzt eine „Cyber Coalition 2014“. Die EU führte eine „Cyber Europe 2014“ durch.

Vorbemerkung der Bundesregierung

Nummer 7 der Cyber-Sicherheitsstrategie für Deutschland fordert ein „effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit“. Die Bundesregierung beteiligt sich auf EU-Ebene sowie im internationalen Kontext an den wesentlichen Prozessen im Bereich Cyber-Sicherheit und Netzpolitik. Es ist erforderlich, weiterhin international zusammenzuarbeiten, wobei gegenseitiges Vertrauen eine entscheidende Rolle spielt. Art und Maß der internationalen Zusammenarbeit können nicht nur von bestimmten Ereignissen abhängig gemacht werden; sie müssen vielmehr strategisch und langfristig auf der Basis von Austausch, Kennenlernen und Vertrauensaufbau erfolgen. Dazu können konkrete Projekte beitragen, z. B. gemeinsame Übungen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 9. März 2015 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Da für die bei der Bundeswehr angesiedelte Gruppe „Computer-Netzwerk-Operationen“ (CNO) zum „Wirken gegen und in gegnerischen Netzen“ in bewaffneten Konflikten aus Sicht der Bundesregierung kein „Unterscheidungserfordernis analog zur Kennzeichnungspflicht von Kombattanten“ bestehe (Bundestagsdrucksache 18/3963), diese also ihre offensiven oder defensiven Angriffe mit „Tarnungstechniken“ verschleiern darf, auf welche Weise sollen dann die Angegriffenen unterscheiden, welche gegnerische Streitmacht hierfür verantwortlich ist oder ob diese staatlichen oder nichtstaatlichen Ursprungs sind?

Die „Computer-Netzwerk-Operationen“-Kräfte (CNO-Kräfte) der Bundeswehr unterliegen – wie alle Teile der deutschen Streitkräfte – den jeweils anwendbaren Bestimmungen des Völkerrechts, d. h. die Angehörigen der CNO sind in einem internationalen bewaffneten Konflikt als Kombattanten verpflichtet, sich zu unterscheiden (vgl. die Antwort der Bundesregierung zu Frage 23 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/3963 vom 6. Februar 2015). Darüber hinaus gibt es kein völkerrechtliches Verbot der Tarnung. Tarnung dient dem Schutz vor frühzeitiger Entdeckung, um die Wahrscheinlichkeit der Durchsetzung eigener Wirkmittel zu erhöhen. So werden etwa bei Cyber-Tarntechniken die Erfassungsmöglichkeiten durch die Schutzsensorik des gegnerischen Netzes eingeschränkt. Von der zulässigen Tarnung strikt zu unterscheiden ist die unzulässige Nutzung falscher Identitäten mit dem Ziel, eine Zurechnung zu Zivilisten, zivilen Einrichtungen oder anderen geschützten Personen oder Objekten zu provozieren und sie so zum Ziel eines Gegenangriffs zu machen.

   a) Was ist damit gemeint, wenn die Bundesregierung auf die Frage, wie die CNO sicherstellt, dass keine unbeteiligten Personen sowie zivile Infrastruktur durch ihre Cyberangriffe geschädigt würden, antwortet, es würde „nach den grundsätzlich geltenden Regeln zur Vermeidung dieser Schäden wie bei anderen Wirkmitteln verfahren“?

Mit den „grundsätzlich geltenden Regeln“ zum Schutz der Zivilbevölkerung und zur Vermeidung von Kollateralschäden bezieht sich die Bundesregierung auf die humanitär-völkerrechtlichen Regelungen wie sie in Artikel 48 ff. des Zusatzprotokolls I zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte niedergelegt sind sowie die entsprechenden völkergewohnheitsrechtlichen Regelungen.

Neben der eindeutigen Identifizierung des Ziels wird a priori die Gefahr von unerwünschten Begleitschäden abgeschätzt. Dabei werden alle bekannten Umstände zum Zeitpunkt der Entscheidung und die Effekte, die das Wirkmittel erzielen soll, in Beziehung gesetzt. Dabei werden z. B. geographische Gegebenheiten, Wetter, Eigenschutz und Härtung der gegnerischen Objekte, sekundäre Funktionen von Objekten im Hinblick auf zivile Versorgung und mögliche Bewegungen im Raum beachtet. Zudem werden die Positionen ziviler Objekte und Personen berücksichtigt, um Kollateralschäden weitgehend auszuschließen.

   b) Welche „besonderen Aspekte des Cyber-Raums“ werden dabei „berücksichtigt“?

Bei der Beachtung dieser Prinzipien im Cyber-Raum gibt es durch die Charakteristika des Internets Besonderheiten, die beachtet werden müssen. So muss zum Beispiel sichergestellt werden, dass das Vorgehen in seiner Wirkung auf militärische Ziele beschränkt bleibt und nicht im Internet verbundene zivile Netze beliebig beeinträchtigt werden. Es muss vorher abgeschätzt werden, welche Verknüpfungen existieren, um nicht einen so genannten Dominoeffekt oder Kaskadierungseffekt auszulösen.

2. Welche Konferenzen zu „Cybersicherheit“, „Cyberkriminalität“ oder „Cyberterrorismus“, die von einer EU-Institution ausgerichtet wurden, haben nach Kenntnis der Bundesregierung im Jahr 2014 stattgefunden (Bundestagsdrucksache 18/164)?

   a) Welche Tagesordnung bzw. Zielsetzung hatten diese jeweils?

   b) Wer hat diese jeweils organisiert und vorbereitet?

   c) Welche weiteren Nicht-EU-Staaten waren daran mit welcher Zielsetzung beteiligt?

   d) Mit welchen Aufgaben oder Beiträgen waren auch Behörden der USA eingebunden?

   e) Mit welchem Personal waren deutsche öffentliche und private Einrichtungen beteiligt?

Die Bundesregierung hat Kenntnis von folgenden Konferenzen zu „Cyber-Sicherheit“, „Cyberkriminalität“ oder „Cyberterrorismus“, die im Jahr 2014 von EU-Institutionen (i. S. v. Organen, Einrichtungen und Agenturen) ausgerichtet wurden:

– High Level Conference on the EU Cybersecurity Strategy, 28. Februar 2014, Brüssel

  Sie wurde von der Generaldirektion CONNECT der Europäischen Kommission ausgerichtet. Ziel der Konferenz war die Bewertung der Umsetzungsfortschritte der EU-Cyber-Sicherheitsstrategie ein Jahr nach deren Veröffentlichung.

  Soweit bekannt, waren keine Vertreter der USA bzw. aus Nicht-EU-Mitgliedstaaten an der Konferenz beteiligt. Aktive Beiträge seitens deutscher öffentlicher Stellen sowie die Beteiligung privater Einrichtungen sind nicht bekannt.

– Safety & Security in Cyber Space Conference, 6. und 7. März 2014, Athen

  Diese Konferenz wurde von der griechischen Ratspräsidentschaft in Zusammenarbeit mit der Europäischen Kommission und der International Telecommunication Union (ITU) ausgerichtet. Bei der Konferenz wurden folgende Themen diskutiert:

  - Cyber Space and Contemporary Threats,
  - Legal Aspects in Cyber Domain,
  - Trust and Security,
  - Cyber Security,
  - Capabilities Development in Cyber Environment,
  - Network and Information Security – NIS.

  Über die internationale Organisation ITU hatten auch Teilnehmer aus nicht EU-Staaten grundsätzlich die Möglichkeit, an der Konferenz teilzunehmen. Ausweislich der Tagesordnung war kein Vertreter einer US-amerikanischen Behörde aktiv an der Konferenz beteiligt. Eine Teilnehmerliste liegt der Bundesregierung nicht vor, so dass keine Aussagen darüber möglich sind, ob und ggf. welche Nicht- EU-Staaten an der Veranstaltung teilgenommen haben, ob auch Behörden der USA eingebunden waren und ob und ggf. welche deutschen öffentlichen und privaten Einrichtungen an der Veranstaltung teilgenommen haben.

– EU-Financial Cybercrime Coalition (FCC), 5. und 6. Mai 2014, Den Haag

Die Veranstaltung war das erste Treffen der sogenannten EU Financial Cybercrime Coalition (FCC). Die FCC hat sich zum Ziel gesetzt, Vertreter von Strafverfolgungsbehörden sowie des Finanzsektors zusammen zu bringen und die Zusammenarbeit gegen Cybercrime mit Bezug zum Finanzsektor zu verbessern. Die Veranstaltung wurde von Europol organisiert und vorbereitet. Vertreter der Bundesregierung haben nicht an dem Treffen teilgenommen, daher liegen auch keine Informationen zur Teilnahme „deutscher öffentlicher und privater Einrichtungen“ und zur Präsenz von Nicht-EU-Staaten vor.

– The validity and admissibility of electronic evidence in Cybercrime cases, 5. und 6. Juni 2014, Prag

Die Veranstaltung wurde von der Academy of European Law (ERA) und der Tschechischen Republik ausgerichtet. Die Tagesordnung umfasste laut Einladung folgende Punkte:

- Practical challenges relating to the collection and use of electronic evidence when cyber offences are committed,
- Legal implications of electronic evidence (collection, evaluation and admissibility) in criminal proceedings,
- Practical problems that prosecutors and judges have to deal with to prosecute and adjudicate cybercrime cases,
- Legal challenges for the defence,
- Overview of good practices in various EU Member States,
- Electronic evidence in child pornography, online fraud and cyberlaundering cases.

Von Seiten der Bundesregierung nahm niemand an der Konferenz teil. Ausweislich der Einladung waren von deutscher Seite Vertreterinnen und Vertreter der Staatsanwaltschaft Freiburg sowie des Max-Planck-Instituts für ausländisches und internationales Strafrecht an der Konferenz beteiligt.

Der Bundesregierung liegen keine Erkenntnisse vor, ob und ggf. welche Nicht-EU-Staaten an der Veranstaltung teilgenommen haben und ob und ggf. welche Aufgaben oder Beiträge seitens der USA übernommen wurden.

– Law Enforcement Day at ICANN, 23. Juni 2014, London

Der Law Enforcement Day läuft regelmäßig parallel zu den mehrmals jährlich stattfindenden ICANN-Meetings. Beim Law Enforcement Day im Juni 2014 wurden neben dem neuen WHOIS-System auch der ICANN-Compliance-Prozess und die Frage nach der Einrichtung einer Arbeitsgruppe aus Vertretern der Strafverfolgung bei ICANN erörtert. Die Veranstaltung wurde von Europol, Interpol und dem Federal Bureau of Investigation (FBI) organisiert. Eine Teilnehmerliste liegt der Bundesregierung nicht vor, so dass keine Aussagen darüber getroffen werden können, wer von deutscher Seite teilgenommen hat und welche Nicht-EU-Mitgliedstaaten an der Veranstaltung beteiligt waren. Seitens der USA war das FBI als Mit-Organisator der Veranstaltung beteiligt.

– ENISA High Level Event 1. Oktober 2014, Brüssel

Die Veranstaltung wurde von der EU-Agentur ENISA ausgerichtet. Im Rahmen dieser Veranstaltung wurde über den Zusammenhang zwischen Industriepolitik und Cyber-Sicherheit sowie über sichere Zukunftstechnologien diskutiert. Auch die Herausforderungen an die Cyber-Sicherheit der EU wurden thematisiert. Darüber hinaus nutzte ENISA das High Level Event als offizielle Auftaktveranstaltung für den „Monat der europäischen Cyber-Sicherheit“. Die Tagesordnung des Events ist auf der ENISA-Webseite abruf-

bar (www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2014-and-ecsm-launch/2014-high-level-event-programme).

Nach Kenntnisstand der Bundesregierung waren keine Vertreter der USA bzw. aus Nicht-EU-Mitgliedstaaten an der Konferenz beteiligt. Seitens deutscher öffentlicher Stellen gab es nach Kenntnis der Bundesregierung keine Beiträge. Der Tagesordnung ist zu entnehmen, dass ein Vertreter der deutschen Privatwirtschaft einen aktiven Redebeitrag hatte.

– European Cybercrime Task Force (EUCTF), 6. und 7. November 2014, Den Haag

Die EUCTF wurde 2010 gegründet. Die Expertengruppe besteht aus den Leitern der jeweiligen Cybercrimedienststellen der EU-Mitgliedstaaten, Vertretern von Europol, Eurojust, CEPOL und INTERPOL. Die EUCTF trifft sich zweimal jährlich. Die Treffen dienen der Intensivierung des Informationsaustauschs im Bereich Cybercrime sowie der Unterstützung bei der Entwicklung von Strategien zur effektiven Bekämpfung von Cybercrime. Die Veranstaltung wird von Europol organisiert und vorbereitet. Das Bundeskriminalamt (BKA) war beim letzten EUCTF-Meeting mit Mitarbeitern aus der Gruppe Cybercrime der Abteilung Schwere und Organisierte Kriminalität vertreten. Die USA waren ebenfalls vertreten. Ein Mitarbeiter des FBI hielt einen Vortrag zum Thema „Digital forensics and cyber investigations“.

3. Welche Abteilungen aus den Bereichen Innere Sicherheit, Informationstechnik sowie Strafverfolgung welcher Agenturen bzw. Behörden der EU (auch der Terrorismuskoordinator) nehmen nach Kenntnis der Bundesregierung mit welcher Personalstärke an der im Jahr 2010 gegründeten „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ (High-level EU-US Working Group on cyber security and cybercrime) teil (Bundestagsdrucksachen 17/7578, 18/164)?

An den bekannten Veranstaltungen der Unterarbeitsgruppen haben nach dem Kenntnisstand der Bundesregierung Mitarbeiterinnen und Mitarbeiter der Generaldirektion für Kommunikationsnetze, Inhalte und Technologien (GD CONNECT) der Europäischen Kommission teilgenommen. Darüber hinaus nahmen vereinzelt Vertreterinnen und Vertreter des Generalsekretariates des Rates, des Europäischen Auswärtigen Dienstes, der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) sowie des Joint Research Centre (JRC) teil.

a) Welche Unterarbeitsgruppen existieren derzeit, und welche Behörden der EU bzw. ihrer Mitgliedstaaten nehmen nach Kenntnis der Bundesregierung mit welchen Behörden daran teil?

Nach dem Kenntnisstand der Bundesregierung wurden im Jahr 2010 die Sub-Groups Public Private Partnerships, Cyber Incident Management und Awareness Raising sowie eine Unterarbeitsgruppe zu Cyberkriminalität gegründet. Soweit bekannt, sind Vertreter folgender Behörden der Europäischen Union und ihrer Mitgliedstaaten als Teilnehmer der Unterarbeitsgruppen gemeldet:

GovCERT (AUT), das Bundesministerium des Innern (BMI) (DEU), das Bundesamt für Sicherheit in der Informationstechnik (BSI) (DEU), ANSSI (FRA), BIS (GBR), CPNI (GBR), eKnowledge Agency (PRT), Post and Telecom Agency (SWE), Swedish Contingency Agency (SWE), FORTH-ICS (GRC), CERT-Hungary (HUN), Estonian Informatics Centre (EST), Romanian Intelligence Service (ROM), INTECO (ESP) sowie NLD, FIN, MLT, DNK, BEL und die ENISA.

b) Welche Abteilungen des Bundesministeriums des Innern (BMI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder anderer Behörden waren in welcher Personalstärke (auch anlassbezogen) an der Arbeitsgruppe bzw. den Unterarbeitsgruppen beteiligt?

c) Welche Ministerien, Behörden oder sonstigen Institutionen sind seitens der USA mit welchen Abteilungen an der Arbeitsgruppe bzw. an den Unterarbeitsgruppen beteiligt?

d) Worin besteht der konkrete Beitrag des US-amerikanischen Heimatschutzministeriums (DHS – Department of Homeland Security) für die Gruppe?

Die Fragen 3b, 3c und 3d werden gemeinsam beantwortet.

Die Sub-Groups Public Private Partnerships, Cyber Incident Management und Awareness Raising sind seit dem Jahr 2012 inaktiv, so dass keine weiteren Aussagen zu den Aktivitäten und Besetzungen der Unterarbeitsgruppen möglich sind, die über die Antworten der Bundesregierung zur Kleinen Anfrage der Fraktion DIE LINKE., auf Bundestagsdrucksache 18/164 vom 12. Dezember 2013 hinausgehen.

e) Welche Sitzungen der „high-level EU-US Working Group on cyber security and cybercrime“ oder ihrer Unterarbeitsgruppen haben im Jahr 2014 mit welcher Tagesordnung stattgefunden, und welche deutschen Beteiligten waren dabei anwesend?

Nach Kenntnis der Bundesregierung haben im Jahr 2014 keine Sitzungen der Unterarbeitsgruppen Public Private Partnerships, Cyber Incident Management und Awareness Raising stattgefunden. Entgegen der angekündigten Planung aus dem Jahr 2013 fanden im Jahr 2014 nach Kenntnis der Bundesregierung auch keine EU-US-IT-Krisenübung und kein gemeinsamer „EU-US Security Awareness Month“ statt.

4. Welche „US-EU Working Groups“ bzw. entsprechenden Unterarbeitsgruppen existieren nach Kenntnis der Bundesregierung derzeit, und wer nimmt an den Treffen der Gruppe(n) teil?

Zu derzeit existierenden EU-US Working Groups liegen der Bundesregierung keine Erkenntnisse vor.

5. Welche Treffen der „Security Cooperation Group“ des DHS und des BMI haben in den Jahren 2013 und 2014 stattgefunden, und welche Themen standen auf der Tagesordnung?

Im Jahr 2013 hat eine Sitzung der „Security Cooperation Group“ stattgefunden. Diesbezüglich wird auf die Antwort der Bundesregierung zu Frage 31 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/14474 vom 25. Juni 2013 verwiesen.

Im Jahr 2014 haben zwei Sitzungen der „Security Cooperation Group“ stattgefunden.

Im Wesentlichen standen in der Sitzung im ersten Halbjahr 2014 die Themen

- Austausch zur Gefährdungslage,
- Berichte aus den Arbeitsgruppen,
- Foreign Fighters,

- Bekämpfung des gewalttätigen Extremismus,
- Cyberthemen

und in der Sitzung im zweiten Halbjahr 2014 die Themen

- Austausch zur Gefährdungslage,
- Berichte aus den Arbeitsgruppen,
- Luftsicherheit und Foreign Fighters,
- Cybersicherheit

auf der Tagesordnung.

6. Welche „EU-/US-Senior-Officials-Treffen“ haben nach Kenntnis der Bundesregierung im Jahr 2014 stattgefunden?

EU-US Senior-Officials-Treffen haben im Jahr 2014 am 24./25. Februar in Athen und am 17./18. September in Rom stattgefunden.

7. Inwiefern hat sich das „EU-/US-Senior-Officials-Treffen“ nach Kenntnis der Bundesregierung im Jahr 2014 auch mit den Themen „Cybersicherheit“, „Cyberkriminalität“ oder „Sichere Informationsnetzwerke“ befasst, und welche Inhalte standen hierzu jeweils auf der Tagesordnung?

Am 17./18. September 2014 fand ein „EU-/US-Senior-Officials-Treffen“ statt, dass im Wesentlichen den Stand der gemeinsamen EU-US-Kooperation im Bereich Cyberkriminalität behandelt. Es wurde über die Themen Kindesmissbrauch im Onlinebereich, Regulierung von Domain-Namen, Förderung der Umsetzung der Budapester Konvention gegen Datennetzkriminalität und anonyme Peer-to-Peer Netzwerk-Attacken gesprochen. Weiteres Thema war der Kapazitätsaufbau im internationalen Bereich.

8. Welche Regierungen von den Mitgliedstaaten der EU oder anderer Länder sowie sonstigen, privaten oder öffentlichen Einrichtungen sind bzw. waren nach Kenntnis der Bundesregierung mit welchen Aufgaben am NATO-Manöver „Cyber Coalition 2014“ aktiv beteiligt, und welche hatten eine beobachtende Position inne (bitte auch die Behörden der Teilnehmenden aufführen)?

An der Übung nahmen neben NATO-Einrichtungen bzw. NATO-Organisationen insgesamt 28 Nationen aktiv teil.

Aus Deutschland hat die Bundeswehr (Federführung) gemeinsam mit dem BSI an der Übung teilgenommen. Das BSI war in seiner Rolle als National Cyber Defense Authority (NCDA) gegenüber der NATO als zentrales Element des nationalen IT-Krisenmanagements aktiv. Die Bundeswehr hat an „Cyber Coalition 2014“ (CC14) mit Vertretern des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung, des IT-Zentrums der Bundeswehr, des Kommandos Strategische Aufklärung sowie des Amtes für den Militärischen Abschirmdienst teilgenommen.

Im Rahmen der seitens der NATO angebotenen Teilnahme eines Vertreters pro Nation aus dem Bereich Industrie oder Wissenschaft nahmen Beobachter aus zwölf Nationen teil. Für Deutschland war ein Vertreter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie als Beobachter vor Ort.

Die Aufzählung der weiteren teilnehmenden Staaten kann nicht veröffentlicht werden. Die Unterlage, aus der die teilnehmenden Nationen entnommen wurden, ist „NATO UNCLASSIFIED“ eingestuft. Informationen und Dokumente mit dieser Geheimhaltungsstufe dürfen nur für offizielle Zwecke genutzt werden, und nur Einzelpersonen, Körperschaften oder Organisationen, die diese Informationen für offizielle NATO-Zwecke benötigen, dürfen Zugriff auf diese haben, so dass eine Veröffentlichung dieser Information im Internet als Bundestagsdrucksache ausgeschlossen ist. (Quelle: NATO C-M(2002)60, The Management of NON-CLASSIFIED Information).

a) Welches Ziel verfolgte „Cyber Coalition 2014“?

Übungsziel der CC14 war das Üben und Validieren von Verfahren der NATO und der Nationen im multinationalen Informationsaustausch bei gravierenden Vorfällen im Cyber-Raum.

b) Welche Szenarien wurden hierfür durchgespielt?

Basierend auf einem fiktiven Szenario wurden Schutzmaßnahmen gegen vielfältige Angriffe auf die eingesetzten „Missions“ IT-Systeme auf der Netzwerk-, System- und Applikationsebene durchgespielt. Ergänzt wurden die technisch geprägten Szenare durch rechtliche Aspekte betreffende Cyber-Vorfälle im Rahmen des NATO-Einsatzes im fiktiven Einsatzraum.

c) Wer war für die Erstellung und Durchführung der Szenarien verantwortlich?

Die Verantwortung für die Erstellung und Durchführung oblag dem durch die NATO gestellten Direktor der Übung und seinem Planungsteam.

d) Auf welche Weise haben deutsche Behörden welche Szenarien mitbestimmt?

Vertreter der Bundeswehr und des BSI haben an den Vorbereitungsveranstaltungen des Planungsteams teilgenommen, sich an den Diskussionen beteiligt und in Abstimmung die nationalen Szenario-Anteile (eine gleiche Vorlage für alle Nationen, welche diese für ihre Teilnehmer anpassen konnten) für die deutschen Übungsteilnehmer angepasst. Eine Mitbestimmung, welche Szenarien zur Anwendung gekommen sind, fand nicht statt.

e) An welchen Standorten fand die Übung statt?

Die Übung wurde von Tartu (Estland) gesteuert; die beteiligten Nationen nahmen von Standorten innerhalb ihres Landes an der vernetzten Übung teil.

f) Wie hat sich die Bundesregierung in die Vor- und Nachbereitung von „Cyber Coalition 2014“ eingebracht?

Das BMI und das Bundesministerium der Verteidigung (BMVg) haben an den vorbereitenden Planungskonferenzen teilgenommen sowie Beiträge für den After Action Report zur Übung erstellt.

9. Welche Regierungen von den Mitgliedstaaten der EU oder anderer Länder sowie sonstigen, privaten oder öffentlichen Einrichtungen sind bzw. waren nach Kenntnis der Bundesregierung mit welchen Aufgaben an „Cyber Europe 2014“ aktiv beteiligt, und welche hatten eine beobachtende Position inne (bitte auch die Behörden der Teilnehmenden aufführen)?

An der Übung waren 29 EU- und EFTA-Staaten einschließlich Deutschland sowie 200 Organisationen beteiligt. Der Bundesregierung liegt keine detaillierte Teilnehmerübersicht mit Aufgabenzuordnung vor.

In der Regel gehörte zu den übernommenen Aufgaben neben der Teilnahme auch in Einzelfällen eine Unterstützung der Übungsvorbereitung und Durchführung. Die Federführung für die Gesamtkoordination und Vorbereitung lag bei der ENISA. Seitens Deutschland waren das BSI sowie zwei Energieversorger und zwei IKT-Anbieter aus der Privatwirtschaft beteiligt.

a) Welches Ziel verfolgte „Cyber Europe 2014“?

Ziel der „Cyber Europe 2014“ war, die Zusammenarbeit zwischen den Nationen bei der Bewältigung schwerwiegender pan-europäischer Cyber-Sicherheitsvorfälle zu üben. Das Übungsziel umfasste das Austesten:

- von Alarmierungs-, Kooperations- und Austauschmechanismen zwischen den zuständigen nationalen IT-Sicherheitsbehörden,
- existierender nationaler Krisenpläne für den Bereich Cyber-Sicherheit,
- von Auswirkungen einer Vielzahl paralleler Kommunikationsbeziehungen auf die Generierung eines nationalen/europäischen Lagebilds (zwischen europäischen KRITIS-Betreibern und zwischen KRITIS-Betreibern und IT-Sicherheitsbehörden),
- von Eskalierungs- und Deeskalierungsprozessen (technische/operationelle/strategische Ebene),
- von Auswirkungen einer übergreifenden europäischen Cyber-Krise auf die Presse- und Öffentlichkeitsarbeit.

b) Welche Szenarien wurden hierfür durchgespielt?

Die Antwort zu Frage 9b ist als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft, was im Hinblick auf das Staatswohl erforderlich ist. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann, entsprechend einzustufen.*

Detailinformationen insbesondere bezüglich der Teilnehmer und Szenarien der Übung „Cyber-Europe 2014“ unterliegen einem „Non Disclosure Agreement“ (NDA) (TLP AMBER), das eine Weitergabe außerhalb der Bundesregierung verbietet, oder unterliegen seitens der federführenden Organisation einer VS-Einstufung und sind dadurch nicht zur Veröffentlichung freigegeben. Ein NDA ist eine Vertraulichkeitsvereinbarung zwischen Partnern, in der die Weitergabe von Informationen geregelt wird. Derartige NDAs werden in vornehmlich inter-

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

nationalen und Wirtschafts-Umgebungen genutzt, in denen staatliche Verschlusssachenregelungen nicht anwendbar sind.

Dabei bedeutet TLP AMBER, dass die Information ausschließlich in der eigenen Organisation weitergegeben werden darf. AMBER ist nach ROT (Nur zur persönlichen Unterrichtung) die zweithöchste Einstufung. Es muss daher ausdrücklich von einer Veröffentlichung abgesehen werden. Ein Nichtbeachten des NDAs führt zum Ausschluss aus dem Informationsaustausch und damit zu signifikanten Nachteilen für die Behörden der Bundesrepublik Deutschland, die Frühwarnungen, Hinweise und Informationen zum Schutz der Regierungsnetze nicht mehr erhalten würden.

c) Wer war für die Erstellung und Durchführung der Szenarien verantwortlich?

Unter Federführung der ENISA haben die Mitgliedstaaten Ideen und Anregungen in die Vorbereitung eingebracht, die von ENISA in konkrete Einspielungen umgesetzt wurden. Die Einspielungen wurden durch die nationalen Vertreter, die in die zentrale Übungssteuerung eingebunden waren, an die jeweiligen Übungsteilnehmer gesendet und dort von den Teilnehmern bearbeitet.

d) Auf welche Weise haben deutsche Behörden welche Szenarien mitbestimmt?

Das BSI hat an den Planungsveranstaltungen der ENISA teilgenommen und übergreifend Ideen und Anregungen aus den eigenen Erfahrungen eingebracht.

e) An welchen Standorten fand die Übung statt?

Grundsätzlich erfolgte die Teilnahme von den jeweiligen Arbeitsplätzen der Teilnehmer aus. Die innerhalb des BSI beteiligten Übungsteilnehmer nahmen vom Standort der Behörde in Bonn teil. Die zentrale Übungssteuerung war in Athen bei der ENISA angesiedelt. Des Weiteren fand eine Veranstaltung in Brüssel statt.

f) Wie hat sich die Bundesregierung in die Vor- und Nachbereitung von „Cyber Europe 2014“ eingebracht?

Das BSI hat sich an der Vorbereitung (siehe Antwort zu den Fragen 9c bis 9e) sowie der Nachbereitung der Übung durch Entsendung von Fachpersonal und das Einbringen von Erfahrungen und Erkenntnissen beteiligt.

10. Innerhalb welcher zivilen oder militärischen „Cyberübungen“ oder vergleichbarer Aktivitäten haben welche deutschen Behörden im Jahr 2014 „Sicherheitsinjektionen“ vorgenommen, bei denen Schadsoftware eingesetzt oder simuliert wurde, und worum handelte es sich dabei?

a) Welche Programme wurden dabei „injiziert“?

b) Wo wurden diese entwickelt, und wer war dafür jeweils verantwortlich?

Deutsche Behörden haben bei zivilen oder militärischen „Cyberübungen“ keine „Sicherheitsinjektionen“ vorgenommen, bei denen Schadsoftware eingesetzt oder simuliert wurde.

11. Bei welchen Cyberübungen unter deutscher Beteiligung wurden im Jahr 2014 Szenarien „geprobt“, die über das Internet ausgeführte Angriffe auf kritische Infrastrukturen, „cyberterroristische Anschläge“ oder „politisch motivierte Cyberangriffe“ zum Inhalt hatten, und um welche Szenarien handelte es sich dabei konkret (Bundestagsdrucksache 17/11341; bitte mitteilen, wann und wo die Übungen stattfanden)?

Die Antwort zu Frage 11 ist als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft, was im Hinblick auf das Staatswohl erforderlich ist. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann, entsprechend einzustufen.*

Detailinformationen insbesondere bezüglich der Teilnehmer und Szenarien der Cyberübungen unterliegen einem „Non Disclosure Agreement“ (NDA) (TLP AMBER), das eine Weitergabe außerhalb der Bundesregierung verbietet, oder unterliegen seitens der federführenden Organisation einer VS-Einstufung und sind dadurch nicht zur Veröffentlichung freigegeben. Ein NDA ist eine Vertraulichkeitsvereinbarung zwischen Partnern, in der die Weitergabe von Informationen geregelt wird. Derartige NDAs werden in vornehmlich internationalen und Wirtschafts-Umgebungen genutzt, in denen staatliche Verschlusssachenregelungen nicht anwendbar sind. Dabei bedeutet TLP AMBER, dass die Information ausschließlich in der eigenen Organisation weitergegeben werden darf. AMBER ist nach ROT (Nur zur persönlichen Unterrichtung) die zweithöchste Einstufung. Es muss daher ausdrücklich von einer Veröffentlichung abgesehen werden. Ein Nichtbeachten des NDAs führt zum Ausschluss aus dem Informationsaustausch und damit zu signifikanten Nachteilen für die Behörden der Bundesrepublik Deutschland, die Frühwarnungen, Hinweise und Informationen zum Schutz der Regierungsnetze nicht mehr erhalten würden.

12. Welche weiteren, ähnlichen Übungen unter deutscher Beteiligung sind derzeit geplant?

Folgende ähnliche Übungen unter deutscher Beteiligung befinden sich derzeit in Planung:

Locked Shields 2015, IWWN 2015, NATO Cyber Coalition 2015.

13. Mit welchen technischen Mitteln bzw. Fähigkeiten soll die innerhalb des Bundeswehrkommandos „Strategische Aufklärung“ eingerichtete Gruppe „Computer-Netzwerk-Operationen“ (CNO) „legitime Ziele“ angreifen und/ oder zerstören (Bundestagsdrucksache 18/3963; bitte erläutern)?

Die technischen Möglichkeiten, im Internet zu operieren, sind universal, grundsätzlich bekannt und werden in offen zugänglichen Foren und Kongressen diskutiert. Schwachstellen in Soft- und Hardware werden genutzt, um in gegnerische Netzwerke einzudringen, dort aufzuklären, einzelne Funktionen zu stören und zeitweise außer Betrieb zu setzen oder dauerhaft zu schädigen.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Das Vorgehen im Einzelfall hängt ab vom Operationsziel und von der Konstellation der Schutzfunktionen des gegnerischen Netzwerks. Dabei werden die Vorgehensweise und die dabei zu nutzenden Werkzeuge auf den Einzelfall zugeschnitten.

14. Inwiefern bzw. wodurch unterscheiden sich die technischen Mittel bzw. Fähigkeiten des CNO von Mitteln des „elektronischen Kampfes“?

CNO richten sich gegen gegnerische Computernetzwerke und dringen in diese ein. Dabei werden u.a. Zugangsmöglichkeiten über das Internet genutzt.

Die Mittel des elektronischen Kampfes nutzen die physikalischen Bedingungen für die Wellenausbreitung im elektromagnetischen Spektrum.

15. Worin genau besteht bzw. bestand der konkrete Beitrag der deutschen Tochterfirma des US-Geheimdienstzulieferers CSC Deutschland Solutions GmbH für das militärische EU-Überwachungsnetzwerk MARSUR, das seit dem 28. Oktober 2014 in den operativen Betrieb übergegangen ist, und an dem auch die Bundeswehr beteiligt ist (EDA-Mitteilung vom 15. April 2013, Bundestagsdrucksache 18/3884)?

Die Firma CSC Deutschland Solutions GmbH war mit der technischen Lösung zum Lagebildaustausch beauftragt.

16. Wer sind die von einer Verlängerung einer bereits im Jahr 2012 erteilten, aber nicht ausgeschöpften Genehmigung über Zieldarstellungsgeräte für Infanteriewaffen, Geräteausstattung für ein Übungsgelände, Schießsimulationssysteme GLADIO, Radare, optronische Ausrüstung, Software und Technologie zur Verwendung in Saudi-Arabien betroffenen Hersteller (DIE WELT vom 4. Februar 2015 sowie www.jan-van-aken.de/files/bsr_2_2015.pdf)?

Bei den in der Frage angesprochenen Fällen handelt es sich entgegen der Fragestellung nur in einem Fall um eine Verlängerung einer bereits im Jahr 2012 erteilten, aber nicht ausgeschöpften Genehmigung (Radare, optronische Ausrüstung, Software und Technologie) für das Unternehmen Airbus Defence and Space GmbH, die bereits im Rüstungsexportbericht 2012 veröffentlicht ist. Eine Genehmigung über Zieldarstellungsgeräte für Infanteriewaffen (im Umfang der Ausstattung für ein Übungsgelände) wurde an das Unternehmen Theissen Training Systems GmbH erteilt. Eine Genehmigung über vier Schießsimulationssysteme GLADIO wurde an das Unternehmen e.sigma systems GmbH erteilt.

a) Welche weiteren Details kann die Bundesregierung zu Typ und Leistungsmerkmalen der Radare, optronischen Ausrüstung, Software und Technologie für das Grenzsicherungssystem bzw. die Grenzsicherungssysteme mitteilen?

Es handelt sich im vorliegenden Fall um die Verlängerung einer bereits 2012 erteilten, aber nicht ausgeschöpften Genehmigung.

Bei den genehmigten Gütern handelt es sich um Radare, optronische Ausrüstung, Software und Technologie zur Verwendung für ein Grenzsicherungssystem. Darüber hinausgehende Informationen zu den Gütern können zum Schutz der Geschäftsgeheimnisse des betroffenen Unternehmens nicht gemacht werden. Das Bundesverfassungsgericht hat hierzu in seinem Urteil vom 21. Oktober 2014 (2 BvE 5/11) festgestellt, dass Angaben der Bundesregierung gegenüber

dem Deutschen Bundestag, die Rückschlüsse auf die Spezifikationen des Rüstungsgutes zuließen, einen unverhältnismäßigen Eingriff in die verfassungsmäßig geschützten Betriebs- und Geschäftsgeheimnisse der an dem Geschäft beteiligten Unternehmen darstellen würden. An diesen Daten bestehe auch kein berechtigtes Informationsinteresse, weil sie für die parlamentarische Kontrolle der Regierungstätigkeit nicht erforderlich seien (2 BvE 5/11, Rn. 192).

b) Welche dieser Ausrüstung, Software und Technologie soll nach Kenntnis der Bundesregierung in das System zur Überwachung der insgesamt 6 125 km langen Land- und Seegrenze Saudi-Arabiens integriert werden, das von der Bundespolizei und der Bundeswehr unter anderem im Rahmen der Ausbildung zum Führen mittelgroßer Drohnen unterstützt wird (Telepolis vom 8. März 2012)?

Bei der Verlängerung einer bereits im Jahr 2012 erteilten, aber nicht ausgeschöpften Genehmigung über Radare, optronische Ausrüstung, Software und Technologie zur Verwendung für Grenzsicherungssystem handelt es sich um Güter, die zur Sicherung von insgesamt 6 125 km Land- und Seegrenze dienen sollen.

Die Bundespolizei führt keine Ausbildung an den vorgenannten Gütern durch. Dies gilt auch für eine Ausbildung zum Führen mittelgroßer Drohnen. Die Bundeswehr hat die Firma EMT bei der Ausbildung saudi-arabischer Soldaten am System LUNA unterstützt.

17. Welche Behörden der Bundesregierung nahmen Anfang Februar 2015 mit welcher Zielsetzung am „African Security & Counter-Terrorism Summit 2015“ in London teil?

Die zuständigen Behörden der Bundesregierung haben nicht an dieser Veranstaltung teilgenommen.

18. Inwieweit bzw. mit welchem Inhalt oder konkreten Maßnahmen sind Behörden der Bundesregierung auch im Jahr 2014 mit „Cyber Situation Awareness“ oder „Cyber Situation Prediction“ beschäftigt, bzw. welche Kapazitäten sollen hierfür entwickelt werden (Bundestagsdrucksache 18/164)?

Im Jahr 2011 wurde im Rahmen der Umsetzung der Cybersicherheitsstrategie für Deutschland das Nationale Cyber-Abwehrzentrum für den behördenübergreifenden Informationsaustausch zur Bedrohungslage und zur Koordinierung von Maßnahmen gegründet. Auch die Teilnehmer und Arbeitskreise der Allianz für Cyber-Sicherheit beschäftigen sich mit Beiträgen zum Lagebild „Cyber Situation Awareness and Prediction“.

Die Bundeswehr beteiligt sich an einem ad-hoc Projekt der Europäischen Verteidigungsagentur (EDA) mit dem Ziel des Aufbaus eines Cyberlagebildes auf strategischer und operativer Ebene im Rahmen von Einsätzen bzw. Missionen unter Führung der EU (Gemeinsame Sicherheits- und Verteidigungspolitik).

Aufgrund der steigenden Bedrohungslage im Informationsraum führt die Bundeswehr zusätzlich eine Studie „strategisches Cyberlagebild“ durch, die die Führung eines aktuellen und ebenengerechten Cyberlagebildes im Sinne der Cyber Situation Awareness verbessern soll.

19. Inwiefern bzw. in welchem Umfang waren Spionagetätigkeiten Großbritanniens und der USA in Deutschland auch im Jahr 2014 „Bestandteil der täglichen Lagebeobachtung durch das Cyberabwehrzentrum“ (Bundestagsdrucksache 18/164)?

Die aus der Presse bekannten Vorgänge wurden im Nationalen Cyber-Abwehrzentrum thematisiert.

20. Auf welche Weise waren oder sind Bundesbehörden an der mit deutschen Landeskriminalämtern geführten Datei „USA“ beteiligt, die nach den Anschlägen in den USA am 11. September 2001 zur Erfassung von „Hinweisen auf mögliche Täter und Gehilfen“ eingerichtet wurde, und wie viele Personen und Sachen waren bzw. sind dort nach Kenntnis der Bundesregierung zuletzt gespeichert (Niedersächsischer Landtag, Drucksache 16/2770)?

Die Inpol-Fall-Datei „USA“ ist eine gemeinsame Datei des BKA und der Landeskriminalämter gemäß § 486 Absatz 1 der Strafprozessordnung (Verbunddatei).

Die zuständigen Polizeidienststellen der Länder, die Landeskriminalämter und das BKA haben Zugriff und können Daten eingeben und abrufen.

Nach derzeitigem Stand (26. Februar 2015) sind in der Datei USA

– 362 Personen,
– 49 Organisationen,
– 399 Adressen,
– 168 Telekommunikationsmittel,
– 39 Sachen (Kfz und Sachen)

gespeichert.

21. Wie viele Verbindungsbeamtinnen und Verbindungsbeamte des DHS sind derzeit beim Bundeskriminalamt (BKA) akkreditiert, wo verrichten diese ihren Dienst, und mit welchen Aufgaben sind diese nach Kenntnis der Bundesregierung betraut?

Das US Department of Homeland Security (DHS) hat sechs Mitarbeiter beim BKA als Verbindungsbeamte akkreditiert. Die Verbindungsbeamten gehören dem „Immigration Customs Enforcement (ICE) an, welches dem US-amerikanischen DHS unterstellt ist und verrichten ihren Dienst am US-amerikanischen Generalkonsulat in Frankfurt am Main. Das ICE beschäftigt sich mit Einwanderungs- und Zollfragen. Ansprechpartner sind neben dem BKA auch die Landeskriminalämter, der Zoll und die Bundespolizei.

Ein Mitarbeiter des Secret Service (DHS) unterstützt aktuell den Fachbereich Cybercrime im BKA.

22. Welche Treffen der „Friends of the Presidency Group on Cyber Issues“ haben nach Kenntnis der Bundesregierung im Jahr 2014 stattgefunden, wer nahm daran jeweils teil, und welche Tagesordnung wurde behandelt (Bundestagsdrucksache 18/164)?

Die folgenden Treffen der „Friends of the Presidency Group on Cyber Issues” (Cyber-FoP) haben nach Kenntnis der Bundesregierung im Jahr 2014 stattge-

funden (die jeweiligen Tagesordnungen sind als Anlage beigefügt – auch abrufbar unter http://register.consilium.europa.eu)

- 24. Februar 2014 (CM 1490/14),
- 23. Mai 2014 (CM 2819/14),
- 22. September 2014 (CM 4047/14),
- 8. Dezember 2014 (CM 5240/14).

An den Sitzungen nahmen regelmäßig Vertreterinnen und Vertreter des BMI und des Auswärtigen Amts teil.

23. An welchen Projekten des „Operational Action Plan 2015" werden sich welche deutschen Behörden bezüglich der Priorität „Cyber Attacks" beteiligen, und wer sind die sonstigen Beteiligten der entsprechenden Projekte (bitte nach deren Rolle in den Projekten auflisten)?

In der Priorität Cyberangriffe im OAP 2015 sind Maßnahmen mit deutscher Beteiligung (u. a. des Landeskriminalamts Bayern) geplant. Deutschland wird hier als Aktionsleiter, Co-Aktionsleiter oder Teilnehmer fungieren.

Es sind im OAP 2015 folgende Maßnahmen mit deutscher Beteiligung geplant:

– Erstellung des Internet Organised Crime Threat Assessment-I-OCTA. Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Eurojust und Interpol

– Identifizierung von Cyberbedrohungen mit Auswirkung auf zwei oder mehr Mitgliedstaaten. Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen

– Entwicklung gemeinsamer Methoden zur Cybercrimebekämpfung. Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Interpol

– Identifizierung von wertigen Tätergruppen für gemeinsame Ermittlungen. Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol; Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), J-CAT.

– Konsolidierung einer Internetauswertungskoordinierungsgruppe. Aktionsleiter ist das BKA; Co-Aktionsleiter ist Spanien; Unterstützer sind die EU-Mitgliedstaaten, Norwegen, Schweiz, Europol und Eurojust

– Gründung einer europäischen Cybercrime Expertengruppe. Aktionsleiter sind das BKA, das bayerische LKA sowie Frankreich. Unterstützer sind die EU-Mitgliedstaaten, CEPOL, EUCTF, Eurojust.

– Sammlung und Auswertung von Schadsoftware, die gegen Banken eingesetzt werden. Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), J-CAT, Interpol.

– Maßnahmen gegen wertige Cybercrime-Gruppierungen. Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Rumänien, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), EUCTF, Europol, Eurojust.

– Identifizierung von und Ermittlungen gegen Cybercrime-Gruppierungen, die den Service von OK-Gruppierungen nutzen. Aktionsleiter ist Frankreich, Co-Aktionsleiter ist Rumänien, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Europol, Eurojust.

- Maßnahmen gegen inkriminierte Kommunikationsplattformen. Aktionsleitung durch das BKA, Unterstützer sind Griechenland und Spanien.
- Etablierung der Arbeitsgruppe Joint Cyber Action Task Force (J-CAT). Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die J-CAT Mitglieder (für Deutschland das BKA).
- Unterstützung der EU-Mitgliedstaaten und operativen Partner in der Integration von Finanzermittlungen in Ermittlungen im Rahmen des OAP. Aktionsleiter ist Europol; Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Eurojust.
- Implementierung eines Koordinierungsmechanismus zur Bekämpfung von Botnetzen. Aktionsleiter ist Europol; Unterstützer sind Frankreich, Großbritannien und die EUCTF.
- Erhebung von Informationen zur Notwendigkeit eines „Compromised Data Clearing House“. Aktionsleitung durch das BKA; Co-Aktionsleitung durch die Niederlande; Unterstützer sind EU-Mitgliedstaaten, Europol, Interpol, CERTs
- Erstellung von Richtlinien gemäß Artikel 13 der Richtlinie 2013/40/EU zu Cyberangriffen gegen Informationssysteme. Aktionsleitung durch Kroatien; Co-Aktionsleitung durch Slowenien; Unterstützer sind Deutschland (BKA), Portugal, Europol, Eurojust, EUCTF, DG Home
- Entwicklung von Kursen und Kursmaterialien zur Aus- und Fortbildung von Cybercrime-Ermittlern. Aktionsleiter ist CEPOL; Co-Aktionsleiter sind Europol, Eurojust, ECTEG. Unterstützung durch die EU-Mitgliedstaaten (für Deutschland durch das BKA), DG Home
- Entwicklung/Implementierung eines Anonymisierungsverfahrens für die Datenauswertung. Aktionsleitung durch Europol; Unterstützung durch Deutschland (BKA), Kroatien, J-CAT, Eurojust
- Entwicklung/Implementierung einer Online-Ausbildungsplattform. Aktionsleitung durch Europol; Unterstützung durch Deutschland (BKA), CEPOL, ECTEG
- Unterstützung einer operativen ITOM-Maßnahme zu Trainingszwecken. Aktionsleitung durch Niederlande; Co-Aktionsleitung durch Europol, Eurojust; Unterstützer: EU-Mitgliedstaaten (für Deutschland das BKA).

24. Welche konkreten Themen bzw. Fähigkeiten wurden bei einem „mehrtägigen Arbeitsbesuch“ des BKA mit den Behörden der Ukraine zum Thema „Cybercrime“ behandelt (Bundestagsdrucksache 18/3979)?

Im Rahmen des im BKA durchgeführten Arbeitsbesuches wurden allgemeine und rechtliche Themen zur polizeilichen Zusammenarbeit zwischen der Ukraine und der Bundesrepublik Deutschland erörtert. Weiterhin konnte eine Ausbildungshilfe in Bezug auf einen allgemeinen technischen Lehrgang gewährt werden, der im BKA durchgeführt wurde und das Thema Malware im Allgemeinen behandelte.

a) Auf wessen Initiative kam die Veranstaltung zustande?

Es handelte sich um einen seitens des BKA initiierten und durch das BMI genehmigten Arbeitsbesuch im Rahmen der Polizeilichen Ausbildungshilfe (PAH).

b) Wo fand die Veranstaltung statt?

Der Besuch erfolgte im BKA.

c) Welche ukrainischen Behörden oder sonstigen Institutionen nahmen an der Veranstaltung teil?

Von Seiten der Ukraine wurde ein Vertreter der Verwaltung für Bekämpfung von Cybercrime der Hauptverwaltung des Innenministeriums der Ukraine in Kiew entsandt.

d) Welche weiteren, ähnlichen Veranstaltungen sind mit der Ukraine geplant?

Aktuell ist eine Fortsetzung der im Jahr 2014 begonnenen Maßnahmen im Zuge der Polizeilichen Ausbildungshilfe für das Jahr 2015 geplant.

25. Worum handelte es sich bei einem „Studienbesuch der Financial Intelligence Unit“ zwischen den ukrainischen Behörden und dem BKA (Bundestagsdrucksache 18/3979)?

Es handelte sich um einen Studienbesuch im Rahmen des EU-Programms „TAIEX“ (Technical Assistance and Information Exchange Instruments) unter Beteiligung der Financial Intelligence Unit (FIU) Ukraine, der Bundesanstalt für Finanzdienstleistungsaufsicht, des Landeskriminalamtes Hamburg und des BKA.

a) Auf wessen Initiative kam die Veranstaltung zustande?

Die Initiative zur Durchführung der Veranstaltung ging von der FIU Ukraine, Abteilung „Internationale Zusammenarbeit“, aus.

b) Wo fand die Veranstaltung statt?

Die Veranstaltungsorte waren Hamburg und Bonn.

c) Welche ukrainischen Behörden oder sonstigen Institutionen nahmen an der Veranstaltung teil?

Teilgenommen haben Vertreter des „International Cooperation Department“ der FIU Ukraine sowie des „Financial Investigation Department – FID“.

d) Welche weiteren, ähnlichen Veranstaltungen sind mit der Ukraine geplant?

Zurzeit sind keine weiteren vergleichbaren Veranstaltungen mit der Ukraine geplant.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333