Deutscher Bundestag **Drucksache 18/3027**

18. Wahlperiode 30.10.2014

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/2850 –

Zivil-militärische Krisenübungen der Europäischen Union zu Störungen des Internets

Vorbemerkung der Fragesteller

Am 30. September 2014 startete die Europäische Union (EU) ihre zweite „Multi-Layer"-Krisenübung. Das Manöver „ML14" dauert bis zum 23. Oktober 2014 und steht unter der Ägide der Gemeinsamen Sicherheits- und Verteidigungspolitik, verantwortlich ist der Europäische Auswärtige Dienst (EAD). Auch die Europäische Kommission und Delegationen einzelner EU-Mitgliedstaaten sind beteiligt (Pressemitteilung EAD, 30. September 2014). Geführt wird die Operation von einem militärischen Kommandozentrum in Italien sowie dem Hauptquartier der „EU Battlegroup" in Belgien. „ML14" simuliert Szenarien, die an die Lage in der Ukraine, in Libyen und Algerien erinnern: Der fiktive Staat „Sarunia" muss auf bewaffnete Auseinandersetzungen an seinen Grenzen reagieren, wo sich die Staaten „Ranua" und „Celego" Scharmützel liefern. Eine EU-Militärmission greift ein. Nach einem Angriff auf einen Öltanker droht eine Ölpest, während zahlreiche Staatsangehörige von EU-Mitgliedstaaten in einer Ölraffinerie von einer Entführung bedroht sind. Schließlich wird eine Stadt „Batela" Ziel eines „Cyber-Angriffs". In „Batela" befinden sich EU-Kommunikationssysteme.

Ende des Jahres soll ein weiteres Manöver abgehalten werden, das ebenfalls einen „Cyberangriff" simuliert (Bundestagsdrucksache 18/2674). Dabei handelt es sich um eine „Integrated Political Crisis Response" (IPCR) der EU. Die Bundesregierung stimmt derzeit zwischen dem Bundesministerium des Innern (BMI) und dem Auswärtigen Amt (AA) ihre Formen der Teilnahme an der IPCR-Übung ab. Auch wenn es sich in den Szenarien von „ML14" und der IPCR-Übung nicht unbedingt um militärische „Cyberangriffe" handelt, werden sie vom Militär beantwortet. Möglich ist dies unter anderem durch die neue „Solidaritätsklausel", wonach ein EU-Mitgliedstaat alle nationalen und auf EU-Ebene vorhandenen Mittel und Instrumente zu Hilfe holen kann. Hierzu gehören Militär, Polizei und Geheimdienste. Laut der Bundesregierung können als Auslöser der „Solidaritätsklausel" auch „Cyberkrisen" zählen, wenn diese „katastrophale Auswirkungen haben oder auf einem Terroranschlag beruhen". Zusätzlich könne das EU-Katastrophenschutzverfahren zum Einsatz kommen,

Die Antwort wurde namens der Bundesregierung mit Schreiben des Auswärtigen Amts vom 27. Oktober 2014 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

wenn durch den Ausfall von IT-Systemen „gravierende Folgen auftreten sollten, die mit Mitteln des Katastrophenschutzes zu bewältigen wären“.

Vorbemerkung der Bundesregierung

Die „Multi-Layer“-Krisenübung „ML14“ findet im Rahmen des von der Europäischen Union (EU) beschlossenen Konzepts zur Durchführung von Übungen zur Verbesserung der Krisenmanagementfähigkeiten im Bereich der Gemeinsamen Außen- und Sicherheitspolitik statt.

Ziel ist es, die Fähigkeit der EU, ihrer Institutionen und der Mitgliedstaaten zu stärken und auszubauen, um auf entstehende Krisen rechtzeitig und geschlossen antworten zu können. Dadurch soll die EU in die Lage versetzt werden, effektiv und gut vorbereitet ihre Rolle als globaler außen- und sicherheitspolitisch handelnder Akteur wahrzunehmen. Im Rahmen solcher Übungen wird sowohl der Einsatz der personellen als auch der systemischen Ressourcen geübt, einschließlich der Strukturen, Konzepte und Prozesse.

Es handelt sich hierbei grundsätzlich um Planungsübungen. Alle Übungsteilnehmer nehmen ihre jeweilige Rolle im Krisenmanagement der EU gemäß der festgelegten EU-Krisenmanagementverfahren wahr. Die Planungsmaßnahmen erfolgen dabei durch die jeweils in den einzelnen Mitgliedstaaten zuständigen Behörden, in den Vertretungen der Mitgliedstaaten in Brüssel, im Rat der EU (einschließlich des Generalsekretariats des Rates in Brüssel), in einzelnen Botschaften der Mitgliedstaaten, im Europäischen Auswärtigen Dienst (sowohl in Brüssel als auch in einzelnen EU-Delegationen), in der Europäischen Kommission in Brüssel, im EU-Satellitenzentrum in Spanien und – im Falle von ML14 – im Übungs-Operationshauptquartier in Italien sowie dem Übungs-Truppenhauptquartier in Belgien. An der Vorbereitung und Durchführung von ML14 sind zudem das Europäische Sicherheits- und Verteidigungskolleg und die Europäische Verteidigungsagentur beteiligt.

Die Übungen basieren auf fiktiven, aber realistischen Krisenszenarien außerhalb der EU und umfassen jeweils die Planung, Durchführung, Evaluation und die Erstellung eines Abschlussberichts.

ML14 ist insbesondere darauf gerichtet, Maßnahmen zur Unterstützung der Aufrechterhaltung bzw. Wiederherstellung von Sicherheit und Ordnung als auch Zivilschutzmaßnahmen bei Umweltkatastrophen sowie humanitäre Hilfsaktionen für Flüchtlingslager zu üben. Als zusätzliche Komponente wird die Reaktion auf einen Cyber-Zwischenfall in einer EU-Delegation getestet.

Von Übungen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik grundsätzlich zu unterscheiden sind Übungen im Rahmen der integrierten politischen Krisenreaktion der EU (IPCR). Die nächste, für Ende November 2014 angesetzte Übung, die nach Arbeiten des Planungsteams und Entscheidung des Ratsvorsitzes gemeinsam mit dem Ratssekretariat nun wie ein Workshop aufgebaut ist, soll eine erste Gelegenheit geben, das Krisenmanagement im Rahmen der IPCR auf EU-Ebene zu „üben“ und die standardisierten Abläufe (SOPs) auf ihre Tauglichkeit zu überprüfen. Bei der Durchführung der Übung steht eine Einbeziehung der Hauptstädte nicht im Fokus. Die Natur der Krise, auf Basis derer der IPCR-Mechanismus aktiviert wird, ist dabei grundsätzlich nebensächlich; dies gilt auch für diese Übung.

Die Arbeit an diesem Mechanismus zur politischen Krisenkoordination auf EU-Ebene hat der Rat als Ergebnis eines längeren Überprüfungsprozesses der alten Vorkehrungen der EU zur Koordinierung in Krisen- und Notfällen (CCA) am 25. Juni 2013 beschlossen. Sowohl inner- als auch außerhalb der EU können Notfälle oder Krisen größeren Ausmaßes auftreten, die von so großer Tragweite oder politischer Bedeutung sind, dass sie eine zeitnahe Koordinierung und

Reaktion auf der politischen Ebene der EU erfordern. Erfahrungen wie die Terroranschläge in Mumbai im Jahr 2008 oder die Folgen des Ausbruchs des Vulkans Eyjafjallajökull im Jahr 2010 brachten die Erkenntnis, dass die EU ihre koordinierende Funktion in derartigen Krisen trotz der CCA nur unzureichend wahrnehmen konnte. Die neuen IPCR sind darauf ausgerichtet, mögliche Synergien zwischen den Akteuren und zwischen den vorhandenen Mitteln, Strukturen und Fähigkeiten auf EU-Ebene voll auszunutzen, wobei eine Duplizierung bestehender Strukturen und die Schaffung neuer ständiger Strukturen vermieden werden soll.

1. Auf welche besondere Weise wird das Thema „Cybersicherheit“ bzw. „Cyberverteidigung“ nach Kenntnis der Bundesregierung von der italienischen Ratspräsidentschaft behandelt?

Die italienische Ratspräsidentschaft hat sich zur Umsetzung aller Aspekte der „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“ (Gemeinsame Mitteilung der Europäischen Kommission und der Hohen Vertreterin der Europäischen Union für die Außen- und Sicherheitspolitik vom 7. Februar 2013) bekannt.

Auf dieser Grundlage unterstützt die italienische Präsidentschaft die Verhandlungen zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der Union, der auf eine Angleichung von Kapazitäten und Maßnahmen zur Netz- und Informationssicherheit in den Mitgliedstaaten gerichtet ist.

Die Präsidentschaft unterstützt außerdem die Umsetzung der in der Cybersicherheitsstrategie der Europäischen Union vorgesehenen Maßnahmen zur Förderung industrieller und technischer Ressourcen für die Cybersicherheit, u. a. durch den Ausbau der Zusammenarbeit zwischen der Europäischen Union und industriellen und wissenschaftlichen Partnern. Außerdem soll in Kooperation mit der Kommission, Europol und anderen relevanten Partnern die Ausbildung im Bereich der Abwehr von Cyberbedrohungen in den Mitgliedstaaten unterstützt werden. Im Übrigen wird auf die Antworten zu den Fragen 2 und 3 verwiesen.

2. Worum handelt es sich nach Kenntnis der Bundesregierung bei der „Cyber Defense-Konferenz“, die Ende Oktober 2014 in Rom abgehalten wird, und mit welcher Zielsetzung werden welche Bundesbehörden dort teilnehmen?

Die Konferenz „The role of Cyber Defence to protect and sustain EU economy“, durchgeführt von der italienischen Präsidentschaft des Rates der Europäischen Union, findet vom 30. bis 31. Oktober 2014 in Rom statt. Das Bundesministerium der Verteidigung (BMVg) plant, mit einem Referenten an der Veranstaltung teilzunehmen. Ziel der Teilnahme des BMVg-Vertreters ist es, weitergehende Kenntnisse zum Thema Cyberverteidigung zu erlangen, insbesondere über die Ziele, Initiativen und Projekte im Rahmen der italienischen Präsidentschaft. Darüber hinaus sollen bestehende Expertennetzwerke gestärkt werden.

3. Mit welcher Zielsetzung werden welche Bundesbehörden an der ebenfalls in Rom abgehaltenen Konferenz „Financial cybercrime-cross country coalition“ teilnehmen?

Nach hier vorliegenden Informationen ist eine EU-Konferenz mit dem Titel: „Fighting financial Cybercrime – Cross Country Cooperation between Banks

and Law Enforcement Agencies“ für den 24. Oktober 2014 in Mailand vorgesehen. Die Bundesregierung hat noch nicht über eine Teilnahme entschieden.

4. Welche EU-Mitgliedstaaten oder sonstigen Staaten bzw. welche Einrichtungen der EU waren nach Kenntnis der Bundesregierung an der Vorbereitung der zweiten „Multi-Layer“-Krisenübung „ML14“ beteiligt?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. Auf Basis welcher Annahmen, Risikoanalysen oder sonstigen Einschätzungen wurden nach Kenntnis der Bundesregierung die Szenarien festgelegt und ausgestaltet?

ML14 ist darauf ausgerichtet, die Fähigkeiten der EU in Bezug auf ihr Krisenmanagement zu verbessern und den Einsatz aller zur Verfügung stehenden Ressourcen zu üben und auf die Probe zu stellen. Die Szenarien wurden auf der Basis der Ergebnisse früherer Übungen erstellt. Neu ist die Einbeziehung eines Cyber-Zwischenfalls.

6. Worin genau bestanden die Szenarien der „Multi-Layer“-Krisenübung „ML14“?

Das Szenario für die Planungsübung ML14 basiert auf einer fiktiven geografischen Umgebung im Nordosten Afrikas. Im Zentrum steht der fiktive Staat SARUNIA, dessen Sicherheit durch Ereignisse in den Nachbarländern bedroht wird. Zunehmende Grenzübergriffe durch eine terroristische Gruppe veranlassen SARUNIA, die EU um eine militärische Intervention und die Einrichtung einer zivilen Mission zu bitten. Die humanitäre Situation in Flüchtlingslagern verschlechtert sich dramatisch aufgrund starker Regenfälle, Piraten greifen (erfolglos) einen Öltanker an und verursachen eine Umweltkatastrophe, außerdem dringen Hacker in das Computersystem der EU-Delegation vor Ort ein. Das simulierte EU-Engagement, das den Rahmen zur Übung der Krisenmanagementverfahren bildet, soll folgende Elemente umfassen:

– eine schnelle militärische Reaktion zur Unterstützung der Afrikanischen Union bei der Sicherstellung von Sicherheit und Ordnung im Osten SARUNIAs, insbesondere der Flüchtlingslager;
– eine Polizeimission mit Schwerpunkt Grenzmanagement;
– eine Justizkomponente mit Schwerpunkt Beratung bei Gerichtswesen und Strafvollzug;
– eine Zivilschutzkomponente in Bezug auf die Ölverseuchung;
– eine humanitäre Unterstützung für die Flüchtlingslager;
– eine Reaktion auf einen Cyberzwischenfall (Diebstahl von Email-Informationen) in der EU-Delegation in SARUNIA sowie
– eine Evakuierung von EU-Bürgern.

7. Auf welche Art und Weise sind nach Kenntnis der Bundesregierung „Cyberkrisen“ in der Übung vorgesehen, die „katastrophale Auswirkungen haben oder auf einem Terroranschlag beruhen“, sodass die „Solidaritätsklausel“ zu ihrer Beantwortung greifen könnte und die EU bzw. die Mitglied-

staaten dann auch geheimdienstliche oder militärische Mittel bereithält (Bundestagsdrucksache 18/2674)?

In ML14 sind keine „Cyberkrisen“ vorgesehen, die zu ihrer Beantwortung einen Rückgriff auf die „Solidaritätsklausel“ erforderlich machen. Im Übrigen wird auf die Antworten zu den Fragen 5 und 6 und die Vorbemerkung der Bundesregierung verwiesen.

8. Welche EU-Mitgliedstaaten oder sonstigen Staaten bzw. welche Einrichtungen der EU sind nach Kenntnis der Bundesregierung an der Durchführung der zweiten „Multi-Layer“-Krisenübung „ML14“ beteiligt?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

9. Mit welchen konkreten Maßnahmen sind nach Kenntnis der Bundesregierung die EU-Mitgliedstaaten oder sonstigen Staaten bzw. Einrichtungen der EU an „Multi-Layer“-Krisenübung „ML14“ beteiligt, und wo wurden diese vorgehalten bzw. eingesetzt?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

10. Was ist aus Sicht der Bundesregierung das Ziel der „Multi-Layer“-Krisenübung „ML14“?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Wann und wo soll die „Multi-Layer“-Krisenübung „ML14“ nach Kenntnis der Bundesregierung ausgewertet werden?

Die Übungsauswertung erfolgt in Brüssel im Rahmen eines mehrstufigen Prozesses unter Einbeziehung der Übungsteilnehmer. Der Abschlussbericht soll voraussichtlich Anfang Januar 2015 dem Politischen und Sicherheitspolitischen Komitee vorgelegt werden.

12. Worin besteht die Rolle des EAD innerhalb der „Multi-Layer“-Krisenübung „ML14“?

Der Europäische Auswärtige Dienst ist einerseits verantwortlich für die Vorbereitung, Durchführung und Auswertung der Übung, andererseits aber auch Übungsteilnehmer. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

13. Worin besteht die Rolle der Europäischen Kommission innerhalb der „Multi-Layer“-Krisenübung „ML14“?

Die Europäische Kommission ist einerseits beteiligt an der Vorbereitung, Durchführung und Auswertung der Übung, andererseits aber auch Übungsteilnehmer. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

14. Auf welche Weise soll das Political and Security Committee (PSC) der EU die Übung „politisch kontrollieren“?

Das Politische und Sicherheitspolitische Komitee nimmt im Rahmen der Übung die ihm gemäß Artikel 38 des Vertrages über die Europäische Union zukommende politische Kontrolle und strategische Leitung von Krisenbewältigungsoperationen wahr, verfolgt die internationale Lage in den Bereichen der Gemeinsamen Außen- und Sicherheitspolitik und trägt auf Ersuchen des Rates, der Hohen Vertreterin oder von sich aus durch an den Rat gerichtete Stellungnahmen zur Festlegung von Politiken bei. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

15. Auf welche Weise und nach welchen Kriterien legt das PSC die strategische Ausrichtung der Übung fest?

Das Politische und Sicherheitspolitische Komitee bestimmt die strategische Ausrichtung der Übung durch seine Befassungen mit der Übungsspezifikation und den Übungsanweisungen. Die dabei zur Anwendung gelangenden Kriterien sind die der Mitgliedstaaten, die in allen Befassungen ihre jeweiligen Positionen einbringen können.

16. Was ist der Bundesregierung über die Rolle des militärischen Kommandozentrums in Italien sowie dem Hauptquartier der „EU Battlegroup“ in Belgien bekannt, die laut dem EAD als Lagezentren dienen?

Das Übungs-Operationshauptquartier in Italien und das Übungs-Truppenhauptquartier in Belgien nehmen ihre jeweiligen Rollen als Hauptquartiere im Planungsprozess einer militärischen EU-Operation gemäß EU-Krisenmanagementverfahren wahr. Da bei ML14 insbesondere ein beschleunigtes Entscheidungsverfahren (sog. Fast Track) geübt werden soll, besteht die Hauptaufgabe in Erstellung und Abstimmung des Operationsplanes für eine schnelle militärische Reaktion zur Unterstützung der Afrikanischen Union bei der Sicherstellung von Sicherheit und Ordnung im Osten SARUNIAs, insbesondere der Flüchtlingslager. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

17. Wo genau sind die Zentren nach Kenntnis der Bundesregierung angesiedelt, und welche Mitgliedstaaten haben hierzu Verbindungsbeamtinnen bzw. Verbindungsbeamte entsandt?

Das Übungs-Operationshauptquartier wird durch das italienische Joint Operations Headquarters, Centocelle Airport, Rom, gestellt. Das Verstärkungspersonal stammt aus Österreich, Belgien, Deutschland, Spanien, Finnland, Frankreich, Ungarn, Litauen, den Niederlanden, Polen und Schweden.

Das Übungs-Truppenhauptquartier wird durch das Hauptquartier der belgischgeführten EU-Battlegroup 2014-2 in Leopoldsburg (Nähe Brüssel) in Belgien dargestellt. Das Verstärkungspersonal stammt aus den Niederlanden, Luxemburg, Spanien und Deutschland.

18. Aus welchen Einheiten oder Abteilungen stammten diese Verbindungsbeamtinnen bzw. Verbindungsbeamten nach Kenntnis der Bundesregierung jeweils?

Zu den Dienststellen des Verstärkungspersonals anderer Mitgliedstaaten der Europäischen Union liegen der Bundesregierung keine Informationen vor. Das

deutsche Verstärkungspersonal des Übungs-Operationshauptquartiers in Italien stammt aus dem Sanitätslehrregiment, dem Lazarettregiment 11 und der Marineortungsschule. Im Übungs-Truppenhauptquartier stammt das deutsche Personal aus dem Zentrum Luftoperationen und aus dem Bereich Kommando Streitkräftebasis.

19. Wie genau wurde bzw. wird auf die Simulation einer „Bedrohung“ der Stadt „Batela“ durch einen „Cyber-Angriff“ geantwortet?

Eine Bedrohung der Stadt BATELA durch einen Cyber-Angriff ist nicht Bestandteil des ML14-Szenarios. Im Übrigen wird auf die Antwort zu Frage 6 verwiesen.

20. Welche zivilen Einheiten bzw. militärischen Stäbe welcher Mitgliedstaaten der EU oder sonstigen Staaten sind nach Kenntnis der Bundesregierung mit welchen Abteilungen mit der Beantwortung des „Cyber-Angriffs“ befasst?

Es wird auf die Antwort zu Frage 19 verwiesen.

21. Was ist der Bundesregierung über Teilnehmende und die Tagesordnung des „EU-US Cyber-Dialogue“ Anfang Dezember 2014 in Brüssel bekannt, und auf welche Weise werden welche Bundesbehörden dort teilnehmen?

Der EU-US-Cyberdialog ist Teil der vom EAD vorangetriebenen „EU-Cyberdiplomatie“. Inhaltlich steht bei diesen Dialogen der EU mit Drittstaaten der Austausch über Cyberpolitiken Dritter im Vordergrund. Teilnehmerkreis und Tagesordnung für den EU-US-Cyberdialog im Dezember 2014 sind derzeit noch nicht bekannt. Die Mitgliedstaaten werden aber in der Ratsarbeitsgruppe COTRA sowie in der Gruppe „Freunde der Präsidentschaft CYBER“ in den kommenden Wochen hiermit befasst. Die Bundesregierung ist bei diesen Dialogen regelmäßig über die Ständige Vertretung als Beobachter vertreten.

22. Was ist der Bundesregierung über Teilnehmende und die Tagesordnung der „Cyber Week“ im September 2014 in Israel bekannt, und welche Bundesbehörden haben mit welchen Zielsetzungen und/oder Aufgaben dort teilgenommen?

Bei der diesjährigen „Cyber Week“ präsentierte sich Israel mit hochrangig besetzten Konferenzen, der Einweihung eines neuen Forschungszentrums an der Tel Aviv University und der Vorstellung eines neuen High-Tech-Campus in Ber-Sheeva als Land, das Cybersicherheit als strategische Priorität behandelt. Tagesordnung und Redner sind auf der Webseite des israelischen Außenministeriums einsehbar (http://mfa.gov.il/MFA/InnovativeIsrael/Conferences/Pages/National-Cyber-Week-2014.aspx).

Insgesamt nahmen etwa 3 000 Personen aus 40 Ländern teil. Die „Cyber Week“ 2014 diente neben der offenen Diskussion über sicherheitspolitische Ansätze auch der Nachwuchsgewinnung für Informatik-Studenten und der Standortwerbung. Die Bundesregierung war vertreten durch den Leiter des Koordinierungsstabs Cyber-Außenpolitik im Auswärtigen Amt.

23. Inwiefern bzw. wozu hat Israel nach Kenntnis der Bundesregierung im Anschluss an die Konferenz Interesse an weiteren Zusammenarbeitsformen mit der EU hinsichtlich Cybersicherheit geäußert?

Der Bundesregierung ist nicht bekannt, inwiefern bzw. wozu Israel Interesse an weiteren Zusammenarbeitsformen mit der EU hinsichtlich Cybersicherheit geäußert hat.

24. Wer gehört nach Kenntnis der Bundesregierung dem „Exercise Planning Team“ der IPCR der EU an (Bundestagsdrucksache 18/2674)?

Im Vorfeld der ersten Sitzung des Planungsteams am 17. Juli 2014 haben sich die folgenden Mitgliedstaaten angemeldet: Österreich, Belgien, Zypern, Finnland, Frankreich, Griechenland, Irland, Italien, Niederlande, Rumänien, Schweden. Bei der zweiten Sitzung des Planungsteams am 22. September 2014 nahmen neben Europäischer Kommission, EAD und Ratssekretariat die Mitgliedstaaten Belgien, Finnland, Ungarn, Griechenland, Rumänien und Schweden teil.

25. Wann und wo soll die Übung nach derzeitigem Stand nach Kenntnis der Bundesregierung abgehalten werden?

Die Übung soll am 27. November 2014 in Brüssel stattfinden. Es wurde am 14. Oktober 2014 in der Sitzung der „Gruppe der Freunde der Präsidentschaft zum EU-Krisenreaktionsmechanismus (ICPR) und zur Umsetzung der Solidaritätsklausel“ präzisiert, dass es sich um eine „working group exercise“ handle, bei der die Mitglieder der Gruppe den neuen EU-Krisenreaktionsmechanismus auf EU-Ratsebene im Rahmen eines Workshops üben. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

26. Auf welche konkrete Art und Weise hat sich die Bundesregierung in die Planung und Vorbereitung der Übung eingebracht?

Die Bundesregierung hat sich nicht an den Planungen beteiligt.

27. Auf welche Art und Weise sind nach Kenntnis der Bundesregierung „Cyberkrisen“ in der Übung vorgesehen, die „katastrophale Auswirkungen haben oder auf einem Terroranschlag beruhen“ sodass die „Solidaritätsklausel“ zu ihrer Beantwortung greifen könnte und die EU bzw. die Mitgliedstaaten dann auch geheimdienstliche oder militärische Mittel bereithält (Bundestagsdrucksache 18/2674)?

Im Workshop wird für die Auslösung des IPCR ein fiktives Cyber-Szenario zugrunde gelegt. Für den Mechanismus ist die Natur der auslösenden Krise an sich unerheblich. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

28. Inwiefern wird nach Kenntnis der Bundesregierung auch eine „Unterstützung bei der Folgenbeseitigung“ geprobt, nachdem „durch den Ausfall von IT-Systemen“ gravierende Folgen aufgetreten sind?

Bei dem Workshop wird keine Unterstützung bei der Folgenbeseitigung geprobt. Den Mitgliedern der IPCR wird im Rahmen der Übung Gelegenheit gegeben, Fragen zur Krisenbewältigung nach Aktivierung des IPCR zu klären. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

29. Inwiefern und mit welchem Ergebnis hat sich die Bundesregierung mittlerweile zwischen dem BMI und dem AA zu den Formen der Teilnahme an der IPCR-Übung abgestimmt?

Die detaillierte Klärung der Teilnahme steht noch aus. Den Anregungen aus dem Planungsteam der Übung folgend wurde bislang die Teilnahme des deutschen Vertreters in der „Gruppe der Freunde der Präsidentschaft zum IPCR“ am Workshop bestätigt.

30. Welche Abteilungen des BMI und des AA sind an der Abstimmung beteiligt?

Die Entscheidung über eine Teilnahme wird von der Europaabteilung im Auswärtigen Amt in Abstimmung mit dem Krisenreaktionszentrum des Auswärtigen Amtes und mit der Abteilung Krisenmanagement und Bevölkerungsschutz sowie IT des Bundesministeriums des Innern getroffen.

31. Sofern noch keine Entscheidung getroffen worden ist, wann wird diese erwartet?

Eine Entscheidung über die Teilnahme soll zeitnah getroffen werden.

32. Welche Haltung vertritt die Bundesregierung zur Frage, in welchem Fall bei „Cyberangriffen“ eine Beistandspflicht im Rahmen der NATO oder auch der „Solidaritätsklausel“ gegeben wäre, die auch militärische Mittel einschließen könnte?

„Cyberangriffe“ können ein Ausmaß erreichen, das Wohlstand, Sicherheit und Stabilität in den Mitgliedstaaten der NATO gefährdet. Eine Entscheidung, wann ein „Cyberangriff“ den kollektiven Beistand nach Artikel 5 des Nordatlantikvertrages auslöst und welche Maßnahmen gegebenenfalls zu ergreifen sind, trifft der Nordatlantikrat im Einzelfall. Die „Solidaritätsklausel“ (Artikel 222 Absatz 1 AEUV) legt fest, dass die EU und ihre Mitgliedstaaten gemeinsam im Geiste der Solidarität handeln, wenn ein Mitgliedstaat von einem Terroranschlag, einer Naturkatastrophe oder einer vom Menschen verursachten Katastrophe betroffen ist. Bei einem „Cyberangriff“ müsste im Einzelfall konkret geprüft werden, ob die Voraussetzungen gegeben sind.

33. Auf welche Weise werden die Übung „ML14“ sowie die IPCR-Übung in ihrer simulierten Beantwortung verschiedener Szenarien nach Kenntnis der Bundesregierung berücksichtigen, dass etwaige „Angriffe“ von Militärs oder Geheimdiensten anderer Staaten ausgeführt worden sein könnten, für deren „Beantwortung“ mit militärischen Mitteln dann aber ein Mandat etwa des UN-Sicherheitsrates oder anderer internationaler Organisationen erforderlich wäre?

Weder bei ML14 noch bei der IPCR-Übung sind derartige Szenarien vorgesehen. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

34. Welche weiteren Veranstaltungen von „Cyber Europe 2014“ sind in diesem und im nächsten Jahr (inklusive Auswertung) geplant, und auf welche Weise bringen sich welche Bundesbehörden dort ein?

Die nächste Veranstaltung ist die zweite Phase der Übung „Cyber Europe 2014“, die Ende Oktober 2014 stattfinden soll. An dieser Übung sowie der Auswertung beabsichtigt das Bundesamt für Sicherheit in der Informationstechnik teilzunehmen. Für eine dritte Phase der Übung wurden erste Vorüberlegungen durch die Europäische Agentur für Netz- und Informationssicherheit angestellt. Im Übrigen wird auf die Antwort zu Frage 38a der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/164 vom 12. Dezember 2013 verwiesen.

35. Welche Berichte werden zur „Cyber Europe 2014“ erstellt, und wem sind diese zugänglich?

Die „Cyber Europe 2014“ wird federführend von der Europäischen Agentur für Netz- und Informationssicherheit geplant. Diese legt fest, welche Berichte erstellt und wie diese zugänglich gemacht werden. Die Berichte zu „Cyber-Europe“-Übungen wurden bislang öffentlich zugänglich gemacht.

36. Welche weiteren Übungen sollen nach Kenntnis der Bundesregierung in den Jahren 2014 und 2015 stattfinden, die „Cyberstörungen“ zum Inhalt haben oder haben könnten, wo werden diese abgehalten, und wer wird bezüglich der Teilnahme adressiert?

Die Übung Cyber Coalition der NATO findet 2014 und 2015 in Tartu, Estland, statt.

Der jeweilige Durchführungsort wird durch die NATO festgelegt. Die Teilnehmer kommen überwiegend aus den sich mit der Thematik beschäftigenden Bereichen der NATO-Kommandostruktur, ergänzt durch nationale Experten.

37. Welche Behörden und/ oder Firmen bzw. Institute haben im Januar 2014 an einem Arbeitstreffen des Bundeskriminalamtes zum „Projekt Hacktivismus“ teilgenommen (www.bdk.de/lv/nordrhein-westfalen/bv/koeln/blickpunkt/blickpunkt-1-2014/hacktivismus)?

Neben Vertretern des BKA nahmen am Arbeitstreffen im Januar 2014 Vertreter folgender Behörden teil:

- Zentralstelle zur Bekämpfung der Internetkriminalität (Generalstaatsanwaltschaft Frankfurt a. M.)
- Bundesamt für Verfassungsschutz
- Bundesministerium der Verteidigung
- Landeskriminalamt Niedersachsen
- Polizeipräsidium Aachen
- Polizeipräsidium Köln
- Polizeipräsidium Düsseldorf.

a) Wie soll das Ziel, „empirisch fundierte, kriminalistisch-kriminologische Erkenntnisse zum Phänomen zusammenzutragen“, konkret umgesetzt werden?

Zur Umsetzung wurde das Ziel in drei Bausteine untergliedert: Die Erstellung einer Basis-Phänomenologie, die Darstellung von Szene-Trends sowie die Feststellung von Tätertypologien. Methodisch wurde hierzu eine auf bundesweiten Falldaten basierende Fallanalyse durchgeführt sowie eine Sekundäranalyse deutsch- und englischsprachiger Literatur. Daneben erfolgt eine Untersuchung des Dunkelfeldes.

b) Welche Daten „zur Vorgehensweise und zu Verschleierungstechniken sowie zur Infrastruktur bezüglich der Kommunikation, Logistik und Timing“ wurden erhoben bzw. verarbeitet?

Im Rahmen der Sekundäranalyse wurden entsprechende Quellen in Form von Büchern, Berichten, Studien und Artikeln ausgewertet. Die Falldatenanalyse basierte auf einer bundesweit angelegten Abfrage relevanter Fälle bei Polizeidienststellen und Staatsanwaltschaften sowie der am Nationalen Cyber-Abwehrzentrum Beteiligten. Die Fallakten wurden anonymisiert im Rahmen eines Erhebungsbogens ausgewertet und statistisch aufbereitet. Im Rahmen der Medienrecherche werden öffentlich zugängliche Bereiche des Internets gesichtet, um Erkenntnisse zu möglicher Kommunikation, Organisation, Infrastruktur und Motivation zu generieren.

c) Welche „Trendwechsel, aktuelle Szenedynamiken, Schäden“ wurden in diesem Zusammenhang betrachtet?

Nachdem in den 90er-Jahren vereinzelt erste hacktivistische Bestrebungen und organisierte Gruppierungen – insbesondere motiviert von weltweiter Informationsfreiheit im Internet – beobachtet werden konnten, steigerte sich die hacktivistische Bewegung nach 2010 merklich. Szenedynamisch war eine Entwicklung zu dezentralen anonymen Interessengemeinschaften im Sinne loser Kollektive zu beobachten. Geschädigte können zielgerichtet ideologische Gegner der Hacktivisten, aber auch unbeteiligte Nutzer des Internet werden. Über Schäden kann derzeit keine Aussage getroffen werden.

d) Welche „erste[n] Erkenntnisse zum bislang phänomenologisch, statistisch und rechtlich wenig erforschten Phänomen“ wurden „zusammengetragen, ausgewertet und aufbereitet“?

Auf Grundlage der erhobenen Informationen wurde das Phänomen Hacktivismus wie folgt definiert: „Der Begriff Hacktivismus beinhaltet die Konzepte Hacking und Aktivismus: Das Nutzen von Hacking- bzw. von Informations- und Kommunikationsinstrumenten für die Verdeutlichung und Durchsetzung bestimmter politischer wie sozialer Ziele (Ideologien) bildet die Schnittmenge beider Konzepte. Die Hacking-Tools werden hierbei u. a. für Protest- und/oder Propagandazwecke eingesetzt und sind nicht profitorientiert, d. h. hacktivistische Taten zielen nicht darauf ab, illegal materielle und finanzielle Gewinne zu erzielen“. Außerdem wurden Grundlagen für eine statistische und rechtliche Bewertung Phänomens gelegt. Eine abschließende Würdigung der Ergebnisse wird erst nach Vorlage des Abschlussberichts möglich sein, der Mitte 2015 erwartet wird. Im Übrigen wird auf die Antworten zu den Fragen 37a bis 37c verwiesen.

e) Welche „mehr als 180 relevante[n] hacktivistische[n] Einzelfälle und -vorgänge“ wurden zugeliefert und verarbeitet?

Die Falldatenabfrage erbrachte insgesamt 183 Rückläufer von Polizei und Staatsanwaltschaften. 72 Akten wurden von den Polizeidienststellen zugeliefert, 111 von den Staatsanwaltschaften, von denen wiederum 106 Akten einem Sammelverfahren zuzuordnen waren.

f) Durch welche Maßnahmen soll aus Sicht des Bundeskriminalamtes ein „relevante[r] Strafrahmen noch besser ausgeschöpft werden“?

Konkrete Maßnahmen zur Ausschöpfung des Strafrahmens zu benennen, fällt nicht in die Zuständigkeit des Bundeskriminalamts.

g) Auf welche Weise wird nach „der Befassung mit dem phänomenologischen Hellfeld des Hacktivismus“ in der weiteren Folge des „Projektes Hacktivismus“ außer durch „Medienrecherchen und Unternehmensbefragungen“ das „Dunkelfeld beleuchtet werden“?

Nach methodischer Abwägung von weiteren Maßnahmen wie Täterbefragungen oder teilnehmenden Beobachtungen zur Untersuchung des Dunkelfeldes wurde entschieden, ausschließlich auf die Unternehmensbefragung und Medienrecherche zurückzugreifen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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