Deutscher Bundestag **Drucksache 17/11100**

17. Wahlperiode 18. 10. 2012

Kleine Anfrage

der Abgeordneten Andrej Hunko, Herbert Behrens, Ulla Jelpke, Dr. Petra Sitte, Kathrin Vogler und der Fraktion DIE LINKE.

Gemeinsame internationale Übung „Cyber Europe 2012“ mit Behörden, Banken und Internetdienstleistern

Am 4. Oktober 2012 hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zum zweiten Mal die Übung „Cyber Europe“ ausgerichtet. Im Gegensatz zur gleichnamigen Übung 2010 sollen diesmal auch „Experten von Großbanken, Telecom-Unternehmen und Internetprovidern“ auf einen fiktiven Cyberangriff reagieren (heise.de, 4. Oktober 2012). 60 Banken waren beteiligt. 25 Länder haben an der Übung teilgenommen, vier weitere waren als Beobachter präsent. Ziel war die Erprobung und Zusammenschaltung nationaler und europäischer Cyberinfrastrukturen der Behörden und Telekommunikationsanbieter. Laut einer Mitteilung von ENISA sei die diesjährige Übung gegenüber 2010 in ihrem Ausmaß ebenso wie in ihrer Komplexität gewachsen (www.enisa.europa.eu/media/news-items/cyber-europe-2012-2013-first-results-show-success). Weitere Ziele werden mit „Testeffektivität und Skalierbarkeit der existierenden Mechanismen, Methoden und des Informationsflusses für die Kooperationen öffentlicher Behörden in Europa“ angegeben. Zudem sollen „Sicherheitslücken und Herausforderungen für einen effektiveren Umgang mit umfangreichen Internetstörfällen“ gefunden werden. Als Szenario wurde eine gezielte „Distributed Denial of Service“-Offensive auf „Online-Dienste in allen teilnehmenden Ländern“ angenommen, die durch weitere „ernsthafte Bedrohungen“ angereichert wurde. Derart protestiert etwa die Aktivistengruppe „Anonymous“ regelmäßig gegen nationale oder internationale Behörden und Firmen. Insgesamt wurden laut ENISA mehr als 1 000 als „Injektionen“ bezeichnete „Internetstörungen“ simuliert.

In Veröffentlichungen der ENISA findet sich kein Hinweis auf die weitere Zusammenarbeit mit den USA, die auch dieses Jahr Teile ihrer regelmäßigen Übung „Cyber Storm“ ausgeführt hatten. Auf Fragen zur Beteiligung deutscher Stellen an den zivil-militärischen Inhalten und Akteuren hatte die Bundesregierung mit dem Textbaustein „An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, haben keine militärischen Stellen teilgenommen“ geantwortet (Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/7578). In der Auswertung der Übung „Cyber Storm III“ wurde verabredet, zukünftig weitere gemeinsame Übungen mit Mitgliedstaaten der EU abzuhalten. Dazu wurde eine „High-level EU-US Working Group on cyber security and cybercrime“ eingerichtet. Unter anderem hat die Arbeitsgruppe 2011 eine Übung der EU und der USA „Cyber Atlantic“ ausgerichtet.

Wir fragen die Bundesregierung:

1. Welche europäischen Länder waren an der „Cyber Europe 2012“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?
   a) Welche weiteren Stellen des öffentlichen und privaten Bereichs waren beteiligt (bitte insbesondere die beteiligten Firmen und Banken aufführen)?
   b) Welche Aufgabe erfüllte das zentrale Lagezentrum der ENISA in Athen?
   c) Inwieweit waren die „Computer Emergency Response-Teams“ (CERT) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundeswehr in die Übung eingebunden?
   d) Welche weiteren CERT waren mit welchen Aufgaben integriert?
   e) Welche Aufgaben übernahm das CERT der EU?
2. Mit welchem Ziel haben deutsche Behörden an der Übung „Cyber Europe 2012“ teilgenommen?
   a) Mit welchen Kräften waren öffentliche und private Teilnehmer aus Deutschland beteiligt?
   b) Worin bestand der Beitrag der Bundesnetzagentur bei der Übung?
   c) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?
3. Wie war die Übung strukturell angelegt?
   a) Welche Szenarien wurden für die Übung angenommen und durchgespielt?
   b) Worin bestanden die über 1 000 „Injektionen“?
   c) Inwieweit berücksichtigte die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?
   d) Auf welche Weise wurde den in Frage 3c erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?
4. Wie wurde die „Cyber Europe 2012“ geplant und vorbereitet?
   a) Wer gehörte einer diesbezüglichen Planungsgruppe an, und von wem wurde diese initiiert?
   b) Inwieweit wurden hierzu 2010 und 2012 welche Beratungsunternehmen mit welchen Aufgaben eingebunden?
5. Welches Szenario liegt der diesjährigen „Länderübergreifenden Krisenmanagementübung“ LÜKEX zugrunde?
   a) Wann soll die nächste LÜKEX stattfinden, und wer bereitet diese vor?
   b) Welche Bundesministerien, Bundesbehörden, Hilfsorganisationen, Verbände und Wirtschaftsunternehmen werden daran teilnehmen, und worin besteht ihre Aufgabe?
   c) Welche ausländischen privaten oder öffentlichen Stellen sind in die Übung integriert oder beobachten diese?
   d) Inwieweit berücksichtigt die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?

e) Auf welche Weise wurde den in Frage 5d erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?

6. Welche europäischen Länder waren an der „Cyber Atlantic 2011“ (www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011) aktiv beteiligt, und welche hatten eine beobachtende Position inne?

   a) Welche weiteren Stellen des öffentlichen und privaten Bereichs waren beteiligt (bitte insbesondere die beteiligten Firmen und Banken aufführen)?

   b) Welche Aufgaben übernahmen die ENISA und das damals provisorische CERT der EU bzw. vergleichbare Strukturen?

   c) Mit welchem Ziel haben deutsche Behörden an der Übung „Cyber Atlantic 2011“ teilgenommen?

   d) Mit welchen Kräften waren öffentliche und private Teilnehmer aus Deutschland beteiligt?

   e) Worin bestand der Beitrag der Bundesnetzagentur bei der Übung?

   f) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?

7. Wie war die „Cyber Atlantic 2011“ strukturell angelegt?

   a) Welche Szenarien wurden für die Übung angenommen und durchgespielt?

   b) Inwieweit berücksichtigte die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?

   c) Auf welche Weise wurde den in Frage 7b erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?

8. Wie wurde die „Cyber Atlantic 2011“ geplant und vorbereitet?

   Wer gehörte seitens der EU oder ihrer Mitgliedstaaten einer diesbezüglichen Planungsgruppe an, und welche Aufgaben wurden hierfür übernommen?

9. Welche (auch virtuellen) Treffen der Unterarbeitsgruppe „Cybercrime“ des „EU-/US-Senior- Officials-Treffen“ hat es 2012 gegeben, und welchen Inhalt hatten diese?

10. Welche Regierungen von EU-Mitgliedstaaten sowie anderer Länder waren 2012 (auch als Beobachter) an Aktivitäten der US-Übung „Cyberstorm“ beteiligt (auch an etwaigen Auswertungen), die laut dem „Department of Homeland Security“ auch dieses Jahr andauert (www.dhs.gov/cyber-storm-securing-cyber-space)?

    a) Welche US-Ministerien bzw. -Behörden waren dieses Jahr an „Cyberstorm“ beteiligt?

    b) Wie viele Angehörige welcher deutscher Behörden haben an welchen Standorten an den Aktivitäten zu „Cyberstorm“ teilgenommen?

    c) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden?

d) Was ist damit gemeint, wenn die Bundesregierung für 2010 von einer „dislozierte[n] Stabrahmenübung mit einem ‚Computerwurm'-Szenario" spricht (vgl. Bundestagsdrucksache 17/7578)?

11. Wie war das Verhältnis von zivilen zu staatlichen Akteuren bei Aktivitäten zu „Cyberstorm" in diesem Jahr?

a) Welche privaten Firmen bzw. sonstigen zivilgesellschaftlichen Akteure haben daran teilgenommen?

b) Wie bewertet die Bundesregierung die Trennung bei „Cyberstorm" in einen militärischen und einen nicht-militärischen „Strang" hinsichtlich einer Trennung polizeilicher und militärischer Belange?

Berlin, den 18. Oktober 2012

Dr. Gregor Gysi und Fraktion

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