Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1117
FAX +49 (0)30 18 681-1019

INTERNET www.bmi.bund.de
DATUM 28. April 2011

BETREFF **Kleine Anfrage der Abgeordneten Petra Pau u. a. und der Fraktion DIE LINKE.**
Die Strategie der Bundesregierung zur Bekämpfung der Internet-Kriminalität - Das Nationale Cyber-Abwehrzentrum
BT-Drucksache 17/5560

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte Antwort in 5-facher Ausfertigung.

In Vertretung

Rogall-Grothe

Cornelia Rogall-Grothe

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
VERKEHRSANBINDUNG S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Kleine Anfrage der Abgeordneten Petra Pau u. a. und der Fraktion DIE LINKE.

Die Strategie der Bundesregierung zur Bekämpfung der Internet-Kriminalität - Das Nationale Cyber-Abwehrzentrum

BT-Drucksache 17/5560

---

1. Welche genauen tatsächlichen Sachverhalte und Vorkommnisse sowie eventuell offenbar geworden Schwächen in der bisherigen Arbeit der Sicherheitsbehörden haben dazu geführt, dass ein Nationales Cyber-Abwehrzentrum am 01. April 2011 seine Arbeit aufnehmen soll? (Bitte für die einzelnen Behörden, Gremien und Kooperationseinrichtungen gesondert darstellen)

Zu 1.

Die Cyber-Sicherheitsstrategie der Bundesregierung einschließlich der Einrichtung eines Nationalen Cyber- Abwehrzentrums ist eine kontinuierliche Weiterentwicklung der bisherigen IT-Sicherheitspolitik und IT-Sicherheitsaktivitäten. Hochkomplexe Angriffe wie Stuxnet orientieren sich nicht entlang von Behördenzuständigkeiten. Ein intensiverer Informationsaustausch zwischen den Behörden ist erforderlich.

2. Auf welcher gesetzlichen Grundlage soll dieses Nationale Cyber-Abwehrzentrum arbeiten und ist hierfür – nach Ansicht der Bundesregierung - ein eigenes Errichtungsgesetz oder eine Errichtungsanordnung (falls vorhanden bitte der Antwort beifügen) erforderlich und wenn nein, warum nicht?

Zu 2.

Das Cyber-Abwehrzentrum ist keine eigenständige Behörde, weswegen eine gesetzliche Grundlage entbehrlich ist. Die Grundlage der Zusammenarbeit sind Kooperationsvereinbarungen. Die beteiligten Behörden arbeiten hierbei unter strikter Wahrung ihrer Aufgaben und gesetzlichen Befugnisse zusammen. Aus diesem Grund ist auch ein Errichtungsgesetz nicht notwendig.

3. Aufgrund welcher sonstigen Verwaltungsvereinbarung wurde das Nationale Cyber-Abwehrzentrum dann errichtet (die Dokumente, Vereinbarungen etc. bitte der Antwort beifügen)?

Zu 3.

Wie in der vom Bundeskabinett am 23. Februar 2011 verabschiedeten Cyber-Sicherheitsstrategie für Deutschland benannt, sind Kooperationsvereinbarungen Grundlage für die Zusammenarbeit.

4. Welche Behörden sollen in dem Nationalen Cyber-Abwehrzentrum mit wie vielen Personen ständig arbeiten und welche Ad-hoc-Assoziationen sind denkbar?

Zu 4.

Die Kernbehörden (Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Verfassungsschutz, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) sind ständig im Cyber-Abwehrzentrum vertreten. Sie stellen insgesamt 10 Mitarbeiter (BSI: 6 MA, BfV: 2 MA, BBK: 2 MA). Bundeskriminalamt, Bundespolizei, Zollkriminalamt, Bundesnachrichtendienst, Bundeswehr (alle assoziierten Behörden) sowie die aufsichtsführenden Stellen über die Betreiber der Kritischen Infrastrukturen werden unter Wahrung ihrer gesetzlichen Aufgaben und Befugnisse ebenfalls mitwirken. Die assoziierten Behörden werden über Verbindungsbeamte regelmäßig und anlassbezogen eingebunden.

5. Wie ist die Kooperation der unterschiedlichen Behörden im Nationalen Cyber-Abwehrzentrum konkret geregelt (bitte eventuelle Kooperationsvereinbarungen der Antwort beilegen)?

Zu 5.

Die Kooperationsvereinbarungen regeln die Zusammenarbeit. Die trilaterale Kooperationsvereinbarung der unter Frage 4 genannten Kernbehörden ist bereits geschlossen. Die bilateralen Kooperationsvereinbarungen mit den assoziierten Behörden (siehe Frage 4) befinden sich noch in der Abstimmung.

6. Wie sollen die Arbeit und die Arbeitsabläufe des Zentrums konkret aussehen?

Zu 6.

Das Cyber-Abwehrzentrum ist eine Informationsdrehscheibe und wird den Informations- und Erfahrungsaustausch durch eine institutionalisierte Kooperation optimieren. Alle beteiligten Behörden werden unter strikter Wahrung ihrer Aufgaben und gesetzlichen Be-

fugnisse ihr Fachwissen und ihre Kompetenzen einbringen, um die Cyber-Sicherheit in Deutschland voranzubringen.

7. Wie bewertet die Bundesregierung die verfassungsrechtlichen Probleme der dauerhaften analytischen und operativen Zusammenarbeit zwischen BKA, Bundespolizei, Bundesamt für Verfassungsschutz, Bundesnachrichtendienst (BND), Bundeswehr, Militärischer Abschirmdienst (MAD) und anderen Behörden?

Zu 7.

Im Cyber-Abwehrzentrum findet keine dauerhaft analytische und keine operative Zusammenarbeit statt. Aus Sicht der Bundesregierung bestehen deswegen keine verfassungsrechtlichen Bedenken. (Auf die Antwort zu Frage 4 wird verwiesen).

8. Welche Vorsorge ist in den Verwaltungsvereinbarungen getroffen, um den Persönlichkeitsschutzes, die Meinungsfreiheit, das Recht auf informationelle Selbstbestimmung der Internet-Nutzer zu schützen?

Zu 8.

Die Rechte der Internetnutzer sind durch die Arbeit des Cyber-AZ nicht berührt. Unabhängig davon wird auch in der zwischen den beteiligten Behörden geschlossenen Verwaltungsvereinbarung noch einmal klargestellt, dass durch das Cyber-AZ keine personenbezogenen Daten verarbeitet werden. Sollte ausnahmsweise ein Austausch personenbezogener Daten erforderlich sein, erfolgt er ausschließlich zwischen den jeweils beteiligten Behörden und Stellen auf der Grundlage der für die jeweilige Behörde geltenden Gesetze und Vorschriften.

9. Sind Informationspflichten gegenüber den von Recherchen betroffenen Nutzern des Internets vorgesehen, wenn ja, wie sehen die aus und wenn nein, warum nicht?

Zu 9.

Das Cyber-AZ nimmt keine derartigen Recherchen vor. Auf die Antworten zu Fragen 2 und 8 wird verwiesen.

10. Welche Deliktgruppen der IuK-Kriminalität werden bzw. sollen im Nationalen Cyber-Abwehrzentrum untersucht werden und gibt es besondere Deliktgruppen der IuK-

Kriminalität, die im Nationalen Cyber-Abwehrzentrum ausdrücklich nicht untersucht und bekämpft werden sollen? Wenn ja, aus welchen Gründen sind ihre Untersuchung und Bekämpfung nicht vorgesehen?

Zu 10.

Es werden keine Deliktgruppen der IuK-Kriminalität im Cyber-Abwehrzentrum untersucht. Diese Aufgabe obliegt den hierfür zuständigen Polizeibehörden.

11. Welche Schwachstellen bei welchen IT-Produkten und bei welchen IT-Vorfällen sollen im Nationalen Cyber-Abwehrzentrum untersucht werden und besteht das Nationale Cyber-Abwehrzentrum darauf, von den Software-Firmen über sog. Backdoors, d.h. absichtlich implementierte Sicherheitslücken informiert zu werden?

Zu 11.

Das Cyber-Abwehrzentrum beschäftigt sich mit Schwachstellen und deren Auswirkungen auf die Verfügbarkeit der Informations- und Kommunikationstechnik sowie die Integrität, Authentizität und Vertraulichkeit der sich darin befindenden Daten. Das Cyber-Abwehrzentrum verfügt über kein Mandat gegenüber Herstellern.

12. Wie wird sich die Zusammenarbeit des Nationalen Cyber-Abwehrzentrum mit dem Bundesministerium für Wirtschaft und Technologie gestalten und welchen Anteil hatte dieses Bundesministerium an der Entwicklung des Konzepts und der Umsetzung des Nationalen Cyber-Abwehrzentrums?

Zu 12.

Eine Zusammenarbeit ist nicht vorgesehen.

13. Wie soll die Zusammenarbeit zwischen dem Nationalen Cyber-Abwehrzentrum und den Organisationen und Verbänden der Wirtschaft gestaltet werden, wie z.B. dem Hightech-Verband BITKOM, dem Bundesverband der deutschen Industrie und anderen?

Zu 13.

Eine Einbindung der Wirtschaft in das Cyber-AZ erfolgt mittelbar. Bereits bestehende Strukturen der beteiligten Behörden zur Wirtschaft wie beispielsweise im UP KRITIS sollen genutzt und konsequent ausgebaut werden.

14. In welchen Räumlichkeiten bei welcher Sicherheitsbehörde soll das Nationale Cyber-Abwehrzentrum zukünftig untergebracht werden?

Zu 14.
Das Cyber-Abwehrzentrum ist beim federführenden Bundesamt für Sicherheit in der Informationstechnik in Bonn untergebracht.

15. Wird das Nationale Cyber-Abwehrzentrum über eine eigene Datei verfügen, und welche nationalen und internationalen Behörden sollen hierauf welche Art von Zugriff (schreibend, lesend, automatisiert – bitte auflisten) haben können?

Zu 15.
Nein.

16. Wem sollen die im Nationalen Cyber-Abwehrzentrum erstellten Lagebilder zur Verfügung gestellt werden und wer sind die Aufsichtsbehörden der kritischen Infrastrukturen (bitte auflisten) und wie soll die Kooperation mit diesen im Nationalen Cyber-Abwehrzentrum aussehen?

Zu 16.
Die Lagebilder werden insbesondere für den Cyber-Sicherheitsrat bzw. die Bundesregierung und die beteiligten Behörden erstellt.
Die zu beteiligenden Aufsichtsbehörden, die zum großen Teil in Länderzuständigkeit sind, sind noch zu bestimmen. Die genaue Einbindung wird derzeit noch erarbeitet.

17. Welche genauen Aufgaben (bitte die genaue Aufgabenbeschreibung der Antwort beifügen) hat bzw. soll der Nationale Cyber-Sicherheitsrat im Rahmen seiner koordinierenden Tätigkeit wahrnehmen und welche interne Organisationsstruktur (vergleiche z.B. GTAZ) wird sich der Nationale Cyber-Sicherheitsrat geben?

Zu 17.
Der Nationale Cyber-Sicherheitsrat (Cyber-SR) wird am 3. Mai 2011 zu seiner konstituierenden Sitzung zusammen treten. Dabei wird neben organisatorischen Fragen auch

über die thematische Schwerpunktsetzung und die Anbindung assoziierter Wirtschaftsvertreter beraten werden.

18. Welche genauen Regelungen und Vereinbarungen gibt es für die Tätigkeit des Nationalen Cyber-Sicherheitsrates (bitte der Antwort beifügen)?

Zu 18.
Auf die Antwort zu Frage 17 wird verwiesen.

19. Wie vereinbart die Bundesregierung den Vorsitz im Cyber-Sicherheitsrat durch die Bundesbeauftragte für Informationstechnik, wenn deren Aufgaben bisher sind, „den Service der Verwaltung zu verbessern, Innovationen zu fördern, administrative Handlungsfähigkeit zu bewahren sowie die Effizienz in der Verwaltung zu steigern. Diese Ziele sollen durch effektiven IT-Einsatz erreicht werden."(www.cio.bund.de/DE/Ueber_uns/ueber_uns_node.html)?

Zu 19.
Die Übernahme des Vorsitzes im Cyber-SR durch die Beauftragte der Bundesregierung für Informationstechnik ergibt sich aus der kürzlich beschlossenen Cyber-Sicherheitsstrategie der Bundesregierung und stellt eine logische Weiterentwicklung ihres Aufgabenprofils dar.

20. Welche Personen sind für welche Behörden oder Verbände in dem Nationalen Cyber-Sicherheitsrat vertreten?

Zu 20.
Lt. Ziffer 5 der Cyber-Sicherheitsstrategie sind das Bundeskanzleramt, sowie mit jeweils einem Staatssekretär, die Ressorts Auswärtiges Amt, Bundesministerium des Innern, Bundesministerium der Verteidigung, Bundesministerium für Wirtschaft und Technologie, Bundesministerium der Justiz, Bundesministerium der Finanzen, Bundesministerium für Bildung und Forschung sowie Vertreter der Länder vertreten. Über die Anbindung assoziierter Wirtschaftsvertreter wird der Cyber-Sicherheitsrat in seiner konstituierenden Sitzung beraten.

21. Treffen Medienmeldungen zu, dass diesem Nationalen Cyber-Sicherheitsrat auch „assoziierte Mitglieder" der Wirtschaft angehören sollen, und wenn ja, welche Vertreter sollen dies sein, wer wählt oder bestimmt sie und wem gegenüber sind sie verantwortlich?

Zu 21.
Auf die Antwort zu Frage 17 wird verwiesen.

22. Welche Aufgaben gehören zur Koordinationstätigkeit des Nationalen Cyber-Sicherheitsrats gegenüber dem Nationalen Cyber-Abwehrzentrum und ist damit auch eine Art Weisungsbefugnis verbunden?

Zu 22.
Eine Weisungsbefugnis des Cyber-SR gegenüber dem Nationalen Cyber-Abwehrzentrum (Cyber-AZ) ist schon aufgrund der fehlenden Behördenstruktur nicht gegeben. Auf die Antwort zu Frage 17 wird verwiesen.

23. Wie ist die parlamentarische Kontrolle des Nationalen Cyber-Sicherheitsrates und des Nationalen Cyber-Abwehrzentrums geregelt?

Zu 23.
Es gelten die üblichen Regelungen zur parlamentarischen Kontrollfunktion des Deutschen Bundestags.

24. Treffen Medienmeldungen zu, dass im Falle einer „unmittelbar bevorstehenden oder eingetretenen Krise" ein nationaler Krisenstab eingerichtet wird, und wenn ja, wie sind die Tätigkeit und die Befugnisse dieses Krisenstabes durch welche Richtlinien geregelt (bitte der Antwort beilegen), welche Personen aus welchen Behörden und Einrichtungen sollen in diesem Krisenstab mitarbeiten und wie soll die Tätigkeit des Krisenstabes parlamentarisch kontrolliert werden?

Zu 24.
Im Bundesministerium des Innern wurden personelle, organisatorische und technische Vorkehrungen getroffen, um aus Teilen der Allgemeinen Aufbauorganisation eine Besondere Aufbauorganisation in Form des Krisenstabes des BMI bilden zu können. Für

die in die Ressortzuständigkeit des BMI fallenden besonderen Lagen, koordiniert dieser Krisenstab die betroffenen Ressorts der Bundesregierung und die Maßnahmen der BMI-Geschäftsbereichsbehörden.
Grundlage für diese in die Organisationshoheit der Hausleitung des BMI fallende Organisationsentscheidung ist eine interne BMI-Hausanordnung.

Die Mitglieder des Krisenstabes (Abteilungsleiter des BMI) sowie die Mitarbeiter der verschiedenen Stabsbereiche (UAL, SV, RL, Ref, SB, BSB) stammen aus der AAO des BMI und werden durch Verbindungspersonal der Ressorts und des Geschäftsbereiches ergänzt.

Der Krisenstab wird regelmäßig durch den Sicherheitsstaatssekretär des BMI geleitet, sofern nicht der Minister oder ein anderer Staatssekretär die Leitung übernimmt oder einem zuständigen Fachabteilungsleiter die Leitung übertragen wird. Im Krisenstab wird die ressortübergreifende Expertise gebündelt und eine ressort- und länderübergreifende Koordination von Maßnahmen veranlasst. In den Stabsbereichen des Krisenstabes werden die Organisationeinheiten des BMI nach Schwerpunkten der Aufgabenerfüllung, unabhängig von der Zuordnung in der allgemeinen Aufbauorganisation, zusammengefasst. Die Besetzung der Stabsbereiche kann lage- und bedarfsgerecht erweitert oder reduziert werden.

Die Möglichkeiten der parlamentarischen Kontrolle unterscheiden sich nicht von denen, die in anderen Angelegenheiten bestehen.

25. Wie definiert die Bundesregierung in diesem Zusammenhang eine Situation einer „unmittelbar bevorstehenden Krise" im Vergleich zu einer „eingetretenen Krise" und wer ist für die Feststellung der einen und der anderen mit welchen Befugnissen zuständig?

Zu 25.

Für das Krisenmanagement gibt es erprobte Meldewege, die auch im Falle einer IT-Krise gültig sind. Eine Krise steht dann unmittelbar bevor, wenn aufgrund von konkreten Ereignissen bei ungehindertem Geschehensablauf das Eintreten einer Krise mit hoher Wahrscheinlichkeit anzunehmen ist.

26. Welche Art von Rechenschafts- und Berichtspflichten gibt es für das NCAZ und den Nationalen Cyber-Sicherheitsrat?

Zu 26.

Das Cyber-Abwehrzentrum wird dem Cyber-Sicherheitsrat regelmäßig und anlassbezogen Empfehlungen vorlegen.

27. Treffen Medienmeldungen zu, dass auch eine Task force „IT-Sicherheit in der Wirtschaft" zum 29. März 2011 eingerichtet werden sollte und wenn ja, nach welchen Richtlinien soll diese Task force arbeiten (bitte der Antwort beifügen), welche Vertreter welcher Wirtschaftsverbände und welcher Sicherheitsbehörden sollen in dieser Task force vertreten sein, welche Aufgaben haben sie, wie viele Kosten fallen für diese Task force an, wird diese Task force über eine eigene Datei verfügen und wer soll auf diese Datei Zugriff haben?

Zu 27.

Es ist zutreffend, dass am 29. März 2011 im BMWi eine Task Force IT-Sicherheit in der Wirtschaft eingerichtet worden ist. Für die Arbeit der Task Force ist keine Richtlinie erforderlich. Nachfolgende Wirtschaftsverbände und Sicherheitsbehörden haben sich zu einer Mitarbeit in der Task Force bereit erklärt: ASW, BDI, BITKOM, BVMW, Cio-Circle, DIHK, Eco-Verband, NIFIS, SIBB, TeleTrust, ZDH, ZVEI, BfV und BSI. Die Aufgabe besteht in erster Linie darin, kleine und mittlere Unternehmen für das Thema IT-Sicherheit zu sensibilisieren. Für die Task Force werden nach bisheriger Einschätzung keine nennenswerten Kosten anfallen. Die Task Force wird über keine eigene Datei verfügen.

28. Mit welchen Einrichtungen der EU soll das Nationale Cyber-Abwehrzentrum nach den bisherigen Planungen und Vorgesprächen zusammenarbeiten oder kooperieren?

Zu 28.

Das Cyber-Abwehrzentrum soll mit keinen EU-Einrichtungen unmittelbar zusammenarbeiten oder kooperieren. Bereits bestehende Strukturen der beteiligten Behörden zur EU sollen genutzt und konsequent ausgebaut werden, um die im Cyber-AZ getroffenen gemeinsamen Entscheidungen zu transportieren.

29. Wann wurde das Bundesministerium des Innern durch wen beauftragt, eine „Cyber-Außenpolitik (so zu) gestalten, dass deutsche Interessen in Bezug auf Cybersicherheit in ...der Nato koordiniert und gezielt verfolgt werden" können (Cyber-Sicherheitsstrategie für Deutschland. Hg. BMI)?

30. Wann wurde das BMI von wem aufgefordert, die Nato bei der Erarbeitung einheitlicher Sicherheitsstandards zu unterstützen, die dann „freiwillig" für den Schutz ziviler Kritischer Infrastrukturen übernommen werden sollen (ebda)?

Zu 29 und 30.
Die Cyber-Sicherheitsstrategie für Deutschland wurde am 23.02.2011 vom Bundeskabinett beschlossen. Die zitierten Gestaltungsziele der Strategie richten sich grundsätzlich an die gesamte Bundesregierung im Rahmen der jeweiligen Ressortzuständigkeiten.

31. Welche Vorarbeiten zur Entwicklung dieser einheitlichen Sicherheitsstandards wurden bis heute von der Nato geleistet und inwiefern war das BMI daran beteiligt bzw. in welcher Form hat sich die Befürwortung des Engagements des BMI gegenüber der Nato gezeigt?

32. Seit wann ist die Nato das „Fundament transatlantischer Sicherheit" (ebd.) auch im Bereich ziviler Sicherheit und des Schutzes der deutschen bzw. europäischen Kritischen Infrastrukturen?

Zu 31 und 32.
Mit dem 2010 in Lissabon verabschiedeten strategischen Konzept haben die NATO-Staaten auch das Krisenmanagement sowie die Ertüchtigung der Mitgliedstaaten zur Abwehr von Cyber-Angriffen als Aufgabe und Herausforderung für das Bündnis identifiziert. Vorarbeiten für einheitliche IT-Sicherheitsstandards gibt es bislang nicht.

33. In welcher der beiden Einrichtungen – NCAZ und NCSR – sollen die einheitlichen Nato-Sicherheitsstandards für ihren zivilen Einsatz geprüft werden und welche Nato-Vertreter oder -gremien werden daran teilnehmen?

Zu 33.

Weder im Cyber-Abwehrzentrum noch im Cyber-Sicherheitsrat werden NATO-Sicherheitsstandards für ihren zivilen Einsatz geprüft.

34. Aufgrund welcher Überlegungen, rechtlicher und verfassungsrechtlicher Grundlagen hält es die Bundesregierung für gerechtfertigt, zivile Gremien zu schaffen – NCAZ und NCSR – an denen Bundeswehr und Nato beteiligt sind und die dem Schutz ziviler Strukturen Standards vorgeben sollen, die für den militärischen Bereich entwickelt wurden?

Zu 34.

Durch die Einbindung der Bundeswehr können auch deren Erkenntnisse über Sicherheitslücken und über Angriffswege militärischer Gegner genutzt werden, um höherwertigere technische Empfehlungen zum Schutz der IT der Bundesbehörden und der Kritischen Infrastrukturen geben zu können. Eine Beteiligung der NATO am Cyber-AZ oder NCSR ist nicht geplant.

35. Welche Anstrengungen hat die Bundesregierung bisher unternommen, um für den Schutz Kritischer Infrastrukturen einheitliche zivile Standards zu entwickeln? (Bitte auch die europäische Ebene beachten)

Zu 35.

Die Bundesregierung arbeitet seit einigen Jahren gemeinsam mit Verbänden an der Ergänzung verschiedener fachspezifischer Regelwerke mit dem Ziel, allgemeine Maßnahmen zum Schutz Kritischer Infrastrukturen und zur Erhöhung der Versorgungssicherheit auf dem Wege der Selbstregulierung zu implementieren.
Spezielle Standards zum Schutz auch Kritischer Infrastrukturen im Rahmen der IT-Sicherheit sind die BSI-Standards 101-104; weitere Empfehlungen und Hilfsmittel, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen, finden sich in den IT-Grundschutz-Katalogen.
Den Schutz Kritischer Informationsinfrastrukturen treibt die Bundesregierung seit Jahren gemeinsam mit bedeutenden Betreibern Kritischer Infrastrukturen im Rahmen des UP KRITIS voran.
Überdies wirkt die Bundesregierung in nationalen und internationalen Normungsgremien mit.