Deutscher Bundestag **Drucksache 19/20841**

19. Wahlperiode 06.07.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Ulla Jelpke, Niema Movassat, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/20344 –

Verzögerung des europäischen „Forschungs- und Kompetenzzentrums für Cybersicherheit“ (ECCC)

Vorbemerkung der Fragesteller

Die Europäische Union will ihre „Abwehrfähigkeit, Abschreckung und Abwehr“ im Bereich der Cybersicherheit erhöhen (Ratsdokument 14435/17). Ein neues „Forschungs- und Kompetenzzentrum für Cybersicherheit“ (ECCC) soll entsprechende Maßnahmen koordinieren (Verordnungsvorschlag der Europäischen Kommission 2018/0328/COD). Bislang ist über den Standort eines solchen Zentrums aber noch nicht entschieden (siehe Antwort zu Frage 6 auf Bundestagsdrucksache 19/1900). Deshalb kann auch die vor zwei Jahren von der Europäischen Kommission vorgelegte Verordnung zur Einrichtung eines ECCC nicht beschlossen werden (https://www.europarl.europa.eu/doceo/document/TA-8-2019-0189_DE.html). Auch die Rechtsform des ECCC ist nach wie vor ungeklärt: Würde das ECCC eine „institutionalisierte europäische Partnerschaft“ oder „Struktur“ der Europäischen Union, müsste es aus Sicht der Fragestellerinnen und Fragesteller von einer Generaldirektion der Kommission verwaltet werden. Damit hätte die Kommission automatisch ein Vetorecht im Verwaltungsrat des ECCC.

Gemäß den Schlussfolgerungen des Rates von 2017 (Ratsdokument 14435/17) soll das ECCC die Abhängigkeit der Europäischen Union von „nichteuropäischen Cybersicherheitsanbietern“ reduzieren und Anstrengungen in den Bereichen Industrie, Technologie und Forschung bündeln. Kern der vorgeschlagenen Verordnung ist auch die Vernetzung von nationalen Koordinierungszentren in den Mitgliedstaaten. Nach Kenntnis der Fragestellerinnen und Fragesteller soll im deutschen Koordinierungszentrum auch das Bundesministerium der Verteidigung mitarbeiten. Auch die Kommission schlägt in ihrer Verordnung vor, dass das ECCC die Zusammenarbeit zwischen ziviler und militärischer Forschung koordiniert. Genannt werden hierzu „Technologien und Anwendungen mit doppeltem Verwendungszweck“ sowie die Bereiche Bildung, Schulung und Übungen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 3. Juli 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Handelt es sich bei dem europäischen EEEC aus Sicht der Bundesregierung um eine EU-Agentur oder ist es einer solchen gleichzustellen?

Der Vorschlag für eine Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren basiert mit Artikel 173 Absatz 3 und Artikel 188 i. V. m. Artikel 187 AEUV auf zwei Rechtsgrundlagen. Am 3. Juni 2020 hat der Ausschuss der Ständigen Vertreter der Mitgliedstaaten (AStV) die Allgemeine Ausrichtung des Rats zur Etablierung des ECCC angenommen. Die Bundesregierung unterstützt die gemeinsame teilweise Ausrichtung des Rates und das damit verbundene Mandat für die anstehenden Triloge. Aus Sicht der Bundesregierung ist die Frage der geeigneten Rechtsform des ECCC vom Fortgang der laufenden Beratungen abhängig.

2. Unter welchen Umständen sollte das Zentrum aus Sicht der Bundesregierung als „gemeinsamer Ansatz der EU bzw. „institutionalisierte europäische Partnerschaft“ gemäß den Artikeln 173, 185 und 187 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) installiert werden, und was bedeutet dies für dessen verpflichtende oder freiwillige Finanzierung durch die Mitgliedstaaten?

Die Bundesregierung unterstützt die gemeinsame teilweise Ausrichtung des Rates zur Etablierung des ECCC und das damit verbundene Mandat für die anstehenden Triloge mit dem Europäischen Parlament vom 3 Juni 2020. Mögliche Implikationen der Errichtung des ECCC auf Grundlage der Artikel 185 und 187 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) im Sinne von ‚institutionalisierten Partnerschaften‘ sind abhängig vom Fortgang der laufenden Beratungen.

3. Wo soll das Zentrum nach Kenntnis der Bundesregierung nach derzeitigem Stand errichtet (siehe Antwort zu Frage 6 auf Bundestagsdrucksache 19/1900) werden, bzw. welche Bewerbungen welcher Länder für welche Standorte sind ihr bekannt?

In der Allgemeinen Ausrichtung des Rats vom 3. Juni 2020 wurde keine Festlegung zum Standort getroffen, da noch keine gemeinsame Position zu dieser Frage gefunden wurde. Dies gilt auch für das Prozedere der Auswahl des Standorts. Der Bundesregierung sind folgende Interessenbekundungen bekannt (in alphabetischer Reihenfolge): Belgien (Brüssel), Irland (ohne weitere Angabe), Litauen (Vilnius), Luxemburg, Polen (ohne weitere Angabe), Portugal (ohne weitere Angabe), Rumänien (Bukarest) und Spanien (Leon).

4. Sofern hierzu immer noch keine konkreten Festlegungen getroffen wurden, welche Gründe kennt die Bundesregierung für die Verzögerung?

Der ursprüngliche Vorschlag der Europäischen Kommission sieht Brüssel als Standort vor. Schwerpunkt der Verhandlungen im Rat waren indes die inhaltliche Ausrichtung des ECCC mit dem Ziel die europäischen Bemühungen im Bereich Cybersicherheit in den Handlungsfeldern Industrie, Technologie und Forschung wirksam zu bündeln. Nach Einschätzung der Bundesregierung lag dies vor allem daran, dass die Festlegungen in den Verordnungen zu den europäischen Förderprogrammen Horizont Europa und Digitales Europa zu berücksichtigen sind. Zugunsten der notwendigen Klärungen zum Zusammenwirken und Abstimmungen zu den notwendigen Anpassungen des Verordnungsentwurfs wurde die Frage des Standorts zunächst zurückgestellt.

5. Wer soll aus Sicht der Bundesregierung über die Festlegung des Standortes des EEEC entscheiden?

   a) Welches Mitentscheidungsrecht hat aus ihrer Sicht das Europäische Parlament?

   b) Sofern die Bundesregierung den Rat als entscheidungskompetent ansieht, wie begründet sie dies ob der Tatsache, dass es sich bei dem Zentrum nicht um eine Agentur handelt?

   c) Inwiefern plädiert die Bundesregierung dafür, die Verordnung für das Zentrum hinsichtlich der Sitzfrage zu ändern, sodass das Europäische Parlament nicht mitentscheiden kann?

Die Fragen 5 bis 5c werden gemeinsam beantwortet.

Aus Sicht der Bundesregierung richtet sich die Entscheidung über den Standort des EEEC nach der für die Organisationsform einschlägigen Rechtsgrundlage. Eine abschließende Entscheidung über die Organisationsform wurde noch nicht getroffen.

6. Für welche Fragen sollten aus Sicht der Bundesregierung der Europäischen Kommission ein Mitspracherecht bei Entscheidungen im Verwaltungsrat des Zentrums eingeräumt werden?

Eine abschließende Aussage zu den Fragen, bei denen die Europäische Kommission anzuhören ist bzw. ein Mitspracherecht hat, kann erst nach Zuweisung der endgültigen Aufgaben des Zentrums nach Abschluss der Verhandlungen zwischen dem Rat der Europäischen Union und dem Europäischen Parlament getroffen werden.

   a) Sollte die Kommission ein Vetorecht erhalten, und falls nein, warum nicht?

Die Frage der Stimmrechte im einzurichtenden Verwaltungsrat wurde in der Allgemeinen Ausrichtung vom 3. Juni 2020 ausgeklammert und ist weiterhin Gegenstand der Beratungen im Rat. Aus Sicht der Bundesregierung sollten sich die Stimmgewichte der Europäischen Kommission im Verwaltungsrat vor allem an der Verantwortung der Kommission für die rechtskonforme Verwendung der Haushaltsmittel der Europäischen Union (EU) bemessen. Wenn die Aufgaben des Zentrums feststehen, sollte dies nach Ansicht der Bundesregierung der Maßstab für die Festlegung der Stimmverhältnisse sein.

   b) Wie definiert die Bundesregierung den Begriff „Finanzfragen“?

Die Frage kann erst im konkreten Kontext der in der Frage gegenständlichen künftigen Rechtsverordnung beantwortet werden.

7. Welche Pilotprojekte (auch „koordinierende Zentren“) mit welchen Beteiligten an welchen Standorten sind nach Kenntnis der Bundesregierung aus der entsprechenden Ausschreibung bis Mai 2018 hervorgegangen (siehe Antwort zur Frage auf Bundestagsdrucksache 19/1900)?

Im Rahmen der Ausschreibung „SU-ICT-03-2018“ werden folgende vier Pilotprojekte gefördert:

- „Cyber security cOmpeteNCe fOr Research anD InnovAtion” (CONCORDIA)

- „Cyber Security Network of Competence Centres for Europe" (CyberSec4 Europe)
- „European network of Cybersecurity centres and competence Hub for innovation and Operations" (ECHO)
- „Strategic programs for advanced research and technology in Europe" (SPARTA)

Zwei der vier Pilotprojekte werden von deutschen Einrichtungen koordiniert, „CONCORDIA" von der Universität der Bundeswehr München und „CyberSec4 Europe" von der Johann Wolfgang-Goethe-Universität Frankfurt. Das Projekt „ECHO" wird von der Königlichen Militärakademie in Belgien und das Projekt „SPARTA" vom Kommissariat für Atomenergie und alternative Energien (CEA) in Frankreich koordiniert.

Insgesamt sind 175 Einrichtungen an diesen Pilotprojekten beteiligt, davon 24 Einrichtungen aus Deutschland. Die Zahl der Antragsbeteiligungen liegt bei insgesamt 184, wobei 8 Einrichtungen an mehr als einem Pilotprojekt beteiligt sind. Einrichtungen aus Deutschland sind an allen vier Pilotprojekten beteiligt. Im Folgenden sind alle Beteiligten der vier Pilotprojekte nach Standorten (Ländern) sortiert aufgelistet.

„CONCORDIA"

Beteiligte Einrichtungen
AT – Austria
SBA RESEARCH GEMEINNÜTZIGE GMBH
BE – Belgium
EIT DIGITAL
CH – Switzerland
RUAG Schweiz AG
UNIVERSITÄT ZÜRICH
CY – Cyprus
TECHNOLOGIKO PANEPISTIMIO KYPROU
CZ – Czechia
MASARYKOVA UNIVERZITA
FLOWMON NETWORKS AS
DE – Germany
AIRBUS CYBERSECURITY GMBH
UNIVERSITÄT DER BUNDESWEHR MÜNCHEN
SIEMENS AKTIENGESELLSCHAFT
INFINEON TECHNOLOGIES AG
JACOBS UNIVERSITY BREMEN GGMBH
BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
DFN-CERT SERVICES GMBH
EESY-INNOVATION GMBH
TÜV TRUST IT GMBH UNTERNEHMENSGRUPPE TÜV AUSTRIA
TECHNISCHE UNIVERSITÄT BRAUNSCHWEIG
SECUNET SECURITY NETWORKS AG
UNIVERSITÄT PASSAU
RUHR-UNIVERSITÄT BOCHUM
EL – Greece
IDRYMA TECHNOLOGIAS KAI EREVNAS
PANEPISTIMIO PATRON
MINISTRY OF DIGITAL GOVERNANCE
ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS

Beteiligte Einrichtungen
ES – Spain
TELEFONICA INVESTIGACION Y DESARROLLO SA
CAIXABANK SA
ATOS SPAIN SA
FR – France
UNIVERSITE DE LORRAINE
CYBER-DETECT
IL – Israel
BEN-GURION UNIVERSITY OF THE NEGEV
IT – Italy
CENTRO RICERCHE FIAT SCPA
UNIVERSITA DEGLI STUDI DELL'INSUBRIA
TELECOM ITALIA SPA
UNIVERSITA DEGLI STUDI DI MILANO
LU – Luxembourg
UNIVERSITE DU LUXEMBOURG
NL – Netherlands
UNIVERSITEIT TWENTE
STICHTING INTERNET DOMEINREGISTRATIE NEDERLAND
ARTHUR'S LEGAL BV
SURFnet bv
NO – Norway
TELENOR ASA
OSLOMET – STORBYUNIVERSITETET
UNIVERSITETET I OSLO
PT – Portugal
EFACEC ENERGIA – MAQUINAS E EQUIPAMENTOS ELECTRICOS SA
RO – Romania
BITDEFENDER SRL
SE – Sweden
RISE RESEARCH INSTITUTES OF SWEDEN AB
ERICSSON AB
SI – Slovenia
UNIVERZA V MARIBORU
INSTITUT JOZEF STEFAN
UK – United Kingdom
UNIVERSITY OF LANCASTER
IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE

„CyberSec4 Europe“

Beteiligte Einrichtungen
AT – Austria
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
BE – Belgium
KATHOLIEKE UNIVERSITEIT LEUVEN
OPEN & AGILE SMART CITIES
TIME.LEX
TRUST IN DIGITAL LIFE
BG – Bulgaria
INTERNATIONAL CYBER INVESTIGATION TRAINING ACADEMY
CH – Switzerland
ARCHIMEDE SOLUTIONS SARL

Beteiligte Einrichtungen
CONCEPTIVITY SARL
CY – Cyprus
UNIVERSITY OF CYPRUS
CZ – Czechia
Masarykova univerzita
DE – Germany
JOHANN WOLFGANG GOETHE-UNIVERSITÄT FRANKFURT AM MAIN
NEC LABORATORIES EUROPE GMBH
SIEMENS AKTIENGESELLSCHAFT
DK – Denmark
DANMARKS TEKNISKE UNIVERSITET
EE – Estonia
CYBERNETICA AS
EL – Greece
IDRYMA TECHNOLOGIAS KAI EREVNAS
INSTITOUTO TECHNOLOGIAS YPOLOGISTONKAI EKDOSEON DIOFANTOS
UNIVERSITY OF PIRAEUS RESEARCH CENTER
ES – Spain
ATOS IT SOLUTIONS AND SERVICES IBERIA SL
ATOS SPAIN SA
BANCO BILBAO VIZCAYA ARGENTARIA SA*
UNIVERSIDAD DE MALAGA
UNIVERSIDAD DE MURCIA
FI – Finland
JYVASKYLAN AMMATTIKORKEAKOULU
TEKNOLOGIAN TUTKIMUSKESKUS VTT OY
FR – France
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS
DAWEX SYSTEMS
INFORMATIQUE BANQUES POPULAIRES
INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE
UNIVERSITE PAUL SABATIER TOULOUSE III
UNIVERSITE TOULOUSE II-JEAN JAURES
IE – Ireland
UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN
IT – Italy
ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA
COMUNE DI GENOVA
CONSIGLIO NAZIONALE DELLE RICERCHE
ENGINEERING – INGEGNERIA INFORMATICA SPA
FONDAZIONE BRUNO KESSLER
INTESA SANPAOLO SPA
POLITECNICO DI TORINO
UNIVERSITA DEGLI STUDI DI TRENTO
LU – Luxembourg
UNIVERSITE DU LUXEMBOURG
NL – Netherlands
TECHNISCHE UNIVERSITEIT DELFT
NO – Norway
NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU

Beteiligte Einrichtungen
SINTEF AS
Beteiligte Einrichtungen
PT – Portugal
UNIVERSIDADE DO PORTO
SE – Sweden
KARLSTADS UNIVERSITET
SI – Slovenia
UNIVERZA V MARIBORU
SK – Slovakia
VAF S.R.O.

„ECHO“

Beteiligte Einrichtungen
BE – Belgium
RHEA SYSTEM
ECOLE ROYALE MILITAIRE – KONINKLIJKE MILITAIRE SCHOOL
VITROCISET BELGIUM SPRL
BG – Bulgaria
INSTITUT PO OTBRANA
TELELINK BUSINESS SERVICES EAD
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES
FONDATSIYA EVROPREYSKI SOFTUEREN INSTITUT – TSENTAR IZTOCHNA EVROPA
DE – Germany
VISIONSPACE TECHNOLOGIES GMBH
EE – Estonia
GUARDTIME OU
TALLINNA TEHNIKAULIKOOL
EL – Greece
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS
ES – Spain
TELEFONICA MOVILES ESPANA SA
FI – Finland
LAUREA-AMMATTIKORKEAKOULU OY
FR – France
NAVAL GROUP
HU – Hungary
SEMMELWEIS EGYETEM
IE – Ireland
NATIONAL UNIVERSITY OF IRELAND MAYNOOTH
IT – Italy
CONSORZIO ITALIANO PER LA RICERCA MEDICA
FINCANTIERI SPA
ACEA SPA
ZANASI ALESSANDRO SRL
EXPRIVIA SPA
LINK CAMPUS UNIVERSITY
AON SPA INSURANCE & REINSURANCE BROKERS
SEASTEMA SPA
ARETI S.P.A.
VITROCISET SOCIETA PER AZIONI

Beteiligte Einrichtungen
CONSORTIUM FOR RESEARCH ON INTELLIGENCE AND SECURITY SERVICES
ACEA ATO2 SPA
RHEA SYSTEM SPA
NL – Netherlands
ENQUIRYA BV
RHEA SYSTEM BV
PL – Poland
AKADEMIA GORNICZO-HUTNICZA IM. STANISLAWA STASZICA W KRAKOWIE
RO – Romania
SIVECO ROMANIA SA
CERTSIGN SA
UNIVERSITATEA NATIONALA DE APARARE CAROL I
UA – Ukraine
NATIONAL AEROSPACE UNIVERSITY KHARKIV AVIATION INSTITUTE NAMED BY N ZUKOVSKIY
UK – United Kingdom
BOURNEMOUTH UNIVERSITY

„SPARTA“

Beteiligte Einrichtungen
AT – Austria
TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH
JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH
BE – Belgium
CENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
UNIVERSITE DE NAMUR ASBL
CZ – Czechia
VYSOKE UCENI TECHNICKE V BRNE
CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB
CZ.NIC, ZSPO
DE – Germany
TECHNISCHE UNIVERSITÄT MÜNCHEN
SAP SE
FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT BONN
FORTISS GMBH
UNIVERSITÄT KONSTANZ
EE – Estonia
TARTU ULIKOOL
EL – Greece
KENTRO MELETON ASFALEIAS
NATIONAL CENTER FOR SCIENTIFIC RESEARCH „DEMOKRITOS“
ES – Spain
FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH
FUNDACION TECNALIA RESEARCH & INNOVATION
INDRA SISTEMAS SA
FUNDACIO EURECAT
FR – France

Beteiligte Einrichtungen
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
INSTITUT MINES-TELECOM
INSTITUT NATIONAL DE RECHERCHE ENINFORMATIQUE ET AUTOMATIQUE
THALES SIX GTS FRANCE SAS
YES WE HACK
SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE
CENTRALESUPELEC
INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON
IT – Italy
CONSIGLIO NAZIONALE DELLE RICERCHE
CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA
LEONARDO – SOCIETA PER AZIONI
CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI
DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA – ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE
LT – Lithuania
LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS
MYKOLO ROMERIO UNIVERSITETAS
KAUNO TECHNOLOGIJOS UNIVERSITETAS
GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA
LU – Luxembourg
SECURITY MADE IN LETZEBUERG
UNIVERSITE DU LUXEMBOURG
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LV – Latvia
LATVIJAS MOBILAIS TELEFONS SIA
PL – Poland
ITTI SP ZOO
NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA – PANSTWOWY INSTYTUT BADAWCZY
STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO
PT – Portugal
INOV INESC INOVACAO – INSTITUTO DE NOVAS TECNOLOGIAS
INSTITUTO SUPERIOR TECNICO

8. Ist das EEEC nach Kenntnis der Bundesregierung „um eine Cyberabwehr-Abteilung ergänzt“ worden (https://ec.europa.eu/germany/news/20170919-lage-der-union-2017-eu-kommission-cyberkriminalitaet_de), bzw. welche Planungen existieren hierzu?

Nach Kenntnis der Bundesregierung werden die organisatorischen Entscheidungen zum Zentrum für Cybersicherheit erst dann getroffen, wenn die übertragenen Zuständigkeiten und Verantwortungen abschließend feststehen. Entsprechend ist der Bundesregierung zum Zeitpunkt der Beantwortung nichts über etwaige Ergänzungen um eine „Cyberabwehr-Abteilung“ bekannt.

9. Wo soll die deutsche Kontaktstelle des EEEC angesiedelt werden, und welche Bundesministerien und nachgeordnete Behörden sollen dort mitarbeiten?

   a) Sofern auch das Bundesministerium der Verteidigung dort mitarbeiten soll, welche Aufgaben soll das Militär dort übernehmen?

Die Entscheidung zur Einrichtung des Nationalen Koordinierungszentrum wurde noch nicht getroffen und ist von den an die Nationalen Koordinierungszentren übertragenen Zuständigkeiten und Verantwortungen abhängig. Diese stehen erst nach Einigung mit dem Europäischen Parlament fest.

   b) Mit welchem Ergebnis ist die konzeptionelle Prüfung der Einrichtung eines „Kompetenzzentrums Krisenfrüherkennung“ bei der Bundeswehr inzwischen abgeschlossen (siehe Antwort zu Frage 21 auf Bundestagsdrucksache19/11920), und welche Details kann die Bundesregierung zu dessen Standort, Zielsetzung und technischer Infrastruktur mitteilen?

Über die Einrichtung eines Kompetenzzentrums Krisenfrüherkennung bei der Bundeswehr wird im dritten Quartal 2020 abschließend entschieden.

10. Welche neuen Kapazitäten sollte die Europäische Union aus Sicht der Bundesregierung zur „Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen“ entwickeln (bitte die auf Bundestagsdrucksache 19/1900 erbetene Antwort zu Frage 12 ausführen)?

Im Kontext von Cybercrime und Cyberangriffen werden üblicherweise täterseitig Mittel zur Verschleierung der technischen Identität (Anonymisierung) sowie zur Geheimhaltung der Kommunikation (Verschlüsselung) verwendet. Aus Sicht von Sicherheitsbehörden besteht grundsätzlich das Erfordernis, eine wirkungsvolle Strafverfolgung insbesondere durch die Schaffung von Kapazitäten zur anlassbezogenen Erlangung unverschlüsselter Täter-Kommunikation wie auch zur anlassbezogenen Erlangung technischer Identifikationsmerkmale trotz täterseitiger Anonymisierung zu ermöglichen.

11. Über wie viele weitere Störsignaldetektoren und GPS-Ortungsgeräte neben den sechs bzw. fünf über das EU-Projekt SPECTRE beschafften Einheiten verfügt das Bundeskriminalamt (siehe Antwort zu Frage 9 auf Bundestagsdrucksache 19/19799), und ab welchem Datum will das BKA nach derzeitigem Stand im Anschluss an seine Beteiligung an der Testphase sowie der aktuellen Planungsphase und Aufbauphase für den Wirkbetrieb der „European Tracking Solution“ als Kontaktstelle bzw. nationales Gateway bei Europol zur europaweiten Nutzung von GPS-Ortungsgeräten fungieren?

Das Bundeskriminalamt (BKA) verfügt neben den sechs bzw. fünf über das EU-Projekt SPECTRE beschafften Einheiten über acht weitere Störsenderdetektoren sowie über ca. 160 GPS-Ortungsgeräte. Der Bundesregierung liegen keine konkreten Informationen darüber vor, wann Europol den Wirkbetrieb mit der „European Tracking Solution“ aufnehmen wird. Sobald dies erfolgt, fungiert das Bundeskriminalamt als Kontaktstelle bzw. nationales Gateway.

12. Was ist der Bundesregierung über Begünstigte und Zwecke eines Zuschusses der Europäischen Kommission für das Europäischen Zentrum für Computerkriminalität (EC3) von Europol in Höhe von fünf Mio. Euro bekannt, mit dem technische Fähigkeiten gegen Geräteverschlüsselung, darunter ein neues „Entschlüsselungssystem“, beschafft werden sollen (https://netzpolitik.org/2020/eu-beamter-fordert-gesetz-gegen-verschluesselung; bitte die Hersteller und die zu beschaffenden Produkte darstellen)?

Nach Kenntnis der Bundesregierung hat die EU-Kommission im Jahr 2018 dem Europäischen Zentrum für Cyberkriminalität (EC3) von EUROPOL 5.000.000 Euro zugewiesen, um Kapazitäten für die Dekryptierung von verschlüsselten Informationen zu schaffen. Diesem Auftrag wird das EC3 mit der Entwicklung einer neuen Dekryptierungs-Plattform für Datenträger gerecht. Kernkomponente der Plattform sind NVIDIA Grafikprozessoren, die eine schnelle Rechenleistung ermöglichen. Softwareseitig wird das Open-Source-Tool „Hashcat“ verwendet.

a) Welche weiteren Zuschüsse haben die Gemeinsame Forschungsstelle (GFS) der Kommission gewährt, und inwiefern wird dieser über den Fonds für innere Sicherheit (Polizei) gewährt?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

b) Welche weiteren Zuschüsse sind geplant?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

c) Welche deutschen Behörden nehmen an Schulungskursen der European Cybercrime Training and Education Group (ECTEG) zur Entschlüsselung von Geräten teil?

Das BKA hat an Schulungsmaßnahmen der European CybercrimeTraining and Education Group (ECTEG) teilgenommen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, 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