Rat der
Europäischen Union

Brüssel, den 15. Juni 2018
(OR. en)

10072/18

CYBER 136
COSI 145
TELECOM 185
JAI 634
DAPIX 184
RELEX 551
ENFOPOL 318
DEVGEN 97

I/A-PUNKT-VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Entwurf von Schlussfolgerungen des Rates zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten

1. In der Sitzung der Horizontalen Gruppe "Fragen des Cyberraums" vom 2. Mai 2018 haben die Delegationen – im Rahmen des Aufbaus von Cyberkapazitäten als Teil der internationalen Zusammenarbeit der EU – die Notwendigkeit erörtert, die operativen Leitlinien für die Bemühungen der EU um den Aufbau externer Cyberkapazitäten durch spezielle Schlussfolgerungen des Rates zu flankieren. Diese Schlussfolgerungen vermitteln eine Orientierung für einen kohärenten ganzheitlichen Ansatz, tragen aber auch Menschenrechtserwägungen und den Werten der EU Rechnung.

2. In der Sitzung der Horizontalen Gruppe "Fragen des Cyberraums" vom 30. Mai 2018 haben die Delegationen den Entwurf von Schlussfolgerungen des Rates zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten[1] geprüft

3. Im Anschluss an jene Sitzung wurde auf Grundlage der schriftlichen Bemerkungen der Delegationen eine neue Version[2] ausgearbeitet und in der Sitzung der Gruppe vom 11. Juni 2018 geprüft.

4. In der Sitzung beantragten die Delegationen einige weitere Änderungen, und der Text der Schlussfolgerungen des Rates wurde entsprechend geändert[3]. Anschließend wurden diese Schlussfolgerungen im Verfahren der stillschweigenden Zustimmung bis zum 15. Juni 2018 zur Annahme vorgelegt. Die Mitgliedstaaten erhoben keine Einwände, sodass der Vorsitz die Verhandlungen über den in der Anlage wiedergegebenen Entwurf von Schlussfolgerungen abschließen konnte.

5. Der AStV wird daher gebeten, den Rat zu ersuchen, dass er den in der Anlage wiedergegebenen Entwurf von Schlussfolgerungen des Rates zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten billigt.

---

1 Dok. 8754/18.
2 Dok. 8754/1/18 REV 1 und 8754/2/18 REV 2.
3 Dok. 8754/3/18 REV 3.

ANLAGE

ENTWURF VON SCHLUSSFOLGERUNGEN DES RATES ZU DEN EU-LEITLINIEN FÜR DEN AUFBAU EXTERNER CYBERKAPAZITÄTEN

Der Rat der Europäischen Union –

1. IN ANERKENNUNG der Bedeutung eines globalen, offenen, freien, stabilen und sicheren Cyberraums für den Fortbestand von Wohlstand, Wachstum, Sicherheit, Vernetzung und Integrität unserer freien und demokratischen Gesellschaften und UNTER BETONUNG dessen, wie wichtig es ist, die Rechtsstaatlichkeit sowie die Menschenrechte und Grundfreiheiten im Cyberraum zu schützen;

2. UNTER BEKRÄFTIGUNG dessen, dass der Cyberspace für kontinuierliche globale Entwicklung und dauerhaften globalen Wohlstand wichtig ist. Die Cybersicherheit ist daher eine globale Herausforderung, der es seitens der EU mit Engagement, Zusammenarbeit und Koordinierung auf internationaler Ebene zu begegnen gilt und die eine wirksame globale Zusammenarbeit aller Interessenträger erfordert, damit ein funktionierender und stabiler Cyberraum erhalten bleibt;

3. UNTER BETONUNG der Bedeutung des Zugangs zu Informations- und Kommunikationstechnologien (IKT) und deren ungehinderter, unzensierter und diskriminierungsfreier Nutzung für die Förderung offener Gesellschaften und die Ermöglichung von Wirtschaftswachstum und sozialer Entwicklung auf der ganzen Welt;

4. UNTER BESTÄTIGUNG dessen, dass das bestehende Völkerrecht – einschließlich der Charta der Vereinten Nationen und der internationalen Übereinkünfte, wie etwa das Übereinkommen des Europarates über Computerkriminalität (Übereinkommen von Budapest), und der einschlägigen Übereinkünfte über das internationale humanitäre Völkerrecht und die Menschenrechte, wie etwa der Internationale Pakt über bürgerliche und politische Rechte und der Internationale Pakt über wirtschaftliche, soziale und kulturelle Rechte – im Cyberraum gilt;

5. UNTER BETONUNG dessen, wie wichtig es ist, alle Interessenträger, einschließlich der Wissenschaft, der Zivilgesellschaft und des Privatsektors, in die Internet-Governance einzubeziehen;

6. UNTER HINWEIS AUF seine Schlussfolgerungen zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"[4], zur Cybersicherheitsstrategie der EU[5], zur Cyberdiplomatie[6], zur Internet-Governance[7], zu Sicherheit und Verteidigung im Kontext der Globalen Strategie der EU[8], zur durchgängigen Berücksichtigung digitaler Lösungen und Technologien in der Entwicklungspolitik der EU[9] und zur Digitalisierung im Interesse der Entwicklung (D4D)[10]; UND AUF die Menschenrechtsleitlinien der EU in Bezug auf die Freiheit der Meinungsäußerung – online und offline[11] – sowie den Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen[12];

---

4 Dok. 14435/17 und Gemeinsame Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" ((JOIN (2017) 450 final).

5 Dok. 12109/13 und Dok. 6225/13 (Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum" (COM JOIN(2013) 1 final)).

6 Dok. 6122/15.

7 Dok. 16200/14 und Dok. 6460/14 (Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen "Internet-Politik und Internet-Governance Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance (COM(2014) 72 final)).

8 Dok. 9178/17.

9 Dok. 14682/16.

10 Dok. 14542/17.

11 Dok. 9647/14.

12 Dok. 7688/16 (Gemeinsame Mitteilung an das Europäische Parlament und den Rat: "Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union").

7. UNTER HERVORHEBUNG der Rolle des Aufbaus von Cyberkapazitäten in den Partnerländern und -regionen als strategischer Baustein für die Cyberdiplomatie-Bemühungen der EU um die Förderung und den Schutz der Menschenrechte, der digitalen Gleichstellung der Geschlechter, der Rechtsstaatlichkeit, der Sicherheit, des inklusiven Wachstums und der nachhaltigen Entwicklung als Kerndimension der Strategie zur Digitalisierung im Interesse der Entwicklung (D4D);

8. IN DER ERKENNTNIS, dass der Aufbau von Cyberkapazitäten vor allem mit systematischen Anstrengungen – zusammen mit Partnerländern und einschlägigen Organisationen – im Hinblick auf Folgendes verbunden ist: Stärkung der nationalen, der institutionellen und der organisatorischen Kapazitäten, die die Widerstandsfähigkeit kritischer digitaler Dienste und Netze sowie den Schutz kritischer Informationsinfrastrukturen verbessern; Unterstützung von Strafjustizreformen zur Bekämpfung der Cyberkriminalität; Bekämpfung der Nutzung des Internets für terroristische Zwecke; Verbesserung der Cybersicherheitsfertigkeiten und -kompetenzen; schließlich Erleichterung der Sensibilisierung und der effektiven Zusammenarbeit in Bezug auf diese Themen auf nationaler, regionaler und internationaler Ebene;

9. UNTER HINWEIS DARAUF, dass der Aufbau von Cyberkapazitäten zusehends zu einem der wichtigsten Themen auf der Agenda für die internationale Cyberpolitik wird, wie aus den einschlägigen Abschlussdokumenten hervorgeht, zu denen auch folgende zählen: Berichte der VN-Gruppe der Regierungssachverständigen für Entwicklungen im Bereich Information und Telekommunikation im Kontext der internationalen Sicherheit[13]; Resolution der VN-Generalversammlung über Informations- und Kommunikationstechnologien im Dienste der Entwicklung[14]; Ergebnisdokument zum Weltgipfel über die Informationsgesellschaft (WSIS+10)[15]; Doha-Erklärung des 13. Kongresses der VN für Kriminalprävention und Strafjustiz[16]; hierzu gehört auch die Globale Cyberraum-Konferenz" (auch als "London-Prozess" bezeichnet), auf der 2015 das Globale Forum für Cyber-Fachwissen (GFCE) ins Leben gerufen wurde und die 2017 zur Annahme des Delhi-Kommuniqués über eine Globale Agenda des GFCE für den Aufbau von Cyberkapazitäten[17] führte;

10. IN ANERKENNUNG der zunehmenden Bedeutung, die die einschlägigen internationalen, zwischenstaatlichen und regionalen Organisationen – wie etwa der Europarat, die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD), die Vereinten Nationen und ihre Fachorganisationen und -einrichtungen, das Commonwealth, die Afrikanische Union und ihre regionalen Wirtschaftsgemeinschaften, die Organisation Amerikanischer Staaten (OAS) und der Verband südostasiatischer Nationen (ASEAN) – dem Aufbau von Cyberkapazitäten beimessen;

---

13 A/65/2013 (2010), A/68/98 (2013) und A/70/174 (2015).
14 Dok. 71/212.
15 Dok. 70/125.
16 A/CONF.222/17 (2015).
17 Abrufbar unter: https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

11. UNTER BEGRÜßUNG der Arbeiten zur Stärkung der zivilen Aspekte der GSVP, insbesondere durch die Einbeziehung von Cybersicherheitstätigkeiten mit dem Schwerpunkt auf dem Aufbau von Resilienz und Kapazitäten in Drittländern;

12. IN DER ERKENNTNIS, dass der Aufbau von Cyberkapazitäten wichtig ist, um die Mindestkapazitäten aufzubauen, die zur Umsetzung von vertrauensbildenden Maßnahmen im Dienste der Cybersicherheit auf regionaler Ebene (unter Führung der OSZE, des ASEAN-Regionalforums und der OAS) sowie zur Umsetzung der Regeln, Normen und Grundsätze verantwortungsbewussten staatlichen Handelns, wie sie in den Berichten der VN-Gruppen von Regierungssachverständigen (VN-GGE) im Bereich Information und Telekommunikation im Kontext der internationalen Sicherheit aus den Jahren 2013 und 2015 niedergelegt sind, benötigt werden;

13. UNTER WÜRDIGUNG der Zusammenarbeit zwischen der EU und der NATO bei Cybersicherheit und Cyberabwehr einschließlich der Koordinierung der Unterstützung beim Aufbau der Kapazitäten der Partner zur Abwehr von Cyberbedrohungen unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der EU und im Einklang mit seinen entsprechenden Schlussfolgerungen, einschließlich derjenigen vom 6. Dezember 2016 zur Umsetzung der Gemeinsamen Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des Generalsekretärs der Nordatlantikvertrags-Organisation[18];

[18] Dok. 15283/16.

14. IN ANBETRACHT der wachsenden Nachfrage nach Bemühungen um den Aufbau externer Cyberkapazitäten und UNTER BERÜCKSICHTIGUNG der steigenden Zahl der weltweit an solchen Prozessen beteiligten Interessenträger, was neue Möglichkeiten für Synergieeffekte und Lastenverteilung schafft, aber auch neue Herausforderungen in Bezug auf Koordinierung und Kohärenz bewirkt;

15. IN DER ERKENNTNIS, dass die Bemühungen der EU um den Aufbau externer Cyberkapazitäten vielfältigen Zielen dienen, die einander wechselseitig verstärken: Unterstützung des Aufbaus von Cyberresilienz in den Partnerländern, die zu einem besseren globalen digitalen Ökosystem beiträgt; Förderung strategischer Allianzen, die darauf abstellen, das Konzept eines globalen, offenen, freien, stabilen und sicheren Cyberraums im Einklang mit den wichtigsten Werten und Grundsätzen der EU, der Rechtsstaatlichkeit, der Menschenrechte und Grundfreiheiten zu unterstützen; Ermutigung zur Schaffung von Rahmenregelungen für die formelle und die informelle Zusammenarbeit zwischen Partnerländern und -regionen und der EU und ihren Mitgliedstaaten; ferner Förderung der entwicklungspolitischen Verpflichtungen der EU und Umsetzung der Agenda 2030 für nachhaltige Entwicklung –

STELLT HIERMIT FOLGENDES FEST: ER

16. WÜRDIGT die führende Rolle, die die EU und ihre Mitgliedstaaten bei den weltweiten Bemühungen um den Aufbau von Cyberkapazitäten gespielt haben, und ihren Ansatz einer systematischen Verknüpfung dieser Bemühungen mit ihrer Gemeinsamen Außen- und Sicherheitspolitik und ihrer Entwicklungspolitik, insbesondere seit der Annahme der Cybersicherheitsstrategie von 2013;

17. HEBT HERVOR, wie wichtig es ist, die politischen, wirtschaftlichen und strategischen Interessen der EU angesichts zunehmender und komplexer internationaler Diskussionen über Cyberfragen zu fördern und sicherzustellen, dass die unter Führung der EU und ihrer Mitgliedstaaten erfolgenden Bemühungen um den Aufbau von Cyberkapazitäten und Zusammenarbeit einer übergeordneten Richtschnur folgen, damit ein kohärenter, ganzheitlicher und wirksamer Ansatz gewährleistet wird, der auch die umfassenderen Agenden der EU für Digitales, Entwicklung und Sicherheit sowie strategische Autonomie unterstützt[19];

18. VERWEIST AUF die Grundsätze des Ansatzes der EU für die Cyberdiplomatie auf globaler Ebene, wie sie in den Schlussfolgerungen des Rates von 2015 über Cyberdiplomatie festgelegt sind, UND WEIST ERNEUT DARAUF HIN, dass die wichtigsten Werte und Grundsätze der EU in Bezug auf die Cybersicherheit – wie sie in der EU-Cybersicherheitsstrategie von 2013 festgelegt sind – als Ausgangsrahmen für alle Maßnahmen zum Aufbau von Cyberkapazitäten dienen sollten, um sicherzustellen, dass diese Maßnahmen

- die Überlegung einschließen, dass das geltende Völkerrecht und die geltenden internationalen Normen auch im Cyberraum Geltung haben;
- rechtebasiert und gleichstellungsorientiert konzipiert werden und Schutzmechanismen zum Schutz der Grundrechte und -freiheiten enthalten;
- das Modell einer demokratischen und effizienten Internet-Governance durch viele Interessenträger fördern;
- die Grundsätze des offenen Internetzugangs für alle unterstützen und die Integrität von Infrastrukturen, Hardware, Software und Diensten nicht untergraben;
- einem Ansatz der geteilten Verantwortung folgen, der Einbindung und Partnerschaft zwischen Behörden, Privatunternehmen sowie Bürgerinnen und Bürgern mit sich bringt und die internationale Zusammenarbeit fördert;

[19] Dok. 13202/16.

19. UNTERSTREICHT, dass die bei der Entwicklungszusammenarbeit gemachten Erfahrungen[20] bei den Bemühungen um den Aufbau externer Cyberkapazitäten berücksichtigt werden sollten, um deren Wirksamkeit und Nachhaltigkeit dadurch zu gewährleisten, dass sie

- die Eigenverantwortung der Partnerländer bei den Entwicklungsprioritäten in Bezug auf Cyberresilienz sicherstellen;

- den Schwerpunkt auf nachhaltige Ergebnisse durch die Förderung breiter angelegter politischer, rechtlicher und technischer Reformprozesse und nicht auf einmalige Ad-hoc-Tätigkeiten legen;

- der Notwendigkeit einer Förderung von Partnerschaften – insbesondere der Beteiligung aller Interessenträger, unter Würdigung der Vielfalt und Komplementarität ihrer jeweiligen Funktionen – Rechnung tragen;

- gewährleisten, dass Vertrauen, Transparenz, Rechenschaftspflicht und geteilte Verantwortung die Antriebskräfte für jegliche Hilfe darstellen;

---

20 Dargelegt im Abschlussdokument der Globalen Partnerschaft für wirksame Entwicklungszusammenarbeit ("Busan-Partnerschaft"), 1. Dezember 2011.

20. BETONT die Notwendigkeit, den Bemühungen der EU um den Aufbau von Cyberkapazitäten in ihrer Nachbarschaft und in den Entwicklungsländern mit rasch zunehmender Vernetzung Vorrang zu verleihen, wie in den Schlussfolgerungen des Rates vom 20. November 2017 zu der Gemeinsamen Mitteilung an das Europäische Parlament und den Rat mit dem Titel "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"[21] zum Ausdruck kommt, und generell eine faktengestützte Priorisierung auf der Grundlage von Statistiken über den Anstieg beim Internetzugang, strategischen Interessen und Bewertungen der Bedrohungslage – wie etwa die Europol-Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA) und die ENISA-Berichte über die Bedrohungslandschaft – mit dem Ziel zu verfolgen, Cyberfähigkeitslücken zu schließen;

21. WEIST ERNEUT DARAUF HIN, dass Initiativen zum Aufbau externer Cyberkapazitäten seitens der EU und ihrer Mitgliedstaaten vorrangig auf die Bekämpfung der Cyberkriminalität und die Erhöhung der Cybersicherheit in Partnerländern und -regionen abstellen sollten, wobei der Schwerpunkt auf Reformen bei den Grundpfeilern der Cyberresilienz liegen sollte, indem insbesondere ein übergeordneter strategischer Rahmen unterstützt wird, Gesetzgebungsreformen gefördert und die Kapazitäten des Strafjustizsystems erhöht werden, die Fähigkeiten zur Bewältigung von Vorfällen entwickelt und ausgebaut werden, Bildung, berufliche Ausbildung und Fachkenntnisse in diesem Bereich entwickelt werden und Cyberhygiene und entsprechende Sensibilisierung sowie eine Kultur der Sicherheitsbewertung von digitalen Produkten, Verfahren und Dienstleistungen im Einklang mit europäischen und internationalen Standards und bewährten Verfahren gefördert werden und ein gesamtgesellschaftlicher Ansatz verfolgt wird;

---

[21] Dok. 14435/17 (Gemeinsame Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" ((JOIN (2017) 450 final).

22. RUFT die EU und ihre Mitgliedstaaten AUF, über ihre Maßnahmen zum Aufbau von Kapazitäten für das Übereinkommen des Europarates über Computerkriminalität (Übereinkommen von Budapest) als internationalen wirksamen rechtlichen Standard für die Entwicklung der nationalen Rechtsvorschriften über Cyberkriminalität in den Partnerländern einzutreten, und die erforderlichen Ermittlungs- und Verfolgungskapazitäten auf dieser Grundlage zu entwickeln, bei der Bekämpfung der Cyberkriminalität auf globaler Ebene innerhalb des bestehenden, durch das Übereinkommen von Budapest gebotenen Rahmens zusammenzuarbeiten und die die nationalen Fähigkeiten und kritische Sektoren betreffenden Komponenten der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) als Inspirationsquelle für die Ausarbeitung von Rechtsvorschriften über Cybersicherheit in den Partnerländern zu nutzen;

23. STELLT FEST, dass der Aufbau von Cyberkapazitäten ein integraler Bestandteil der durchgängigen Berücksichtigung der Digitalisierung in der Entwicklungspolitik der EU ist, wie in den Schlussfolgerungen des Rates[22] und im Arbeitsdokument der Kommissionsdienststellen ",Digitalisierung für Entwicklung: durchgängige Berücksichtigung digitaler Technologien und Dienste in der Entwicklungspolitik der EU" (Digital4Development – D4D)[23] dargelegt ist und IST SICH BEWUSST, dass aufgrund der bereichsübergreifenden Aspekte des elektronischen Beweismaterials und der durch den Cyberraum ermöglichten Systeme, Infrastrukturen und Dienste ein ganzheitlicher und kohärenter rechtebasierter Ansatz auch bei anderen Tätigkeiten zum Aufbau externer Kapazitäten, die den Bereich Justiz und Sicherheit betreffen – insbesondere bei Programmen zur Bekämpfung von Terrorismus und organisierter Kriminalität –, erforderlich ist;

---

22 Dok. 14682/16 und 14542/17.

23 SWD(2017)157.

24. BETONT, dass Folgendes notwendig ist: Gewährleistung der kohärenten und effizienten Verwendung der Ressourcen durch die EU und ihre Mitgliedstaaten, vollständige Ausschöpfung der einschlägigen externen Finanzierungsinstrumente und Programme der EU und Nutzung der Hebelwirkung der Fachkenntnisse der für den Cyberraum zuständigen nationalen Behörden der EU-Mitgliedstaaten, der einschlägigen Fachagenturen der EU (insbesondere ENISA, EC3 bei Europol, Eurojust, CEPOL und eu-LISA) und ihrer Netzwerke (z.B. Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität, Europäisches Justizielles Netz gegen Cyberkriminalität) sowie bestehender Experten-, Wissenschafts-, Technik- und Industrienetze (wie beispielsweise GÉANT, FIRST und Meridian);

25. FORDERT die EU und ihre Mitgliedstaaten AUF, ihre Maßnahmen zum Aufbau von Kapazitäten in den Partnerländern und -regionen entsprechend den lokalen Gegebenheiten anzupassen und auf die Schaffung selbsttragender lokaler Fachzentren unter Rückgriff auf Fachwissen und bewährte Verfahren der EU hinzuarbeiten, und ERMUTIGT zur interregionalen, Süd-Süd- und Dreieckskooperation sowie zu einem differenzierten Ansatz – je nach der "Cyberreife" der betreffenden Länder – bei der Durchführung von Maßnahmen zum Aufbau von Cyberkapazitäten;

26. ERMUTIGT die EU und ihre Mitgliedstaaten zu einem kontinuierlichen Dialog mit wichtigen internationalen und regionalen Partnern und Organisationen sowie mit der Zivilgesellschaft, der Wissenschaft und der Privatwirtschaft in diesem Bereich mit dem Ziel, in Anbetracht der begrenzten Ressourcen Doppelarbeit zu vermeiden, und BEGRÜßT die Koordinierungsinitiative des Globalen Forums für Cyber-Fachwissen (Global Forum on Cyber Expertise/GFCE) sowie die Bemühungen, das Thema durch eine Behandlung durch andere internationale Foren wie das Weltwirtschaftsforum, das Internet-Governance-Forum und andere aufzuwerten;

27. BEGRÜßT den Vorschlag, ein Netzwerk der EU für den Aufbau externer Cyberkapazitäten zur Mobilisierung der kollektiven Fachkenntnisse der Mitgliedstaaten der EU für von der EU finanzierte Programme zum Aufbau externer Cyberkapazitäten einzurichten, eine wirksame Koordinierung der von der EU finanzierten Tätigkeiten zum Aufbau externer Cyberkapazitäten zu unterstützen, die Schulungsmöglichkeiten angesichts stark zunehmender Initiativen in den Partnerländern und -regionen und der wachsenden Nachfrage nach den Cyberraum betreffenden Schulungen zu erhöhen und dabei mit dem GFCE-Netz zusammenzuarbeiten und es zu ergänzen;

28. BEGRÜßT die Ausarbeitung einer operativen Richtschnur durch die Kommission für den Aufbau von Cyberkapazitäten in Drittländern[24] sowie für die Einbeziehung des rechtebasierten Ansatzes in die externen Kooperationsmaßnahmen der EU in Bezug auf Terrorismus, organisierte Kriminalität und Cybersicherheit[25];

29. FORDERT den Europäischen Auswärtigen Dienst und die Kommission AUF, die Prioritätensetzung und den Informationsaustausch in Bezug auf die Tätigkeiten zum Aufbau von Cyberkapazitäten in ihren bilateralen Dialogen mit strategischen Partnern sowie den einschlägigen internationalen und regionalen Foren fortzusetzen;

30. FORDERT die Kommission AUF, der horizontalen Gruppe "Fragen des Cyberraums" regelmäßig über den Aufbau externer Cyberkapazitäten zu berichten, und FORDERT die Mitgliedstaaten auf, Informationen über ihre jeweiligen Bemühungen auszutauschen.

---

[24] Abschlussuntersuchung soll im Juni 2018 veröffentlicht werden.

[25] Untersuchung auf Englisch und auf Französisch abrufbar unter https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperation-actions-addressing-terrorism-organised_en.