Rat der
Europäischen Union

Brüssel, den 10. April 2018
(OR. en)

7517/18

CYBER 50
COPS 74
JAI 252
COPEN 78
DROIPEN 36
RELEX 267

I/A-PUNKT-VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Entwurf von Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten – Billigung

1. In der Sitzung der horizontalen Gruppe "Fragen des Cyberraums" vom 22. Februar 2018 führten die Delegationen einen Gedankenaustausch über die Folgemaßnahmen zu einigen der jüngsten Cyber-Angriffe und erörterten die im Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten vorgesehenen Möglichkeiten. Im Laufe der Beratungen wiesen die Mitgliedstaaten deutlich darauf hin, wie wichtig eine angemessene Reaktion der EU auf solche Aktivitäten ist, und zeigten verschiedene Optionen auf, die als Vorgehensweise in Betracht gezogen werden könnten.

2. In der Sitzung der horizontalen Gruppe "Fragen des Cyberraums" vom 5. März 2018 wurden diese Optionen mit der Unterstützung des EAD weiter ausgearbeitet und von den Mitgliedstaaten erörtert. Aus diesen Beratungen ging hervor, dass die bevorzugte Option eine Reaktion der EU in Form von Schlussfolgerungen des Rates ist. Der EAD übernahm die Aufgabe, einen Entwurf von Schlussfolgerungen des Rates zu bösartigen Cyberaktivitäten auszuarbeiten, der dem Rat am 19. März 2018 übermittelt wurde[1].

[1] Dok. 7309/18.

3. Anhand der schriftlichen Bemerkungen der Delegationen zum Entwurf, die am 27. März bzw. 4. April 2018 vorlagen, hat der Vorsitz den ursprünglichen Text entsprechend den Standpunkten der Mitgliedstaaten[2] überarbeitet und konsolidiert, um ihn in der Sitzung der horizontalen Gruppe "Fragen des Cyberraums" vom 10. April 2018 zu erörtern und abzuschließen.

4. In dieser Sitzung wünschten die Delegationen einige weitere geringfügige Anpassungen des Textes, auf die sie sich während der Sitzung verständigten. Somit konnte der Vorsitz die Verhandlungen über den Entwurf von Schlussfolgerungen des Rates erfolgreich abschließen und den endgültigen Kompromisstext[3] ausarbeiten, der vom PSK ebenfalls am 10. April 2018 gebilligt wurde.

5. Der ASTV wird daher gebeten, den Rat zu ersuchen, dass er den in der Anlage wiedergegebenen Entwurf von Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten billigt.

---

[2] Dok. 7584/18 und 7584/1/18 REV1.
[3] Dok. 7584/2/18 REV2.

ANLAGE

Entwurf von Schlussfolgerungen des Rates zu böswilligen Cyberaktivitäten

Die EU betont, wie wichtig ein globaler, offener, freier, stabiler und sicherer Cyberraum, in dem die Menschenrechte und Grundfreiheiten sowie die Rechtsstaatlichkeit uneingeschränkt gelten, für das soziale Wohlbefinden, das Wirtschaftswachstum, den Wohlstand und die Integrität unserer freien und demokratischen Gesellschaften ist.

Die EU verweist auf ihre Schlussfolgerungen über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten[1], die einen Beitrag [...] zur Konfliktprävention, Zusammenarbeit und Stabilität im Cyberraum leisten und in denen Maßnahmen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU, einschließlich restriktiver Maßnahmen, dargelegt werden, mit denen böswillige Cyberaktivitäten verhindert bzw. darauf reagiert werden kann.

Die EU bekundet ihre tiefe Besorgnis darüber, dass Drittstaaten und nichtstaatliche Akteure in zunehmendem Maße in der Lage und bereit sind, zur Verwirklichung ihrer Ziele auf böswillige Cyberaktivitäten zurückzugreifen, und wird ihre Fähigkeiten zur Bekämpfung von Cyber-Bedrohungen weiter ausbauen. Die EU erkennt an, dass der verzahnte und komplexe Charakter des Cyberraums gemeinsame Anstrengungen von Regierungen, Privatwirtschaft, Zivilgesellschaft, Fachkreisen, Nutzern und der Wissenschaft erfordert, um die sich stellenden Herausforderungen zu bewältigen, und fordert diese Akteure auf, ihre jeweilige spezifische Verantwortung für den Erhalt eines offenen, freien, sicheren und stabilen Cyberraums anzuerkennen und wahrzunehmen.

Die EU verurteilt entschieden die böswillige Nutzung von Informations- und Kommunikationstechnologien (IKT), einschließlich im Fall von Wannacry und NotPetya, die beträchtlichen Schaden und wirtschaftlichen Verlust in und außerhalb der EU angerichtet haben. Derartige Zwischenfälle destabilisieren den Cyberraum ebenso wie die physische Welt, da sie leicht falsch interpretiert werden können und Kettenreaktionen auslösen könnten. Die EU betont, dass der Missbrauch von IKT für böswillige Zwecke nicht hingenommen werden kann, da er unsere Stabilität, Sicherheit und die Vorteile untergräbt, die das Internet und die Nutzung von IKT bieten.

[1] Dok. 9916/17.

Die EU wird sich auch weiterhin entschieden dafür einsetzen, dass das geltende Völkerrecht auf den Cyberraum Anwendung findet, und betont, dass die Achtung des Völkerrechts, insbesondere der VN-Charta, von wesentlicher Bedeutung ist, um Frieden und Stabilität zu erhalten. Die EU hebt hervor, dass die Staaten keine Stellvertreter einsetzen dürfen, um mittels IKT völkerrechtswidrige Handlungen zu begehen, und nach bestem Bemühen dafür Sorge tragen sollten, dass nichtstaatliche Akteure von ihrem Hoheitsgebiet aus keine derartigen Handlungen begehen, wie es im Bericht der von den Vereinten Nationen eingesetzten Gruppe von Regierungssachverständigen für den Bereich Information und Telekommunikation im Zusammenhang mit der internationalen Sicherheit (UN-GGE) von 2015 beschrieben wurde.

Die EU betont, dass die Einhaltung freiwilliger, nicht bindender Normen für ein verantwortungsvolles Verhalten der Staaten im Cyberraum zu einem offenen, sicheren, stabilen, zugänglichen und friedlichen IKT-Umfeld beiträgt. Die EU hebt hervor, dass die Staaten gehalten sind, von IKT-Tätigkeiten, die ihren völkerrechtlichen Verpflichtungen zuwiderlaufen, abzusehen, und nicht wissentlich zuzulassen, dass auf ihrem Hoheitsgebiet mit Hilfe von IKT völkerrechtswidrige Handlungen begangen werden, wie in dem Bericht der UN-GGE von 2015 festgestellt wurde.

Die EU bekundet ihre Bereitschaft, innerhalb der VN und anderer einschlägiger internationaler Gremien weiterhin auf die Weiterentwicklung und Umsetzung der freiwilligen, nicht bindenden Normen, Regeln und Grundsätze für ein verantwortungsvolles Verhalten der Staaten im Cyberraum hinzuwirken, wie es in den Berichten der jeweiligen UN-GGE aus den Jahren 2010, 2013 und 2015 deutlich beschrieben wurde.