Rat der
Europäischen Union

Brüssel, den 19. Juni 2017
(OR. en)

10474/17

CYBER 98
RELEX 554
POLMIL 77
CFSP/PESC 557

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	19. Juni 2017
Empfänger:	Delegationen
Nr. Vordok.:	9916/17
Betr.:	Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten ("Cyber Diplomacy Toolbox"), 19. Juni 2017

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten ("Cyber Diplomacy Toolbox"), die der Rat (Auswärtige Angelegenheiten) auf seiner 3551. Tagung vom 19. Juni 2017 angenommen hat.

ANLAGE

SCHLUSSFOLGERUNGEN DES RATES ZU EINEM RAHMEN FÜR EINE GEMEINSAME DIPLOMATISCHE REAKTION DER EU AUF BÖSWILLIGE CYBERAKTIVITÄTEN ("CYBER DIPLOMACY TOOLBOX")

Der Rat der Europäischen Union hat die folgenden Schlussfolgerungen angenommen:

1. Der EU ist bewusst, dass der Cyberraum große Chancen bietet, aber auch sich stetig verändernde Herausforderungen für ihre Außenpolitik, einschließlich der Gemeinsamen Außen- und Sicherheitspolitik, mit sich bringt, und bekräftigt, dass es mehr und mehr notwendig ist, die Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger vor Bedrohungen aus dem Cyberraum und böswilligen Cyberaktivitäten zu schützen.

Die EU erinnert an ihre Schlussfolgerungen zur Cybersicherheitsstrategie[1], insbesondere ihre Entschlossenheit, einen offenen, freien, stabilen und sicheren Cyberraum zu bewahren, in dem die Grundrechte und die Rechtsstaatlichkeit ohne Einschränkungen Geltung finden. Sie verweist ferner auf die Schlussfolgerungen des Rates zur Cyberdiplomatie[2], insbesondere darauf, dass ein gemeinsamer umfassender Ansatz der EU für die Cyberdiplomatie zur Konfliktverhütung, zur Eindämmung von Cyberbedrohungen und zu größerer Stabilität in den internationalen Beziehungen beitragen könnte.

Die EU und ihre Mitgliedstaaten weisen darauf hin, wie wichtig der kontinuierliche Einsatz der EU im Bereich der Cyberdiplomatie ist und dass für Kohärenz zwischen den Cyberinitiativen der EU gesorgt werden muss, um Cyberangriffen besser begegnen zu können; sie sind gewillt, sich im Rahmen einer wirksamen politischen Koordinierung noch stärker um Cyberdialoge zu bemühen und betonen, wie wichtig der Aufbau von Cyberkapazitäten in Drittländern ist.

2. Die EU ist besorgt über die zunehmende Fähigkeit und Bereitschaft staatlicher und nichtstaatlicher Akteure, ihre Ziele durch böswillige Cyberaktivitäten von unterschiedlicher Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung zu verfolgen.

---

[1] Dok. 12109/13.
[2] Dok. 6122/15.

Die EU bekräftigt, dass böswillige Cyberaktivitäten völkerrechtswidrige Handlungen darstellen können, und betont, dass Staaten gehalten sind, von IKT-Tätigkeiten, die ihren völkerrechtlichen Verpflichtungen zuwiderlaufen, abzusehen und diese nicht wissentlich zu unterstützen und auch nicht wissentlich zuzulassen, dass auf ihrem Hoheitsgebiet mit Hilfe von IKT völkerrechtswidrige Handlungen begangen werden, wie die VN-Gruppen von Regierungssachverständigen (UN-GGE) in ihrem Bericht von 2015 erklärt haben.

3. Sie verweist auf ihre Bemühungen und die ihrer Mitgliedstaaten, die Widerstandsfähigkeit gegenüber Cyberangriffen insbesondere durch die Umsetzung der NIS-Richtlinie und der darin vorgesehenen Verfahren der operativen Zusammenarbeit zu verbessern, sowie darauf, dass böswillige, gegen Informationssysteme gerichtete Cyberaktivitäten nach EU-Recht strafbare Handlungen darstellen und die wirksame Ermittlung und Verfolgung solcher Straftaten ein gemeinsames Vorhaben der Mitgliedstaaten bleibt.

Die EU und ihre Mitgliedstaaten nehmen Kenntnis von der laufenden Arbeit der VN-Gruppe von Regierungssachverständigen (UN-GGE) für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit, die auf den Berichten aus den Jahren 2010, 2013 und 2015 aufbaut[3], und sind gewillt, entschieden an dem Konsens festzuhalten, dass das geltende Völkerrecht auch auf den Cyberraum anzuwenden ist. Die EU und ihre Mitgliedstaaten sind fest entschlossen, die Entwicklung freiwilliger, nicht bindender Normen für ein verantwortungsvolles Verhalten der Staaten im Cyberraum und die von der OSZE vereinbarten regionalen vertrauensbildenden Maßnahmen[4] zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, aktiv zu unterstützen.

Die EU bekräftigt, dass sie für eine friedliche Lösung internationaler Streitigkeiten im Cyberraum eintritt und dass alle ihre diplomatischen Bemühungen vorrangig darauf ausgerichtet sein sollten, durch eine verstärkte internationale Zusammenarbeit die Sicherheit und Stabilität im Cyberraum zu erhöhen und gegebenenfalls das Risiko einer Fehleinschätzung, Eskalation oder eines Konflikts infolge von IKT-Vorfällen zu verringern. In diesem Zusammenhang erinnert die EU daran, dass die VN-Generalversammlung die VN-Mitgliedstaaten aufgerufen hat, sich bei der Nutzung von IKT an die Empfehlungen in den Berichten der UN-GGE zu halten.

---

[3] A/68/98 und A/70/174.

[4] PC.DEC/1106 vom 3. Dezember 2013 und PC.DEC/1202 vom 10. März 2016.

4. Die EU betont, dass ein deutlicher Hinweis auf die absehbaren Konsequenzen einer gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten das Verhalten potenzieller Angreifer im Cyberraum beeinflusst und damit die Sicherheit der EU und ihrer Mitgliedstaaten erhöht. Die EU erinnert daran, dass die Zuschreibung zu einem staatlichen oder nichtstaatlichen Akteur eine auf alle verfügbaren Nachrichtenquellen gestützte, souveräne politische Entscheidung bleibt, die im Einklang mit der im Völkerrecht verankerten staatlichen Verantwortung zu treffen ist. In diesem Zusammenhang betont die EU, dass nicht alle Maßnahmen im Rahmen einer gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten die Zuschreibung zu einem staatlichen oder nichtstaatlichen Akteur erfordern.

5. Die EU bekräftigt, dass Maßnahmen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik, erforderlichenfalls einschließlich restriktiver Maßnahmen, die gemäß den einschlägigen Bestimmungen der Verträge angenommen werden, für einen Rahmen für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten geeignet sind und dazu dienen sollten, die Zusammenarbeit zu fördern, unmittelbare und langfristige Bedrohungen einzudämmen und auf lange Sicht Einfluss auf das Verhalten potenzieller Angreifer zu nehmen. Die EU wird den Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten weiter ausbauen und sich dabei von folgenden Grundsätzen leiten lassen: Die Reaktion soll

- dem Schutz der Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger dienen,
- den größeren Zusammenhang der Außenbeziehungen der EU mit dem betreffenden Staat berücksichtigen,
- dafür sorgen, dass die im Vertrag über die Europäische Union (EUV) festgelegten Ziele der GASP erreicht werden, und die dazu vorgesehenen Verfahren bereitstellen,
- auf einer gemeinsamen, zwischen den Mitgliedstaaten abgestimmten Lageerfassung beruhen und dem Bedarf in der jeweiligen konkreten Situation entsprechen,
- der Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung der Cyberaktivität angemessen sein,
- das geltende Völkerrecht achten; sie darf keine Grundrechte und -freiheiten verletzen.

6. Die EU appelliert an die Mitgliedstaaten, den Europäischen Auswärtigen Dienst (EAD) und die Kommission, die Entwicklung eines Rahmens für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten in vollem Umfang auszuführen, und bekräftigt in diesem Zusammenhang, dass sie entschlossen ist, die Arbeit an diesem Rahmen gemeinsam mit der Kommission, dem EAD und weiteren einschlägigen Beteiligten fortzusetzen und hierfür Durchführungsleitlinien, einschließlich Vorbereitungsmodalitäten und Kommunikationsverfahren, festzulegen und im Rahmen von geeigneten Übungen auszuprobieren.