Rat der
Europäischen Union

Brüssel, den 19. Oktober 2017
(OR. en)

13475/17

CYBER 155
TELECOM 242
ENFOPOL 472
JAI 941
MI 733
COSI 237
JAIEX 80
RELEX 881
IND 266

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Cybersicherheit 2.0 – Maßnahmen im Anschluss an die Tagung des Europäischen Rates und den Digital-Gipfel von Tallinn – Orientierungsaussprache

Die Europäische Kommission hat im September 2017 ein ehrgeiziges Cybersicherheitspaket veröffentlicht, in dem insbesondere die exponentiell zunehmenden Cyberbedrohungen und die Tatsache festgestellt wurden, dass böswillige Cyberaktivitäten nicht nur eine Bedrohung für unsere Volkswirtschaften und unsere Bemühungen zur Verwirklichung des digitalen Binnenmarkts darstellen, sondern auch das gesamte Funktionieren unserer Demokratien, unsere Freiheiten und unsere Werte gefährden. Die Kernelemente des Pakets sind die Gemeinsame Mitteilung "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen", der Gesetzgebungsvorschlag für einen Rechtsakt zur Cybersicherheit, mit dem das Mandat der ENISA verlängert und eine Zertifizierung vorgeschlagen wird und der bis 2018 angenommen werden sollte, sowie der Konzeptentwurf, in dem die koordinierte Reaktion auf europäischer Ebene auf Cybersicherheitsvorfälle und -krisen großen Ausmaßes dargelegt wird.

Der Rat hat zügig mehrere Schritte als Reaktion auf die von der Kommission formulierten Ziele unternommen, damit das Paket auch tatsächlich umgesetzt wird. Zunächst sind die Arbeiten für die Konsolidierung der Standpunkte des Rates in einer Reihe von Schlussfolgerungen zur Gemeinsamen Mitteilung, die vom Rat "Allgemeine Angelegenheiten" am 20. November angenommen werden sollen, schon angelaufen und gut vorangekommen. Gleichzeitig hat der Vorsitz bereits die Durchführungsleitlinien für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten finalisiert, mit denen ein Rahmen für die EU zur Nutzung aller ihr zur Verfügung stehenden politischen und diplomatischen Instrumente im Rahmen der GASP geschaffen wurde, um auf böswillige Cyberaktivitäten gegen die EU oder ihre Mitgliedstaaten zu reagieren.

Außerdem wird der Vorsitz mit der Prüfung des "Rechtsakts zur Cybersicherheit" am 20. Oktober beginnen, um dem Rat (Verkehr, Telekommunikation und Energie) auf seiner Tagung im Dezember über die Fortschritte berichten zu können. Darüber hinaus überwacht der Vorsitz genau die Umsetzung der NIS-Richtlinie durch die Mitgliedstaaten im Rahmen des Zuständigkeitsbereichs der Kooperationsgruppe und des CSIRTs-Netzwerks. Fortschritte bei der Arbeit beider Gruppen ist von wesentlicher Bedeutung für die vollständige Umsetzung der NIS-Richtlinie, die die Grundlage für weitere Fortschritte bei der Arbeit im Bereich der Cybersicherheit bildet. Diese Schritte sind in den Prioritäten des Arbeitsprogramms des Dreiervorsitzes zur Cybersicherheit[1] enthalten, das auch den künftigen Weg in anderen Bereichen der Cybersicherheit aufzeigen wird.

Die Staats- und Regierungschefs haben sich auf dem Digital-Gipfel in Tallinn vom 29. September 2017 umfassend mit Fragen der Cybersicherheit befasst. Für sie war unzweifelhaft, dass eine glaubwürdige und effiziente Cybersicherheit eindeutig mit der Schaffung unseres digitalen Binnenmarkts verbunden ist. In seinen Schlussfolgerungen zu diesen Beratungen stellte der estnische Ministerpräsident Ratas Folgendes fest: *"Wir müssen Europa bis zum Jahr 2025 zum Vorreiter in Sachen Cybersicherheit machen, um das Vertrauen, die Zuversicht und den Schutz unserer Bürger und Unternehmen online zu sichern und ein freies und durch Gesetze gesichertes Internet zu ermöglichen."*

---

1 WK 7101/2017.

Neben dieser Zielsetzung haben die führenden Politiker der EU in Tallinn hervorgehoben, wie wichtig es ist, dass die Integrität und Legitimierung der demokratischen Prozesse sichergestellt wird und die EU den Fokus eindeutig auf die Notwendigkeit eines gemeinsamen umfassenden Ansatzes für die Cybersicherheit richtet und dabei den Schwerpunkt insbesondere auf Folgendes legt:

- Notwendigkeit, auf die Schaffung einer Sicherheitszertifizierung, die auf dem neuesten Stand der Technik ist, und eines Binnenmarkts für Cybersicherheit hinzuarbeiten;
- Verbesserung der Abwehrbereitschaft auf nationaler wie auch auf EU-Ebene, um gemeinsam und wirksam auf Cybersicherheitsvorfälle großen Ausmaßes reagieren zu können, und entschlossene Bekämpfung illegale Online-Inhalte;
- stärkere Bekämpfung der Cyberkriminalität und der Nutzung des Internets für kriminelle Zwecke, auch durch Terroristen;
- bessere Zusammenarbeit zwischen den Mitgliedstaaten bei der Aus- und Weiterbildung sowie bei Sensibilisierungskampagnen im Bereich der Cybersicherheit;
- Notwendigkeit einer engeren Zusammenarbeit mit dem privaten Sektor und von Investitionen in sichere und neue Technologien, die zur Sicherheit in allen Sektoren der Wirtschaft beitragen könnten.

Zur Erreichung dieser Zielsetzung sind ein klarer politischer Wille und Ressourcen sowohl von den Organen der EU als auch den Mitgliedstaaten sowie - insbesondere angesichts eines empfindlichen Bereichs wie der Cybersicherheit - eine aktive Rolle der Mitgliedstaten bei der Steuerung der Umsetzung des Cybersicherheitspakets erforderlich. Vor diesem Hintergrund schlägt der Vorsitz vor, einen spezifischen Umsetzungszeitplan auszuarbeiten, in dem der im Entwurf der Schlussfolgerungen des Rates dargelegten konsolidierten Vision Rechnung getragen wird. Der Dreiervorsitz hat sich ferner darauf verständigt, einen Aktionsplan für die Umsetzung des Cybersicherheitspakets auszuarbeiten, der als ein fortzuschreibendes Dokument zu verstehen ist und regelmäßig überarbeitet werden soll. Dadurch wird eine Bewertung der Fortschritte auf Ebene der Arbeitsgruppe (durch die horizontale Ratsgruppe "Fragen des Cyberraums") und eine anschließende Berichterstattung an den Rat und seine Vorbereitungsgremien ermöglicht.

<u>Vor diesem Hintergrund werden die Minister ersucht, zu folgenden Fragen Stellung zu nehmen:</u>

- den konkreten Maßnahmen, die die Mitgliedstaaten zur Beschleunigung der Umsetzung der NIS-Richtlinie und zur Stärkung der Widerstandsfähigkeit und der Abwehrbereitschaft gegenüber Cyberangriffen zu ergreifen beabsichtigen;
- den im Cybersicherheitspaket dargelegten Initiativen und dazu, nach welchen Prioritäten sie im Aktionsplan gestaffelt werden sollten;
- den Schritten, die zur Förderung der Investitionen - auch aus privaten, öffentlichen und europäischen Quellen - in die Cybersicherheit unternommen werden könnten, um die Ziele der Strategie zu erreichen.