RAT DER EUROPÄISCHEN UNION

Brüssel, den 16. Mai 2014 (OR. en)

9757/14

Interinstitutionelles Dossier: 2013/0027 (COD)

TELECOM 111
DATAPROTECT 69
CYBER 27
MI 419
CSC 103
CODEC 1264

VERMERK

des	Vorsitzes
für die	Delegationen
Nr. Komm.dok.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD1 +ADD2
Nr. Vordok.:	7404/14 TELECOM 73 DATAPROTECT 39 CYBER 14 MI 242 CSC 49 CODEC 688
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union *– Entwurf eines Fortschrittsberichts*

Dieser Bericht wurde unter der Verantwortung des hellenischen Vorsitzes erstellt. In dem Bericht wird dargelegt, welche Arbeit in den Vorbereitungsgremien des Rates bereits geleistet worden ist und wie weit die Beratungen über den eingangs genannten Vorschlag gediehen sind; ferner wird eine Richtschnur im Hinblick auf die Vorbereitung der zu gegebener Zeit mit dem Europäischen Parlament aufzunehmenden Verhandlungen vorgegeben.

VERFAHRENSTECHNISCHE ASPEKTE

1. Am 12. Februar hat die Kommission ihren Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über *Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union*[1] (im Folgenden "NIS-Richtlinie"), die Artikel 114 AEUV als Rechtsgrundlage hat, übermittelt. Der Vorschlag ist Bestandteil der "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum"[2], zu der der Rat am 25. Juni 2013 Schlussfolgerungen[3] angenommen hat. Der Rat (Verkehr, Telekommunikation und Energie) hat auf seinen Tagungen vom 6. Juni[4] und 5. Dezember 2013[5] die Fortschritte zur Kenntnis genommen, die bei der Prüfung des Vorschlags für eine NIS-Richtlinie erzielt worden sind.

2. Der Europäische Wirtschafts- und Sozialausschuss[6] und der Ausschuss der Regionen[7] haben am 22. Mai bzw. 3./4. Juli 2013 zu dem Vorschlag Stellung genommen. Das Europäische Parlament hat am 13. März 2014 eine legislative Entschließung und insgesamt 138 Abänderungen angenommen, die vom Ausschuss für Binnenmarkt (IMCO) als federführendem Ausschuss zusammen mit dem Ausschuss für Industrie (ITRE) und dem Ausschuss für bürgerliche Freiheiten (LIBE) als assoziierten Ausschüssen eingebracht worden waren[8].

---

1 Dok. 6342/13.
2 Dok. 6225/13.
3 Dok. 11357/13.
4 Dok. 10076/13 und 10457/13.
5 Dok. 16630/13 und 17341/13.
6 TEN/513.
7 2013/C 280/05.
8 Dok. 7451/14.

3. Unter hellenischem Vorsitz hat die Gruppe "Telekommunikation und Informationsgesellschaft" (TELE-Gruppe) die Beratungen mit der Prüfung der einzelnen Artikel des Vorschlags in sechs Sitzungen fortgesetzt9. Auf der Grundlage der Beratungen in der TELE-Gruppe, für die der Vorsitz Diskussionspapiere erstellt hatte**10**, und der schriftlich von den meisten Mitgliedstaaten eingereichten Bemerkungen hat der hellenische Vorsitz den vorliegenden Fortschrittsbericht erstellt, in dem die Hauptaspekte des Vorschlags dargelegt werden und nach Möglichkeit eruiert wird, wo die Mitgliedstaaten sich grundsätzlich über die zu verfolgende Linie einig sind. Parallel zu diesem Sachstandsbericht hat der Vorsitz zur Verdeutlichung eine erste geänderte Fassung des Vorschlags erstellt**11**, die der TELE-Gruppe am [XXX] vorgestellt wurde und auf deren Grundlage die Beratungen unter italienischem Vorsitz im Hinblick auf die zu gegebener Zeit mit dem Europäischen Parlament zu führenden Verhandlungen fortgesetzt werden könnten.

SACHFRAGEN

Kapitel I: Allgemeine Bestimmungen (Artikel 1-3)

4. Die Delegationen billigen generell den vorgeschlagenen Gegenstand und Geltungsbereich in Artikel 1 "Gegenstand" und sind übereinstimmend der Auffassung, dass die vorgeschlagene Richtlinie ein wesentlicher Bestandteil der gesamten Cybersicherheitsstrategie der EU sein würde. Nach Einschätzung des Vorsitzes könnte die Mehrheit der Mitgliedstaaten eine gewisse Feinabstimmung des Artikels 1 anhand folgender Vorgaben unterstützen:

- *In Absatz 1 wird die Formulierung "zur Gewährleistung" durch "zur Verwirklichung" ersetzt, um zum Ausdruck zu bringen, dass die Mitgliedstaaten weder allein noch zusammen in vollem Umfang eine hundertprozentige Netz- und Informationssicherheit "gewährleisten" können.*
- *Anstatt einen neuen "Kooperationsmechanismus" für die Zusammenarbeit zwischen den Mitgliedstaaten zu schaffen, sollte in Absatz 2 Buchstabe b vielmehr auf den bestehenden Vorkehrungen aufgebaut werden, um die Mitgliedstaaten zwecks Umsetzung der Richtlinie auf strategischer/politischer Ebene "zusammenzuführen". Es sollte eine konkretere operative Zusammenarbeit ins Auge gefasst werden, beispielsweise im Zusammenhang mit den CERT*[12]*.*

---

9 Am 27. Februar, 13. und 28. März, 10. und 28. April sowie 21. Mai 2014.

10 Dok. 7404/14.

11 Dok. [XXX].

12 "CERT" bedeutet IT-Notfallteam (Computer Emergency Response Team). Es wurde darauf hingewiesen, dass, da CERT eine in der EU eingetragene Marke ist, möglicherweise in der Richtlinie ein anderer Begriff wie etwa Soforteinsatzteam für IT-Sicherheitsvorfälle (Computer security incident response team – CSIRT) verwendet werden müsste.

- *Der von einem Vorfall betroffene Mitgliedstaat und/oder sein CERT sollte entscheiden, ob, ob nicht oder inwieweit relevante Informationen (und möglicherweise personenbezogene Daten) weitergegeben werden sollten, wobei den nationalen Sicherheitsinteressen und den einschlägigen Rechtsvorschriften – insbesondere in Bezug auf den Schutz personenbezogener Daten oder für den Fall von Angriffen auf Informationssysteme – Rechnung getragen werden sollte.*
- *Es bedarf einer rechtlichen Präzisierung, um zu klären, ob die verwendete, den Binnenmarkt betreffende Rechtsgrundlage geeignet ist und die Einbeziehung "öffentlicher Verwaltungen" in die Richtlinie zulassen würde.*

5. Die Delegationen stimmen im Allgemeinen Artikel 2 ("Mindestharmonisierung") zu.

6. In Bezug auf die "Begriffsbestimmungen" in Artikel 3 stellt der Vorsitz fest, dass im Verlauf der Beratungen auf diese zurückgekommen werden muss; seines Erachtens befürworten die Delegationen generell folgende Linie:

- *Es sollte eine neue Definition für den Begriff "wesentliche Dienste" in die Begriffsbestimmungen aufgenommen werden, da damit besser bestimmt werden könnte, welche Akteure solche "wesentlichen" Dienste erbringen und welches Risiko oder welche "Bedrohung" hinsichtlich der Sicherheit dieser Dienste besteht.*
- *In der Richtlinie sollte auf eine Auflistung gemeinsamer kritischer Infrastrukturbereiche verwiesen werden, und es sollten Kriterien vorgegeben werden, anhand deren sich bestimmen lässt, welche Betreiber für diese Infrastrukturen maßgeblich sind. Die Mitgliedstaaten müssten noch konkreter werden in der Frage, wie detailliert die Richtlinie (und insbesondere Anhang II) gehalten sein müssten, und angeben, ob etwa auch "Dienste der Informationsgesellschaft" und "Erbringer grundlegender Internetdienste" von der Richtlinie erfasst werden sollten.*
- *Es sollte weiter geprüft werden, ob noch weitere Begriffsbestimmungen aufgenommen werden müssten, wie etwa für kritische IT-Dienste, den nationalen Risikomanagementplan, die NIS-Strategie und den Kooperationsplan.*

Kapitel II: Nationaler Rahmen für die Netz- und Informationssicherheit (Artikel 4-7)

7. Die Delegationen befürworten generell die Streichung des Artikels 4 ("Grundsatz").

8. Hinsichtlich des Artikels 5 ("nationale NIS-Strategie") konnte der Vorsitz breite Zustimmung zu folgender Linie verzeichnen:

- *Obwohl die Entwicklung einer NIS-Strategie einschließlich eines Kooperationsplans grundsätzlich befürwortet wird, sollte bei der Formulierung dieses Artikels stärker auf allgemeine Grundsätze der "Zukunftssicherheit" abgestellt werden und nicht so sehr auf konkrete Anforderungen an die NIS-Strategie und den Kooperationsplan, da ein solcher Ansatz am besten geeignet wäre, zur Vertrauensbildung beizutragen.*

9. Was Artikel 6 ("zuständige Behörde") anbelangt, so sind die Delegationen unter Berücksichtigung des Subsidiaritätsprinzips offensichtlich für einen Ansatz, bei dem den derzeitigen Gepflogenheiten in den Mitgliedstaaten gebührend Rechnung getragen wird:

   - *Die Richtlinie sollte den Mitgliedstaaten ein ausreichendes Maß an Flexibilität bei der Benennung oder Beibehaltung einer oder mehrerer – sektorspezifischer und strategieorientierter – zuständiger Behörden einräumen.*
   - *Die Mitgliedstaaten sollten jedoch jeweils eine "einzige Kontaktstelle" benennen.*

10. Was Artikel 7 ("IT-Notfallteam"/CERT) anbelangt, so unterstützen die Mitgliedstaaten generell die Anforderung der Richtlinie, wonach ein oder mehrere CERT einzurichten oder beizubehalten sind, bei denen es sich um dieselbe Stelle wie die "zuständige Behörde" oder die "einzige Kontaktstelle" handeln könnte; sie stimmen der in Dokument 7404/14 enthaltenen Richtschnur und insbesondere folgender Vorgabe zu:

    - *Die Mitgliedstaaten sollten über genügend Flexibilität hinsichtlich der technischen Einrichtung sowie der finanziellen und personellen Ressourcen der CERT verfügen, was im Wortlaut dieses Artikels und des Anhangs II zum Ausdruck kommen sollte; in der Richtlinie sollte jedoch entschlossen an der ehrgeizigen Zielsetzung und den Anforderungen für die CERT und für die Zusammenarbeit zwischen ihnen festgehalten werden.*

Kapitel III: Zusammenarbeit (Artikel 8-13)

11. Kapitel III des Vorschlags ist der Struktur der Zusammenarbeit in Bezug auf Netz- und Informationssicherheit gewidmet. Dem Vorsitz zufolge sind sich alle Mitgliedstaaten bewusst, dass sich durch eine gewisse Zusammenarbeit EU-weit ähnliche und höhere Niveaus der NIS-Vorsorge erreichen ließen, was auch eine gemeinsame koordinierte Reaktion auf Netz- und Informationssicherheitsprobleme erleichtern würde, wenn und wo es sich denn als notwendig erweisen sollte. Die Standpunkte müssen jedoch noch präzisiert werden in der Frage, wie ein solches strategisches/politisches Kooperationsnetz beschaffen sein sollte und welche Folgen es – wenn überhaupt – für die Bereitstellung koordinierter operativer Reaktionen auf nationale und möglicherweise grenzüberschreitende Cybervorfälle haben würde.

12. Was Artikel 8 ("Kooperationsnetz") anbelangt, so unterstützen die Delegationen nach der Überzeugung des Vorsitzes generell folgenden Ansatz:

- *In der Richtlinie sollte ein politisches/strategisches Konzept für das Kooperationsnetz niedergelegt werden, wobei zum einen auf den Kapazitäten aufgebaut wird, die nach Kapitel II zu entwickeln sind, und zum anderen eine Richtschnur für die Ausarbeitung der ausführlichen Einzelheiten der operativen Zusammenarbeit vorgegeben wird, die bereits an anderer Stelle geregelt sind (z.B. ENISA und CERT).*
- *Der Schwerpunkt der Reaktion im Notfall sollte auf die nationalen Kapazitäten wie die CERT und/oder zuständigen Behörden gelegt werden; wenn es sich in bestimmten (grenzüberschreitenden) Fällen, die noch zu präzisieren sind, als notwendig erweisen sollte, könnte eine weitere freiwillige Zusammenarbeit im Rahmen einer operativen Kooperationsgemeinschaft stattfinden, die alle 28 nationalen CERT umfasst, womit eine koordinierte Reaktion der EU gewährleistet werden soll.*
- *Gegenseitige Begutachtungen der Kapazitäten und des Bereitschaftsstands durch das Kooperationsnetz sollten auf freiwilliger Basis erfolgen.*

13. Was Artikel 9 ("sicheres System für den Informationsaustausch") anbelangt, so sind nach Feststellung des Vorsitzes die meisten Mitgliedstaaten dagegen, dass in der Richtlinie verbindliche Anforderungen an die Weitergabe von (sensiblen Geschäfts-)Informationen im Kooperationsnetz festgelegt werden und eine spezielle sichere Infrastruktur errichtet oder betrieben wird. Die Delegationen machten auch ernste Bedenken zu der vorgeschlagenen Rolle der Kommission in diesem Zusammenhang geltend. In Anbetracht dessen vertritt der Vorsitz die Auffassung, dass dieser Artikel nach folgender Vorgabe neu formuliert werden sollte:

- *Die Richtlinie sollte keinerlei verbindliche Anforderungen an den Informationsaustausch enthalten, was auch in Artikel 9 klar zum Ausdruck kommen sollte; alternativ könnte der Artikel gestrichen werden, da nichtsensible oder nicht als Verschlusssache eingestufte Informationen im Kooperationsnetz oder einschlägige Informationen zwischen den CERT ausgetauscht werden könnten.*

14. Hinsichtlich des Artikels 10 ("Frühwarnungen") können die Delegationen offensichtlich den in Dokument 7404/14 enthaltenen allgemeinen Orientierungen zustimmen; dies gilt insbesondere für Folgendes:

- *Die Ausgabe von Frühwarnungen sollte weiterhin freiwillig sein, und der Austausch der einschlägigen Informationen im Kooperationsnetz sollte in erster Linie dazu beitragen, eine Anschubwirkung auf die Vertrauensbildung zwischen dem Privatsektor und den zuständigen nationalen Stellen sowie zwischen den zuständigen nationalen Behörden untereinander zu entfalten.*
- *Da der Austausch von Informationen über Straftaten im Zusammenhang mit Angriffen auf Informationssysteme unter die Richtlinie 2013/40/EU fällt, besteht keine Notwendigkeit, im Vorschlag auf diesen Aspekt einzugehen (d.h. Streichung des Absatzes 4).*
- *Die Mitgliedstaaten sollten entscheiden, ob dem Kooperationsnetz Informationen bereitgestellt werden sollten und welche Informationen dies sind (d.h. Streichung des Absatzes 5).*
- *Frühwarnungen sollten nationale Maßnahmen zur Reaktion auf Bedrohungen und Vorfälle weder beeinträchtigen noch verzögern.*

15. Hinsichtlich des Artikels 11 ("koordinierte Reaktion") verzeichnete der Vorsitz breite Zustimmung zu den in Dokument 7404/14 enthaltenen Orientierungen; dies gilt insbesondere für Folgendes:

- *Anstatt dass eine faktische Zuständigkeit auf EU-Ebene für die Koordinierung einer Reaktion der EU auf (nationale) Vorfälle begründet wird, sind vielmehr noch weitere Beratungen erforderlich, um zu klären, ob und in welchen Fällen eine "koordinierte Reaktion" der EU erforderlich ist: nur bei größeren grenzüberschreitenden Cyberkrisen oder auch bei begrenzteren alltäglichen Vorfällen?*
- *Unter Berücksichtigung der nationalen Zuständigkeit in Sicherheitsfragen sollte die Richtlinie vielmehr auf den bestehenden Vorkehrungen zur Verwirklichung einer politischen Koordinierung auf EU-Ebene im Falle größerer Cyberkrisen aufbauen, anstatt dass neue und potenziell langsame Mechanismen eingerichtet werden.*
- *Über die politische Koordinierung auf EU-Ebene hinaus sollte die Richtlinie die technische/praktische Zusammenarbeit (beispielsweise zwischen CERT) ermöglichen, wobei weitere Anforderungen an eine operative Reaktion auf Cyberkrisen ausgearbeitet werden könnten.*

16. Der Vorsitz stellt fest, dass zwar der endgültige Standpunkt der Mitgliedstaaten zu Artikel 12 ("NIS-Kooperationsplan der Union") von den Beratungsergebnissen zu den Artikeln 8-11 abhängt, die meisten Delegationen aber billigen könnten, dass folgender Ansatz in den Text des Vorschlags Eingang findet:

- *In der Richtlinie könnte anstelle eines NIS-Kooperationsplans der Union besser ein NIS-Kooperationsrahmen der Union vorgesehen werden, der sich auf politische Koordinierung und Entwicklung konzentriert, bei dem das einschlägige Fachwissen der ENISA umfassend genutzt wird und der regelmäßig von dem gemäß Artikel 8 eingerichteten Kooperationsnetz überprüft würde.*
- *Der Kooperationsrahmen sollte sich auf Themen erstrecken wie etwa die Einzelheiten für die Kommunikation zwischen CERT, den Austausch bewährter Verfahren, die Sensibilisierung sowie Übungen und Schulungen, und diesbezüglich das Fachwissen der ENISA nutzen.*

17. Was Artikel 13 ("internationale Zusammenarbeit") anbelangt, so nahm der Vorsitz Kenntnis vom Wunsch der Mitgliedstaaten, im Text zum Ausdruck zu bringen, dass alle am Kooperationsrahmen beteiligten Mitglieder der Teilnahme von Drittstaaten oder internationalen Organisationen zustimmen müssten.

Kapitel IV: Sicherheit der Netze (Artikel 14-16), Kapitel V: Schlussbestimmungen (Artikel 17-23) sowie Anhänge I und II: CERT und Marktteilnehmer

18. Was Artikel 14 ("Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen") anbelangt, so hat der Vorsitz festgestellt, dass diejenigen Mitgliedstaaten, in denen die nationale Praxis freiwilliger Meldungen zu einem zufriedenstellenden Niveau der Zusammenarbeit zwischen Akteuren und Behörden geführt hat, es vorziehen würden, wenn die Richtlinie an diese Erfahrung anknüpfen würde. Andere Mitgliedstaaten fragen sich, ob darüber hinaus Vorschriften über eine verbindliche Meldepflicht eingeführt werden sollten. Alle Mitgliedstaaten sind sich einig, dass weitere Präzisierungen zu den einzelnen Meldeanforderungen, die sich in verschiedenen Rechtsvorschriften der Union finden, notwendig sind. In Anbetracht dessen empfiehlt der Vorsitz folgenden Ansatz:

- *Die Richtlinie könnte verbindliche Meldeanforderungen für Vorfälle mit erheblichen grenzüberschreitenden Auswirkungen festlegen, die mehrere Mitgliedstaaten betreffen.*
- *Bei Vorfällen im Inland mit begrenzten Auswirkungen sollten die Mitgliedstaaten flexibel im Einklang mit Artikel 2 darüber entscheiden dürfen, ob und wie Meldungen auf nationaler Ebene erfolgen sollen.*

- *In der Richtlinie sollten die Parameter für die Bestimmung der Auswirkungen von (sektorspezifischen) Vorfällen festgelegt werden, aber es sollte Sache der Mitgliedstaaten sein, anhand dieser Parameter zu entscheiden, ob ein bestimmter Vorfall gemeldet werden sollte.*
- *Den Mitgliedstaaten sollte Flexibilität hinsichtlich der Meldung an die für den jeweiligen Sektor zuständigen Behörden eingeräumt werden, die dann ihrerseits der nationalen "einzigen Kontaktstelle" Bericht erstatten könnten.*

19. Zu Artikel 15 ("Umsetzung und Durchsetzung") schlägt der Vorsitz auf der Grundlage der Stellungnahmen der Delegationen Folgendes vor:

    - *Die Richtlinie sollte genügend Raum für nationale Lösungen belassen, damit der Privatsektor – stärker als derzeit vorgeschlagen – eingebunden werden kann, beispielsweise im Hinblick auf Sicherheitsüberprüfungen, Aufbau technischer Kapazitäten, Schulungskurse usw.*
    - *In der Richtlinie sollte auch vorgesehen werden, dass, soweit angezeigt, mehrere, für einzelne Sektoren zuständige Behörden, die auch über Durchführungs- und Durchsetzungsbefugnisse verfügen, vorhanden sein können.*

20. Was die Frage der "Normung" gemäß Artikel 16 anbelangt, so gelangt der Vorsitz zu dem Schluss, dass die Delegationen keine Notwendigkeit für eine Umformulierung des Artikels erkennen können.

21. Zu Artikel 17 ("Sanktionen"), insbesondere Absatz 2, bedarf es weiterer Überlegungen, um das Verhältnis zwischen der NIS-Richtlinie und der künftigen Datenschutzverordnung weiter zu präzisieren.

22. Abschließend stellt der Vorsitz fest, dass die Delegationen zu einem späteren Zeitpunkt auf die Umsetzungsfrist und das "Inkrafttreten" (Artikel 21 und 22) zurückkommen möchten und dass auf die Endfassung des ANHANGS I betreffend die in den Geltungsbereich fallenden Aufgaben der CERT und die Anforderungen an diese sowie auf die Endfassung des ANHANGS II betreffend die in eine erschöpfende oder indikative Liste aufzunehmenden Sektoren oder Rechtssubjekte je nach dem Ergebnis der Verhandlungen über den Inhalt der Artikel des Vorschlags später nochmals eingegangen werden müsste.

FAZIT

23. Der hellenische Vorsitz hat festgestellt, dass sich alle Mitgliedstaaten ohne Ausnahme sehr wohl bewusst sind, dass die Netz- und Informationssicherheit dringend verbessert werden muss und diesbezüglich auf der Ebene der EU zu handeln ist. In diesem Zusammenhang haben die Mitgliedstaaten den Vorschlag der Kommission äußerst aufmerksam geprüft, und in den letzten Monaten sind bei der Bestimmung der Richtung, in die der Vorschlag sich weiterentwickeln sollte, beträchtliche Fortschritte – wie vorstehend dargelegt – erzielt worden.

24. Was die Bestimmungen der Kapitel I, II und IV anbelangt, so vertritt der Vorsitz infolge der Beratungen in den Vorbereitungsgremien des Rates die Auffassung, dass die in diesem Fortschrittsbericht vorgeschlagenen Orientierungen und Schlussfolgerungen als Grundlage für die weitere Bearbeitung des Vorschlags unter dem künftigen italienischen Vorsitz ausreichen dürften. Diese Orientierungen und Schlussfolgerungen wurden in dem Bestreben zusammengestellt, ein ausgewogenes Gleichgewicht zwischen einer Verbesserung der Cybersicherheit, dem Aufbau des notwendigen Vertrauens und – effizienzhalber – der umfassenden Nutzung vorhandenen Fachwissens zu finden und Doppelungen hinsichtlich der Fachkompetenz bestehender Stellen und Mechanismen zu vermeiden.

25. Was Kapitel III anbelangt, so sind sich die Mitgliedstaaten, wie bereits (in Nummer 11) festgestellt, darin einig, dass die strategische/politische Zusammenarbeit in Bezug auf Netz- und Informationssicherheit auf der Ebene der EU verstärkt werden muss. Eine Reihe von Mitgliedstaaten vertritt die Auffassung, dass in der Richtlinie mehr spezifische Kriterien und Anforderungen für die operative Zusammenarbeit bei NIS-Vorfällen angegeben werden sollten. Die meisten Mitgliedstaaten betrachten jedoch die strategische/politische Zusammenarbeit als erste Priorität für den Aufbau des notwendigen Vertrauens, wobei gleichzeitig die Einzelheiten der operativen Zusammenarbeit im Rahmen der bestehenden Mechanismen und Stellen weiter ausgearbeitet werden könnten. Wie bereits (in den Nummern 11-17) angemerkt, ist der Vorsitz zwar nicht der Auffassung, dass die strategische/politische Zusammenarbeit und die operative Zusammenarbeit einander ausschließende Optionen darstellen, ist aber der Überzeugung, dass in der Richtlinie der strategischen/politischen Zusammenarbeit der Vorrang eingeräumt werden sollte, wobei gleichzeitig den bestehenden Mechanismen und Stellen eine Richtschnur für die operative Zusammenarbeit vermittelt werden sollte.

*

* *

Der Vorsitz wird dem Rat diesen Fortschrittsbericht zur Kenntnisnahme vorlegen, nachdem ihn der AStV am 28. Mai geprüft hat.