

---

**Vorsitz: Deutschland****1092. PLENARSITZUNG DES RATES**

1. Datum: Donnerstag, 10. März 2016  
  
Beginn: 10.10 Uhr  
Unterbrechung: 13.00 Uhr  
Wiederaufnahme: 15.30 Uhr  
Schluss: 17.50 Uhr
  
2. Vorsitz: Botschafter E. Pohl  
C. Weil
  
3. Behandelte Fragen – Erklärungen – Beschlüsse/verabschiedete Dokumente:  
  
Punkt 1 der Tagesordnung: **BESCHLUSS ÜBER VERTRAUENSBILENDE  
MASSNAHMEN DER OSZE ZUR VERMINDE-  
RUNG DER KONFLIKTRISIKEN, DIE SICH AUS  
DEM EINSATZ VON INFORMATIONEN- UND  
KOMMUNIKATIONSTECHNOLOGIEN ERGEBEN**

Vorsitz

**Beschluss:** Der Ständige Rat verabschiedete den Beschluss Nr. 1202 (PC.DEC/1202) über vertrauensbildende Maßnahmen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben; der Wortlaut des Beschlusses ist diesem Journal beigelegt.

Russische Föderation (Anhang 1), Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien, Montenegro und Serbien; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; den Mitgliedern des Europäischen Wirtschaftsraums und EFTA-Ländern Island und Norwegen; sowie mit Andorra, Georgien, Moldau, San Marino und der Ukraine) (Anhang 2), Vereinigte Staaten von Amerika (Anhang 3), Vorsitz

Punkt 2 der Tagesordnung: REDE DES STAATSSSEKRETÄRS IM DEUTSCHEN  
BUNDESMINISTERIUM FÜR FAMILIE,  
SENIOREN, FRAUEN UND JUGEND, RALF  
KLEINDIEK

Vorsitz, Staatssekretärs im deutschen Bundesministerium für Familie, Senioren, Frauen und Jugend (CIO.GAL/35/16 OSCE+), Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien, Montenegro und Serbien; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; den Mitgliedern des Europäischen Wirtschaftsraums und EFTA-Ländern Island und Liechtenstein; sowie mit Andorra, Georgien, Moldau, San Marino und der Ukraine) (PC.DEL/286/16/Rev.1), Vereinigte Staaten von Amerika (PC.DEL/288/16), Russische Föderation (PC.DEL/309/16), Schweiz (PC.DEL/301/16 OSCE+), Türkei (PC.DEL/329/16 OSCE+), Kanada, Österreich (auch im Namen Finnlands, Kasachstans und der Türkei), Norwegen (PC.DEL/321/16), Belarus (PC.DEL/317/16 OSCE+), Aserbaidzhan (PC.DEL/298/16 OSCE+), Heiliger Stuhl (PC.DEL/299/16 OSCE+)

Punkt 3 der Tagesordnung: BERICHT DER OSZE-BEAUFTRAGTEN FÜR  
MEDIENFREIHEIT

Vorsitz, OSZE-Beauftragte für Medienfreiheit (FOM.GAL/3/16/Rev.1), Vereinigte Staaten von Amerika (PC.DEL/290/16), Russische Föderation (PC.DEL/310/16), Schweiz (PC.DEL/303/16 OSCE+), Türkei (PC.DEL/324/16 OSCE+), Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien und Montenegro; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; dem Mitglied des Europäischen Wirtschaftsraums und EFTA-Land Island; sowie mit Moldau und der Ukraine) (PC.DEL/318/16), Kanada, Ukraine (PC.DEL/308/16 OSCE+), Norwegen (PC.DEL/322/16), Moldau, Armenien, Heiliger Stuhl (PC.DEL/300/16 OSCE+), Montenegro (PC.DEL/320/16 OSCE+), Georgien (PC.DEL/315/16 OSCE+), Kasachstan, Albanien (PC.DEL/291/16), Österreich, Serbien, Norwegen (auch im Namen Schwedens) (PC.DEL/323/16), Bosnien und Herzegowina (PC.DEL/316/16 OSCE+)

Punkt 4 der Tagesordnung: PRÜFUNG AKTUELLER FRAGEN

Frankreich

- (a) *Fortgesetzte Aggression gegen die Ukraine und anhaltende Verletzungen der OSZE-Prinzipien und -Verpflichtungen durch die Russische Föderation:* Ukraine (PC.DEL/302/16), Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien und Montenegro; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; den Mitgliedern des Europäischen Wirtschaftsraums und EFTA-Ländern Island, Liechtenstein

und Norwegen; sowie mit Georgien, Moldau, San Marino und der Ukraine) (PC.DEL/295/16), Vereinigte Staaten von Amerika (PC.DEL/307/16), Schweiz (PC.DEL/305/16 OSCE+), Türkei (PC.DEL/325/16 OSCE+), Kanada

- (b) *Die Lage in der Ukraine und die Notwendigkeit, die Minsker Vereinbarungen umzusetzen*: Russische Föderation (PC.DEL/314/16), Ukraine
- (c) *Entführung und widerrechtliches Festhalten ukrainischer Staatsbürger durch die Russische Föderation*: Ukraine (PC.DEL/306/16 OSCE+), Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien und Montenegro; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; dem Mitglied des Europäischen Wirtschaftsraums und EFTA-Land Island; sowie mit Georgien, Moldau, San Marino und der Ukraine) (PC.DEL/296/16/Rev.2), Vereinigte Staaten von Amerika (PC.DEL/294/16), Kanada, Schweiz (PC.DEL/304/16 OSCE+), Norwegen, Russische Föderation (PC.DEL/313/16), Vorsitz
- (d) *Medienfreiheit in der Türkei*: Niederlande – Europäische Union (mit den Bewerberländern Albanien, ehemalige jugoslawische Republik Mazedonien, Montenegro und Serbien; dem Land des Stabilisierungs- und Assoziierungsprozesses und potenziellen Bewerberland Bosnien und Herzegowina; dem Mitglied des Europäischen Wirtschaftsraums und EFTA-Land Island; sowie mit Armenien) (PC.DEL/297/16), Vereinigte Staaten von Amerika (PC.DEL/292/16), Schweiz (auch im Namen Kanadas, Islands und Norwegens), Türkei (PC.DEL/326/16 OSCE+), Russische Föderation (PC.DEL/312/16)

Punkt 5 der Tagesordnung:   BERICHT ÜBER DIE TÄTIGKEIT DES  
AMTIERENDEN VORSITZENDEN

- (a) *Teilnahme des Amtierenden Vorsitzenden an einem Treffen der Außenminister des Normandie-Formats am 3. März 2016 in Paris*: Vorsitz (CIO.GAL/34/16)
- (b) *Verurteilung des Anschlags in Tunesien vom 7. März 2016 durch den Amtierenden Vorsitzenden und den Generalsekretär der OSZE*: Vorsitz (CIO.GAL/34/16)
- (c) *Besuch des Sonderbeauftragten des Amtierenden Vorsitzenden der OSZE für den Südkaukasus, Botschafter Bächler, in Tiflis, Zchinwali, Suchumi und Moskau vom 29. Februar bis 10. März 2016*: Vorsitz (CIO.GAL/34/16)

Punkt 6 der Tagesordnung:   BERICHT DES GENERALSEKRETÄRS

- (a) *Security Days zum Thema „Sicherheit und Migration erneut im Blickfeld: Brückenbildung zwischen nationalen und regionalen Reaktionen“ am 4. März 2016 in Rom*: Direktor des Konfliktverhütungszentrums (SEC.GAL/39/16 OSCE+)

- (b) *Podiumsdiskussion zum Thema „Die EU, die OSZE und die Zukunft der europäischen Sicherheit“ am 8. März 2016 in Rom: Direktor des Konfliktverhütungszentrums (SEC.GAL/39/16 OSCE+)*
- (c) *OSZE/UNODC-Gespräche auf Mitarbeiterenebene und Unterzeichnung eines Gemeinsamen Aktionsplans für 2016 – 2017 am 9. März 2016 in Wien: Direktor des Konfliktverhütungszentrums (SEC.GAL/39/16 OSCE+)*

Punkt 7 der Tagesordnung: SONSTIGES

- (a) *Maßnahmen im Anschluss an die am 4. März 2016 in Rom abgehaltenen Security Days zum Thema „Sicherheit und Migration erneut im Blickfeld: Brückenbildung zwischen nationalen und regionalen Reaktionen“: Vorsitz, Schweiz (PC.DEL/327/16 OSCE+)*
- (b) *Aufruf zur Nominierung von Kandidaten für den Posten des Leitenden Beobachters der Beobachtermission der OSZE an zwei russischen Kontrollposten an der russisch-ukrainischen Grenze und den Posten des Leiters des OSZE-Zentrums in Aschabat: Vorsitz*
- (c) *Parlamentswahlen in Serbien am 24. April 2016: Serbien*
- (d) *Ankündigung eines Treffens der Mittelmeer-Kontaktgruppe am 14. März 2016: Österreich*

4. Nächste Sitzung:

Donnerstag, 17. März 2016, um 10.00 Uhr im Neuen Saal

---

**1092. Plenarsitzung**

StR-Journal Nr. 1092, Punkt 1 der Tagesordnung

**ERKLÄRUNG  
DER DELEGATION DER RUSSISCHEN FÖDERATION**

Sehr geehrter Herr Vorsitzender,

die Russische Föderation hat sich dem Konsens zum Beschluss des Ständigen Rates über einen zusätzlichen Satz von vertrauensbildenden Maßnahmen im Sicherheitsbereich bei der Nutzung von Informations- und Telekommunikationstechnologien angeschlossen.

Die Verabschiedung zusätzlicher vertrauensbildender Maßnahmen im Rahmen der OSZE ist das Ergebnis der konstruktiven Zusammenarbeit aller Teilnehmer am Verhandlungsprozess in der informellen Arbeitsgruppe, deren Sitzungen unter amerikanischem Vorsitz stattfanden. Besonders erwähnen möchten wir den Beitrag des deutschen Vorsitzes, der maßgeblich am Zustandekommen eines von Kompromissen geprägten Textes, der die Interessen aller Parteien berücksichtigt, beteiligt war.

Wir möchten die Wichtigkeit der in dem zusätzlichen Satz von Maßnahmen enthaltenen Bestimmungen über die Freiwilligkeit dieser Maßnahmen, die maßgebliche Rolle der Staaten bei der Umsetzung der praktischen Zusammenarbeit im Bereich des Schutzes kritischer Informationsinfrastruktur und die Notwendigkeit des Informationsaustauschs über autorisierte und geschützte Nachrichtenkanäle betonen.

Die Tatsache, dass sich die OSZE auf diese vertrauensbildenden Maßnahmen geeinigt hat, zeigt, dass ein Konsens in Fragen von grundsätzlicher Bedeutung im Zusammenhang mit der Gewährleistung der internationalen Informationssicherheit unabhängig von der politischen Konjunktur zustande kommen kann. Wir halten es für wichtig, dass die internationale Zusammenarbeit in diesem Bereich stetig ausgebaut wird.

Wir ersuchen um Beifügung unserer Erklärung zum Journal der heutigen Sitzung des Ständigen Rates unter dem betreffenden Tagesordnungspunkt.

Ich danke für Ihre Aufmerksamkeit.

---

**1092. Plenarsitzung**

StR-Journal Nr. 1092, Punkt 1 der Tagesordnung

**ERKLÄRUNG  
DES VERTRETERS DER EUROPÄISCHEN UNION**

Die Delegation der Niederlande als EU-Vorsitzland erteilte dem Vertreter der Europäischen Union das Wort, der folgende Erklärung abgab:

„Die Europäische Union und ihre Mitgliedstaaten begrüßen die Verabschiedung der zusätzlichen vertrauensbildenden Maßnahmen in Bezug auf das Internet, durch die die Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, verringert werden sollen. Dieser Beschluss ergänzt und verstärkt den ersten Satz von VBM aus dem Jahr 2013 – der erste seiner Art, der je von einer Regionalorganisation verabschiedet wurde. Er stellt einen bedeutenden Schritt hin zur multilateralen Zusammenarbeit im dynamischen Cyber-Bereich dar. Zusammengenommen sind diese Risikominderungsmaßnahmen eine beachtliche Errungenschaft, verbessern sie doch die Zusammenarbeit zwischen den Staaten, die Transparenz, die Berechenbarkeit und die Stabilität zwischen den Teilnehmerstaaten.

Wir danken den aufeinanderfolgenden Vorsitzen, dem US-Vorsitz der Informellen Arbeitsgruppe und ihren Teams sowie dem Sekretariat der OSZE für ihren enormen Einsatz. Wir gratulieren allen Teilnehmerstaaten dazu, dass sie keine Mühen gescheut haben, um diese praktischen Maßnahmen zu entwickeln, und zu ihrer konstruktiven Einstellung, die es möglich gemacht haben, schon zu Beginn dieses Jahres zu einem Konsens zu gelangen. Allein die Tatsache, dass eine inklusive und repräsentative Organisation wie die OSZE sich erfolgreich mit einem so sensiblen und komplexen Prozess befasst, übermittelt die gewichtige politische und öffentliche Botschaft, dass jeder einzelne Teilnehmerstaat entschlossen ist, einen Beitrag zu dieser wichtigen gemeinsamen Anstrengung zu leisten. Sie ergänzt außerdem die bisherige Leistungsbilanz der OSZE im Bereich der Vertrauensbildung zwischen den Teilnehmerstaaten umfassend und dimensionsübergreifend.

Herr Vorsitzender,

die Wahrung eines friedlichen, offenen, freien und sicheren Cyberspace ist eine globale Herausforderung, der wir uns gemeinsam mit den maßgeblichen internationalen Partnern und Organisationen, dem Privatsektor und der Zivilgesellschaft stellen sollten. Wir werden uns auch von den Grundwerten der Europäischen Union – der Menschenwürde,

Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und Achtung der Grundrechte – leiten lassen.

Liebe Kollegen,

der heute verabschiedete Beschluss ist sicherlich ein Erfolg, doch der Prozess ist hier noch nicht zu Ende. Allen Teilnehmerstaaten muss bewusst sein, dass die Umsetzung der ursprünglichen VBM unverändert Vorrang haben sollte. Wir werden unsere Zusagen weiter praktisch umsetzen, während wir den Blick in die Zukunft richten und uns nach weiteren vertrauensbildenden Maßnahmen umsehen, die geeignet sind, Vertrauen, Zusammenarbeit und Stabilität im Cyber-Bereich aufzubauen und zu festigen.

Die Bewerberländer ehemalige jugoslawische Republik Mazedonien<sup>1</sup>, Montenegro<sup>1</sup>, Serbien<sup>1</sup> und Albanien<sup>1</sup>, das Land des Stabilisierungs- und Assoziierungsprozesses und potenzielle Bewerberland Bosnien und Herzegowina, die Mitglieder des Europäischen Wirtschaftsraums und EFTA-Länder Island und Norwegen sowie die die Ukraine, die Republik Moldau, Georgien, Andorra und San Marino schließen sich dieser Erklärung an.“

---

1 Die ehemalige jugoslawische Republik Mazedonien, Montenegro und Albanien nehmen auch weiterhin am Stabilisierungs- und Assoziierungsprozess teil.

---

**1092. Plenarsitzung**

StR-Journal Nr. 1092, Punkt 1 der Tagesordnung

**ERKLÄRUNG  
DER DELEGATION DER VEREINIGTEN STAATEN VON AMERIKA**

Die Vereinigten Staaten begrüßen die Verabschiedung zusätzlicher vertrauensbildender Maßnahmen (VBM) in Bezug auf das Internet zur Verbesserung der Zusammenarbeit zwischen den Staaten, der Transparenz, der Berechenbarkeit und der Stabilität zwischen den Teilnehmerstaaten. Diese praktischen Risikominderungsmaßnahmen bauen auf einem früheren Satz von VBM aus dem Jahr 2013 auf, die damals auf internationaler Ebene einmalig waren.

Die OSZE erweist sich weiter als Vorreiter im Cyber-Bereich. Die soeben verabschiedeten VBM ergänzen unseren systematischen freiwilligen Informationsaustausch und ermutigen zu gemeinsamen Aktivitäten in Bezug auf sicherheitspolitische Herausforderungen, mit denen wir alle konfrontiert sind. Das ist vor allem dann von besonderer Bedeutung, wenn kritische, lebenswichtige Infrastruktur der Teilnehmerstaaten, etwa Stromnetze, über Netzwerke laufen, die an das Internet angeschlossen sind. Angesichts zunehmend raffinierterer Cyber-Angriffe von globalem Charakter, die buchstäblich unentdeckbar sind, helfen VBM mit, die Ursachen für Misstrauen, Furcht und Spannungen zu verringern oder zu beseitigen bzw. bestehendes Vertrauen zu stärken.

Die Vereinigten Staaten haben diesen Beschluss befürwortet, da sie der festen Überzeugung sind, dass die Informations- und Kommunikationstechnologien, gemeinsam mit dem Internet, das sie verbindet, leistungsfähige Instrumente für die Förderung der Menschenrechte, insbesondere des Rechts auf freie Meinungsäußerung, der Vereinigungsfreiheit und des Rechts auf friedliche Versammlung, sind.

Wir bekräftigen außerdem unser festes Bekenntnis zu einer Internet-Governance unter Einbeziehung zahlreicher Interessengruppen (*multi-stakeholder approach*), die sich durch transparente, von unten nach oben gerichtete, konsensgetragene Prozesse auszeichnet und die legitimen Interessen der Regierungen, des Privatsektors, der Zivilgesellschaft und der technischen Gemeinschaft berücksichtigt.

Die Vereinigten Staaten hatten die Ehre, in der Informellen Arbeitsgruppe (IWG), die diese VBM ausarbeiten sollte, den Vorsitz zu führen. Viele Delegationen arbeiteten hart daran, eine Einigung zu den VBM zu erreichen, und wir möchten allen Sachverständigen in den Hauptstädten danken, die diese Verhandlungen durch fachliche Beratung unterstützt



haben und auch eigens angereist sind. Als Vorsitz der IWG werden die Vereinigten Staaten auch weiterhin einen auf zwei Schwerpunkte gestützten Ansatz verfolgen: einerseits die Betonung der Umsetzung unserer bestehenden Verpflichtungen und andererseits die Suche nach zusätzlichen Maßnahmen, die geeignet sind, die zwischenstaatliche Zusammenarbeit und Stabilität zu verstärken. Wir sehen weiteren Fortschritten in der Arbeit dieser Gruppe in den verbleibenden Sitzungen dieses Jahres mit Zuversicht entgegen.

Ich danke Ihnen, Herr Vorsitzender, und ich möchte Sie bitten, diese Erklärung dem Journal des Tages beizufügen

**1092. Plenarsitzung**

StR-Journal Nr. 1092, Punkt 1 der Tagesordnung

**BESCHLUSS Nr. 1202  
VERTRAUENSBLDENE MASSNAHMEN DER OSZE  
ZUR VERMINDERUNG DER KONFLIKTRISIKEN, DIE SICH  
AUS DEM EINSATZ VON INFORMATIONEN- UND  
KOMMUNIKATIONSTECHNOLOGIEN ERGEBEN**

Die OSZE-Teilnehmerstaaten kamen im Beschluss Nr. 1039 des Ständigen Rates (26. April 2012) überein, die individuellen und kollektiven Bemühungen um die Sicherheit der Informations- und Kommunikationstechnologien (ICTs) und von deren Nutzung (im Folgenden als „Sicherheit der ICTs und von deren Nutzung“ bezeichnet) umfassend und dimensionsübergreifend im Einklang mit den OSZE-Verpflichtungen und in Zusammenarbeit mit einschlägigen internationalen Organisationen zu verstärken. Ferner beschlossen sie, einen Satz von Entwürfen für vertrauensbildende Maßnahmen (VBMs) auszuarbeiten, die die zwischenstaatliche Zusammenarbeit, Transparenz, Berechenbarkeit und Stabilität stärken und das gegebenenfalls mit der ICT-Nutzung verbundene Risiko einer Fehleinschätzung, Eskalation oder eines Konflikts vermindern sollen.

Unter Hinweis auf die Rolle der OSZE als regionale Abmachung im Sinne von Kapitel VIII der UN-Charta bekräftigen die OSZE-Teilnehmerstaaten, dass die in der OSZE ausgearbeiteten VBMs die Bemühungen der Vereinten Nationen zur Förderung von VBMs im Bereich der Sicherheit der ICTs und von deren Nutzung ergänzen. Die Umsetzung der vertrauensbildenden Maßnahmen der OSZE im Bereich der Sicherheit der ICTs und von deren Nutzung durch die OSZE-Teilnehmerstaaten erfolgt im Einklang mit dem Völkerrecht, darunter unter anderem die UN-Charta und der Internationale Pakt über bürgerliche und politische Rechte, sowie mit der Schlussakte von Helsinki und ihrer Verpflichtung zur Achtung der Menschenrechte und Grundfreiheiten.

Die folgenden VBMs wurden erstmals mit Beschluss Nr. 1106 des Ständigen Rates vom 3. Dezember 2013 verabschiedet:

1. Die Teilnehmerstaaten stellen ihre nationalen Sichtweisen zu verschiedenen Aspekten nationaler und grenzüberschreitender Bedrohungen für die ICTs und deren Nutzung auf freiwilliger Basis zur Verfügung. Den Umfang dieser Informationen bestimmen die bereitstellenden Staaten.

2. Die Teilnehmerstaaten erleichtern auf freiwilliger Basis die Zusammenarbeit zwischen den zuständigen nationalen Dienststellen und den Informationsaustausch betreffend die Sicherheit der ICTs und von deren Nutzung.
3. Die Teilnehmerstaaten führen auf freiwilliger Basis und auf geeigneter Ebene Konsultationen durch, um das Risiko von Fehleinschätzungen und möglichen politischen oder militärischen Spannungen oder Konflikten, die sich aus der Nutzung von ICTs ergeben könnten, zu vermindern und kritische nationale und internationale ICT-Infrastrukturen, einschließlich deren Integrität, zu schützen.
4. Die Teilnehmerstaaten tauschen auf freiwilliger Basis Informationen über die von ihnen veranlassten Maßnahmen zur Gewährleistung eines offenen, interoperablen, sicheren und verlässlichen Internets aus.
5. Die Teilnehmerstaaten nutzen die OSZE als Plattform für Dialog, den Austausch bewährter Methoden, Bewusstseinsbildung und Information über den Aufbau von Kapazitäten betreffend die Sicherheit der ICTs und von deren Nutzung, einschließlich wirksamer Maßnahmen gegen diesbezügliche Bedrohungen. Außerdem werden sie Möglichkeiten überlegen, wie die Rolle der OSZE in diesem Bereich ausgebaut werden kann.
6. Den Teilnehmerstaaten wird nahegelegt, für zeitgemäße und wirksame nationale Rechtsvorschriften zu sorgen, die die bilaterale Zusammenarbeit und einen wirksamen zeitnahen Informationsaustausch zwischen den zuständigen Behörden der Teilnehmerstaaten, einschließlich der Strafvollzugsorgane, auf freiwilliger Basis erleichtern, um die Nutzung der ICTs zu terroristischen oder kriminellen Zwecken zu verhindern. Die OSZE-Teilnehmerstaaten sind sich darin einig, dass die OSZE die über bestehende Strafverfolgungskanäle laufenden Bemühungen nicht duplizieren darf.
7. Die Teilnehmerstaaten informieren auf freiwilliger Basis über ihre nationale Organisation sowie über ihre nationalen Strategien, politischen Konzepte und Programme – auch hinsichtlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor –, die für die Sicherheit der ICTs und von deren Nutzung von Belang sind; den Umfang dieser Informationen bestimmen die bereitstellenden Staaten.
8. Die Teilnehmerstaaten bestimmen eine Kontaktstelle, um zweckdienliche Mitteilungen und den einschlägigen Dialog über die Sicherheit der ICTs und von deren Nutzung zu erleichtern. Sie geben auf freiwilliger Basis die Kontaktdaten bestehender amtlicher nationaler Einrichtungen bekannt, die mit Zwischenfällen im ICT-Bereich befasst sind und entsprechende Reaktionen koordinieren, um einen direkten Dialog zu ermöglichen und das Zusammenwirken zwischen den zuständigen nationalen Dienststellen und Experten zu erleichtern. Die Teilnehmerstaaten werden die Kontaktinformationen jährlich aktualisieren und Änderungen spätestens dreißig Tage nach Eintritt der Änderung bekanntgeben. Die Teilnehmerstaaten ergreifen freiwillig Maßnahmen zur Gewährleistung einer schnellen Kommunikation auf politisch zuständiger Ebene, damit Bedenken auf der nationalen Sicherheitsebene zur Sprache gebracht werden können.
9. Um die Gefahr von Missverständnissen, die sich durch das Fehlen vereinbarter Begriffsbestimmungen ergeben können, möglichst gering zu halten und im Interesse der Kontinuität des Dialogs stellen die Teilnehmerstaaten als ersten Schritt freiwillig eine Liste ihrer im Inland im Zusammenhang mit der Sicherheit der ICTs und von deren Nutzung

verwendeten Begriffe samt einer Erklärung oder Definition der einzelnen Begriffe zur Verfügung. Jeder Teilnehmerstaat wählt dazu auf freiwilliger Basis jene Begriffe aus, deren Weitergabe er für besonders zweckmäßig hält. Auf längere Sicht nehmen sich die Teilnehmerstaaten vor, ein einvernehmliches Glossar zu erstellen.

10. Zur Erleichterung der Kommunikation über die VBMs nutzen die Teilnehmerstaaten für ihren freiwilligen Meinungsaustausch – vorbehaltlich des einschlägigen OSZE-Beschlusses – die Plattformen und Mechanismen der OSZE, unter anderem das vom Konfliktverhütungszentrum des OSZE-Sekretariats betriebene OSZE-Kommunikationsnetz.

11. Die Teilnehmerstaaten treten auf Ebene der benannten nationalen Experten alljährlich mindestens dreimal im Rahmen des Sicherheitsausschusses und von dessen mit Beschluss Nr. 1039 des Ständigen Rates eingesetzter Informeller Arbeitsgruppe (IWG) zusammen, um die ausgetauschten Informationen zu besprechen und Überlegungen über eine entsprechende Weiterentwicklung der VBMs anzustellen. Kandidaten für die weitere Prüfung durch die IWG könnten unter anderem Vorschläge aus der vom Vorsitz der IWG am 9. Juli 2012 unter der Dokumentennummer PC.DEL/682/12 verteilten konsolidierten Liste sein, über die nach entsprechender Diskussion mit Konsens zu entscheiden sein wird.

Die folgenden VBMs wurden erstmals mit Beschluss Nr. 1202 des Ständigen Rates vom 10. März 2016 verabschiedet:

12. Die Teilnehmerstaaten tauschen auf freiwilliger Basis Informationen aus und fördern den Austausch zwischen den Staaten in verschiedenen Formaten – darunter Workshops, Seminare und Runde Tische –, auch auf regionaler bzw. subregionaler Ebene, um das Spektrum an kooperativen Maßnahmen sowie anderen Prozessen und Mechanismen auszuloten, die die Teilnehmerstaaten zur Verringerung der Konfliktrisiken, die sich aus der Nutzung von ICTs ergeben, befähigen könnten. Diese Aktivitäten sollten darauf abzielen, Konflikte, die sich aus der Nutzung von ICTs ergeben, zu verhüten und eine friedliche Nutzung von ICTs aufrechtzuerhalten.

Im Hinblick auf diese Aktivitäten wird den Teilnehmerstaaten unter anderem nahegelegt,

- die Aktivitäten in einem Geiste durchzuführen, der die zwischenstaatliche Zusammenarbeit, Transparenz, Berechenbarkeit und Stabilität stärkt;
- mit diesen Aktivitäten die Bemühungen der Vereinten Nationen zu ergänzen und Überschneidungen mit der Arbeit anderer Foren zu vermeiden und
- die Erfordernisse und Anforderungen der Teilnehmerstaaten, die sich an diesen Aktivitäten beteiligen, zu berücksichtigen.

Den Teilnehmerstaaten wird nahegelegt, Vertreter aus dem Privatsektor, der Wissenschaft, von Exzellenzzentren und aus der Zivilgesellschaft einzuladen und in diese Aktivitäten einzubinden.

13. Die Teilnehmerstaaten führen auf freiwilliger Basis Aktivitäten für Beamte und Sachverständige durch, um autorisierte und geschützte Kommunikationskanäle zu ermöglichen und das Risiko einer Fehleinschätzung, Eskalation oder eines Konflikts zu

vermeiden bzw. zu verringern und die technischen, rechtlichen und diplomatischen Mechanismen zur Behandlung ICT-relevanter Ersuchen abzuklären. Dies schließt die Nutzung der Kommunikationskanäle im Sinne von Beschluss Nr. 1106 des Ständigen Rates nicht aus.

14. Die Teilnehmerstaaten fördern auf freiwilliger Basis und im Einklang mit den nationalen Rechtsvorschriften öffentlich-private Partnerschaften und entwickeln Mechanismen für den Austausch bewährter Verfahren im Vorgehen gegen gemeinsame Sicherheits Herausforderungen, die sich aus der Nutzung von ICTs ergeben.

15. Die Teilnehmerstaaten fördern, erleichtern bzw. beteiligen sich an der regionalen und subregionalen Zusammenarbeit zwischen gesetzlich autorisierten Behörden, die für den Schutz kritischer Infrastrukturen zuständig sind, zur Erörterung von Möglichkeiten und Befassung mit Herausforderungen für nationale sowie grenzüberschreitende ICT-Netze, auf die diese kritischen Infrastrukturen angewiesen sind.

Die Zusammenarbeit kann unter anderem Folgendes umfassen:

- Austausch von Informationen über Bedrohungen für ICTs
- Austausch bewährter Verfahren
- gegebenenfalls Entwicklung gemeinsamer Maßnahmen gegen gemeinsame Herausforderungen, einschließlich von Krisenmanagementverfahren im Fall großräumiger oder grenzüberschreitender Störungen von ICT-gestützter kritischer Infrastruktur
- Annahme freiwilliger nationaler Vereinbarungen zur Klassifizierung von Zwischenfällen im ICT-Bereich nach Ausmaß und Schwere des Zwischenfalls
- Austausch nationaler Sichtweisen der Kategorien von ICT-gestützten Infrastrukturen, die die Staaten als kritisch einstufen
- Verbesserung der Sicherheit nationaler und grenzüberschreitender ICT-gestützter kritischer Infrastrukturen einschließlich ihrer Integrität auf regionaler und subregionaler Ebene
- Bewusstseinsbildung im Hinblick auf die Wichtigkeit des Schutzes industrieller Steuerungssysteme und auf Fragen ihrer Sicherheit in Verbindung mit ICTs sowie die Notwendigkeit, Prozesse und Mechanismen zur Lösung dieser Fragen zu entwickeln.

16. Die Teilnehmerstaaten fördern auf freiwilliger Basis eine verantwortungsvolle Berichterstattung über Schwachstellen bei der Sicherheit und Nutzung von ICTs und tauschen einschlägige Informationen über verfügbare Mittel zur Beseitigung dieser Schwachstellen aus, unter anderem mit maßgeblichen Bereichen der ICT-Wirtschaft und -industrie, mit dem Ziel, die Zusammenarbeit und Transparenz in der OSZE-Region zu verstärken. Die OSZE-Teilnehmerstaaten sind sich darin einig, dass dieser Informationsaustausch, wenn er zwischen Staaten erfolgt, über autorisierte und geschützte Kommunikationskanäle abgewickelt werden sollte, einschließlich der gemäß VBM 8 in Beschluss

Nr. 1106 des Ständigen Rates benannten Kontaktstellen, um Überschneidungen zu vermeiden.

### **Praktische Überlegungen<sup>1</sup>**

Die folgenden praktischen Überlegungen werden unbeschadet der Freiwilligkeit der Aktivitäten im Rahmen der oben beschriebenen VBMs vorgestellt.

Die Teilnehmerstaaten beabsichtigen, den ersten Informationsaustausch bis spätestens 31. Oktober 2014 durchzuführen; anschließend findet der in den genannten VBMs beschriebene Austausch einmal jährlich statt. Zur Erzielung von Synergien kann der Termin des jährlichen Austauschs mit themenverwandten Initiativen der Teilnehmerstaaten in UN- und anderen Foren zeitlich abgestimmt werden.

Die von den Teilnehmerstaaten mitgeteilten Informationen sollten von jedem von ihnen vor ihrer Weiterleitung zu einem konsolidierten Beitrag zusammengefasst werden, der so transparent und aufschlussreich wie möglich sein sollte.

Die Teilnehmerstaaten können die Informationen in einer beliebigen offiziellen Sprache der OSZE samt englischer Übersetzung oder nur auf Englisch übermitteln.

Die Informationen werden den Teilnehmerstaaten über das Dokumentenverteilungssystem der OSZE zugeleitet.

Rückfragen zu einzelnen Beiträgen können von den Teilnehmerstaaten in Sitzungen des Sicherheitsausschusses und von dessen mit Beschluss Nr. 1039 des Ständigen Rates eingesetzter Informeller Arbeitsgruppe gestellt oder über etablierte Kontaktmechanismen, etwa die E-Mail-Kontaktliste und das POLIS-Diskussionsforum, im direkten Dialog mit dem betreffenden Staat geklärt werden.

Die Teilnehmerstaaten bedienen sich für ihre Aktivitäten gemäß Punkt 9 und 10 bestehender OSZE-Organen und -Mechanismen.

Die Abteilung „Befassung mit grenzüberschreitenden Bedrohungen“ wird die Teilnehmerstaaten auf Ersuchen und im Rahmen verfügbarer Ressourcen bei der Umsetzung der oben beschriebenen VBMs unterstützen.

Bei der Durchführung der VBMs kann es ratsam sein, dass die Teilnehmerstaaten die Erörterungen und das Fachwissen anderer einschlägiger internationaler Organisationen, die sich mit ICT-Fragen beschäftigen, mit einbeziehen.

### **Überlegungen<sup>2</sup>**

Die Teilnehmerstaaten treten auf Ebene der benannten nationalen Experten alljährlich mindestens dreimal im Rahmen des Sicherheitsausschusses und von dessen mit Beschluss Nr. 1039 des Ständigen Rates eingesetzter Informeller Arbeitsgruppe (IWG) zusammen, um die ausgetauschten Informationen zu besprechen und Überlegungen über eine entsprechende

---

1 Erstmals verabschiedet als Teil von Beschluss Nr. 1106 des Ständigen Rates vom 3. Dezember 2013.  
2 Erstmals verabschiedet als Teil von Beschluss Nr. 1202 des Ständigen Rates vom 10. März 2016.

Weiterentwicklung der VBMs anzustellen. Kandidaten für die weitere Prüfung durch die IWG könnten unter anderem Vorschläge für VBMs zur Verstärkung der Transparenz, der Zusammenarbeit und der Stabilität zwischen Staaten bei der Nutzung von ICTs sein. Diese Bemühungen sollten, soweit sie mit dem Mandat der IWG vereinbar sind, die auf Sachverständigenebene verfassten Konsensberichte der Jahre 2013 und 2015 der Gruppe der Vereinten Nationen von Regierungssachverständigen für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit, einschließlich der darin enthaltenen Empfehlungen betreffend freiwillige VBMs, sowie die Arbeit der Gruppe zugunsten freiwilliger, nicht bindender Normen, Regeln und Grundsätze für ein verantwortungsvolles Verhalten der Staaten bei der Nutzung von ICTs berücksichtigen und möglichst ergänzen.

Die Abteilung „Befassung mit grenzüberschreitenden Bedrohungen“ wird über ihren Referenten für Internetsicherheit die Teilnehmerstaaten auf Ersuchen und im Rahmen verfügbarer Ressourcen bei der Umsetzung der oben beschriebenen VBMs und bei der Entwicklung möglicher zukünftiger VBMs unterstützen.