

**Chairmanship: Germany****1092nd PLENARY MEETING OF THE COUNCIL**1. Date: Thursday, 10 March 2016Opened: 10.10 a.m.  
Suspended: 1 p.m.  
Resumed: 3.30 p.m.  
Closed: 5.50 p.m.2. Chairperson: Ambassador E. Pohl  
Ms. C. Weil3. Subjects discussed – Statements – Decisions/documents adopted:Agenda item 1: **DECISION ON OSCE CONFIDENCE-BUILDING  
MEASURES TO REDUCE THE RISKS OF CONFLICT  
STEMMING FROM THE USE OF INFORMATION AND  
COMMUNICATION TECHNOLOGIES**

Chairperson

**Decision:** The Permanent Council adopted Decision No. 1202 (PC.DEC/1202) on OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, the text of which is appended to this journal.

Russian Federation (Annex 1), Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia, Montenegro and Serbia; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association countries Iceland and Norway, members of the European Economic Area; as well as Andorra, Georgia, Moldova, San Marino and Ukraine, in alignment) (Annex 2), United States of America (Annex 3), Chairperson

Agenda item 2: ADDRESS BY THE STATE SECRETARY OF THE  
FEDERAL MINISTRY OF GERMANY FOR FAMILY  
AFFAIRS, SENIOR CITIZENS, WOMEN AND YOUTH,  
MR. RALF KLEINDIEK

Chairperson, State Secretary of the Federal Ministry of Germany for Family Affairs, Senior Citizens, Women and Youth (CIO.GAL/35/16 OSCE+), Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia, Montenegro and Serbia; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association countries Iceland and Liechtenstein, members of the European Economic Area; as well as Andorra, Georgia, Moldova, San Marino and Ukraine, in alignment) (PC.DEL/286/16/Rev.1), United States of America (PC.DEL/288/16), Russian Federation (PC.DEL/309/16), Switzerland (PC.DEL/301/16 OSCE+), Turkey (PC.DEL/329/16 OSCE+), Canada, Austria (also on behalf of Finland, Kazakhstan and Turkey), Norway (PC.DEL/321/16), Belarus (PC.DEL/317/16 OSCE+), Azerbaijan (PC.DEL/298/16 OSCE+), Holy See (PC.DEL/299/16 OSCE+)

Agenda item 3: REPORT BY THE OSCE REPRESENTATIVE ON  
FREEDOM OF THE MEDIA

Chairperson, Representative on Freedom of the Media (FOM.GAL/3/16/Rev.1), United States of America (PC.DEL/290/16), Russian Federation (PC.DEL/310/16), Switzerland (PC.DEL/303/16 OSCE+), Turkey (PC.DEL/324/16 OSCE+), Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia and Montenegro; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association country Iceland, member of the European Economic Area; as well as Moldova and Ukraine, in alignment) (PC.DEL/318/16), Canada, Ukraine (PC.DEL/308/16 OSCE+), Norway (PC.DEL/322/16), Moldova, Armenia, Holy See (PC.DEL/300/16 OSCE+), Montenegro (PC.DEL/320/16 OSCE+), Georgia (PC.DEL/315/16 OSCE+), Kazakhstan, Albania (PC.DEL/291/16), Austria, Serbia, Norway (also on behalf of Sweden) (PC.DEL/323/16), Bosnia and Herzegovina (PC.DEL/316/16 OSCE+)

Agenda item 4: REVIEW OF CURRENT ISSUES

France

- (a) *Ongoing aggression against Ukraine and violations of OSCE principles and commitments by the Russian Federation:* Ukraine (PC.DEL/302/16), Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia and Montenegro; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association countries Iceland, Liechtenstein and Norway, members of the European Economic Area; as well as Georgia, Moldova, San Marino and Ukraine, in alignment)

(PC.DEL/295/16), United States of America (PC.DEL/307/16), Switzerland (PC.DEL/305/16 OSCE+), Turkey (PC.DEL/325/16 OSCE+), Canada

- (b) *Situation in Ukraine and the need to implement the Minsk agreements:* Russian Federation (PC.DEL/314/16), Ukraine
- (c) *Abduction and illegal detention of Ukrainian citizens by the Russian Federation:* Ukraine (PC.DEL/306/16 OSCE+), Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia and Montenegro; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association country Iceland, member of the European Economic Area; as well as Georgia, Moldova, San Marino and Ukraine, in alignment) (PC.DEL/296/16/Rev.2), United States of America (PC.DEL/294/16), Canada, Switzerland (PC.DEL/304/16 OSCE+), Norway, Russian Federation (PC.DEL/313/16), Chairperson
- (d) *Freedom of the media in Turkey:* Netherlands-European Union (with the candidate countries Albania, the former Yugoslav Republic of Macedonia, Montenegro and Serbia; the country of the Stabilisation and Association Process and potential candidate country Bosnia and Herzegovina; the European Free Trade Association country Iceland, member of the European Economic Area; as well as Armenia, in alignment) (PC.DEL/297/16), United States of America (PC.DEL/292/16), Switzerland (also on behalf of Canada, Iceland and Norway), Turkey (PC.DEL/326/16 OSCE+), Russian Federation (PC.DEL/312/16)

Agenda item 5:           REPORT ON THE ACTIVITIES OF THE  
                                  CHAIRPERSON-IN-OFFICE

- (a) *Participation of the Chairperson-in-Office in a meeting of the Foreign Ministers of the Normandy Format, held in Paris on 3 March 2016:* Chairperson (CIO.GAL/34/16)
- (b) *Condemnation by the Chairperson-in-Office and the OSCE Secretary General of the attack in Tunisia on 7 March 2016:* Chairperson (CIO.GAL/34/16)
- (c) *Visit of the Special Representative of the OSCE Chairperson-in-Office for the South Caucasus, Ambassador Bächler, to Tbilisi, Tskhinvali, Sukhumi and Moscow, undertaken from 29 February to 10 March 2016:* Chairperson (CIO.GAL/34/16)

Agenda item 6:           REPORT OF THE SECRETARY GENERAL

- (a) *Security Days “Refocusing Security and Migration: Bridging National and Regional Responses”, held in Rome on 4 March 2016:* Director of the Conflict Prevention Centre (SEC.GAL/39/16 OSCE+)

- (b) *Panel discussion on the EU, the OSCE and the Future of European Security, held in Rome on 8 March 2016*: Director of the Conflict Prevention Centre (SEC.GAL/39/16 OSCE+)
- (c) *OSCE-UNODC staff talks and the signing of a Joint Action Plan for 2016–2017, held in Vienna on 9 March 2016*: Director of the Conflict Prevention Centre (SEC.GAL/39/16 OSCE+)

Agenda item 7: ANY OTHER BUSINESS

- (a) *Follow-up to the Security Days “Refocusing Security and Migration: Bridging National and Regional Responses”, held in Rome on 4 March 2016*: Chairperson, Switzerland (PC.DEL/327/16 OSCE+)
- (b) *Appeal for the nomination of candidates for the post of Chief Observer of the OSCE Observer Mission at the two Russian checkpoints on the Russian-Ukrainian border and the post of Head of the OSCE Centre in Ashgabat*: Chairperson
- (c) *Parliamentary elections in Serbia, to be held on 24 April 2016*: Serbia
- (d) *Announcement of a Mediterranean Contact Group meeting, to be held on 14 March 2016*: Austria

4. Next meeting:

Thursday, 17 March 2016, at 10 a.m., in the Neuer Saal



**Organization for Security and Co-operation in Europe  
Permanent Council**

PC.JOUR/1092  
10 March 2016  
Annex 1

Original: ENGLISH

---

**1092nd Plenary Meeting**  
PC Journal No. 1092, Agenda item 1

**STATEMENT BY  
THE DELEGATION OF RUSSIAN FEDERATION**

Mr. Chairperson,

The Russian Federation has joined the consensus on the Permanent Council decision on an additional set of confidence-building measures in the field of security in the use of information and telecommunication technologies.

The adoption within the OSCE of additional confidence-building measures is the result of constructive co-operation by all participants in the negotiation process within the informal working group chaired by the United States of America. We should like in particular to mention the contribution by the German Chairmanship, which was instrumental in the achievement of a compromise text reflecting the interests of all parties.

We should like to emphasize the importance of provisions in the additional set of measures regarding their voluntary nature, the key role of States in facilitating practical co-operation in protecting critical information infrastructures and the need to share information using authorized and protected communication channels.

The fact that agreement has been reached in the OSCE on these confidence-building measures confirms that, regardless of the political situation, consensus can be reached on questions of fundamental importance connected with ensuring international information security. We believe it important to steadily build up international co-operation in this area.

We request that our statement be attached to the journal of the day.

Thank you for your attention.



**Organization for Security and Co-operation in Europe  
Permanent Council**

PC.JOUR/1092  
10 March 2016  
Annex 2

Original: ENGLISH

---

**1092nd Plenary Meeting**

PC Journal No. 1092, Agenda item 1

**STATEMENT BY  
THE REPRESENTATIVE OF THE EUROPEAN UNION**

The delegation of the Netherlands, in its capacity as EU Presidency, passed the floor to the representative of the European Union, who delivered the following statement:

The European Union and its Member States welcome the adoption of the additional cyber confidence-building measures to reduce the risks of conflict stemming from the use of the information and communication technologies. This decision complements and consolidates the initial set of CBMs that was adopted in 2013, which was the first of its kind adopted by a regional organization. It represents a big step forward for multilateral co-operation in the dynamic cyber domain. Taken together, these risk-reduction measures are a significant achievement as they will enhance inter-State co-operation, transparency, predictability and stability among participating States.

We thank the consecutive Chairmanships, the US Chairmanship of the Informal Working Group and their teams as well as the OSCE Secretariat for their tremendous efforts. We congratulate all participating States for investing time and effort in developing these practical measures and for their constructive spirit, which led to reaching consensus early this year. The very fact that an inclusive and representative organization like the OSCE has successfully engaged in such a sensible and complex process sends a strong political and public message that each and every participating State is determined to contribute to this important common effort. It adds to the OSCE's record of building confidence among participating States in a comprehensive and cross-dimensional manner.

Mr. Chairperson, preserving a peaceful, open, free and secure cyberspace is a global challenge, which should be addressed together with the relevant international partners and organizations, the private sector and civil society. We will also be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

Colleagues, the decision adopted today is certainly a success but the process does not end here. All participating States need to keep in mind that the implementation of the initial CBMs should remain a priority. We will continue to put our commitments into practice while we look forward to exploring additional confidence-building measures that seek to build and consolidate trust, co-operation and stability in the cyber domain.

The candidate countries the former Yugoslav Republic of Macedonia<sup>1</sup>, Montenegro<sup>1</sup>, Serbia<sup>1</sup>, and Albania<sup>1</sup>, the country of the Stabilisation and Association Process and potential candidate Bosnia and Herzegovina, and the European Free Trade Association countries Iceland and Norway, members of the European Economic Area, as well as Ukraine, the Republic of Moldova, Georgia, Andorra and San Marino align themselves with this statement.

---

1 The former Yugoslav Republic of Macedonia, Montenegro and Albania continue to be part of the Stabilisation and Association Process.



**Organization for Security and Co-operation in Europe  
Permanent Council**

PC.JOUR/1092  
10 March 2016  
Annex 3

Original: ENGLISH

---

**1092nd Plenary Meeting**  
PC Journal No. 1092, Agenda item 1

## **STATEMENT BY THE DELEGATION OF THE UNITED STATES OF AMERICA**

The United States welcomes the adoption of additional cyber confidence-building measures (CBMs) to enhance inter-State co-operation, transparency, predictability and stability among participating States. These practical risk-reduction measures build on an earlier set of CBMs adopted in 2013 that were without precedent in the international arena.

The OSCE continues to break ground in the cyber realm. The CBMs just adopted add to our systematic, voluntary exchanges of information, and encourage joint undertakings of activities to address common security challenges. This is particularly important when participating States critical, lifesaving infrastructure, such as power grids, run on networks connected to the Internet. As we witness increasingly sophisticated cyberattacks, that are global in nature and virtually untraceable, CBMs help reduce or eliminate causes of mistrust, fear, and tensions, and reinforce confidence where it exists.

In supporting this decision, the United States will be guided by the firm conviction that information and communication technologies, along with the Internet that connects them, are powerful tools for advancing human rights, especially the freedoms of expression, association, and peaceful assembly.

We also reiterate our firm commitment to the multi-stakeholder approach to Internet governance, that is characterized by transparent, bottom-up, consensus driven processes, in which the legitimate interests of governments, the private sector, civil society, and the technical community are all taken into account.

The United States had the privilege of serving as chairmanship of the Informal Working Group (IWG) tasked with elaborating these CBMs. Reaching consensus on the CBMs required considerable effort by many delegations, and we offer our gratitude to all capital level experts who provided guidance and travelled to support these negotiations. As chairmanship of the IWG, the United States will continue to pursue a dual-focused approach, stressing the implementation of our existing commitments, and pursuing additional measures that seek to increase inter-State co-operation and stability. We look forward to advancing the work of this group through our remaining meetings this year.

Thank you, Mr. Chairperson, and I would be pleased if you would attach this statement to the journal of the day.





**1092nd Plenary Meeting**  
PC Journal No. 1092, Agenda item 1

**DECISION No. 1202**  
**OSCE CONFIDENCE-BUILDING MEASURES TO**  
**REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE**  
**OF INFORMATION AND COMMUNICATION TECHNOLOGIES**

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as “security of and in the use of ICTs.” They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, *inter alia*, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.
2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.
3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of

political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms *inter alia*, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals from the Consolidated List

circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, *inter alia*, to:

- Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;
- Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and
- Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, *inter alia*, include:

- Sharing information on ICT threats;
- Exchanging best practices;

- Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;
- Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;
- Sharing national views of categories of ICT-enabled infrastructure States consider critical;
- Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and
- Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

### **Practical Considerations<sup>1</sup>**

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group

---

1 First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013.

established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

### **Considerations<sup>2</sup>**

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group's work in support of voluntary non-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

---

2 First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.