Republic of Serbia
Ministry of Interior

OSCE activities in the field of cyber security and Confidence Building Measures

Nebojša Jokić
Sector for Analytics, Telecommunications and Information Technologies
CERT

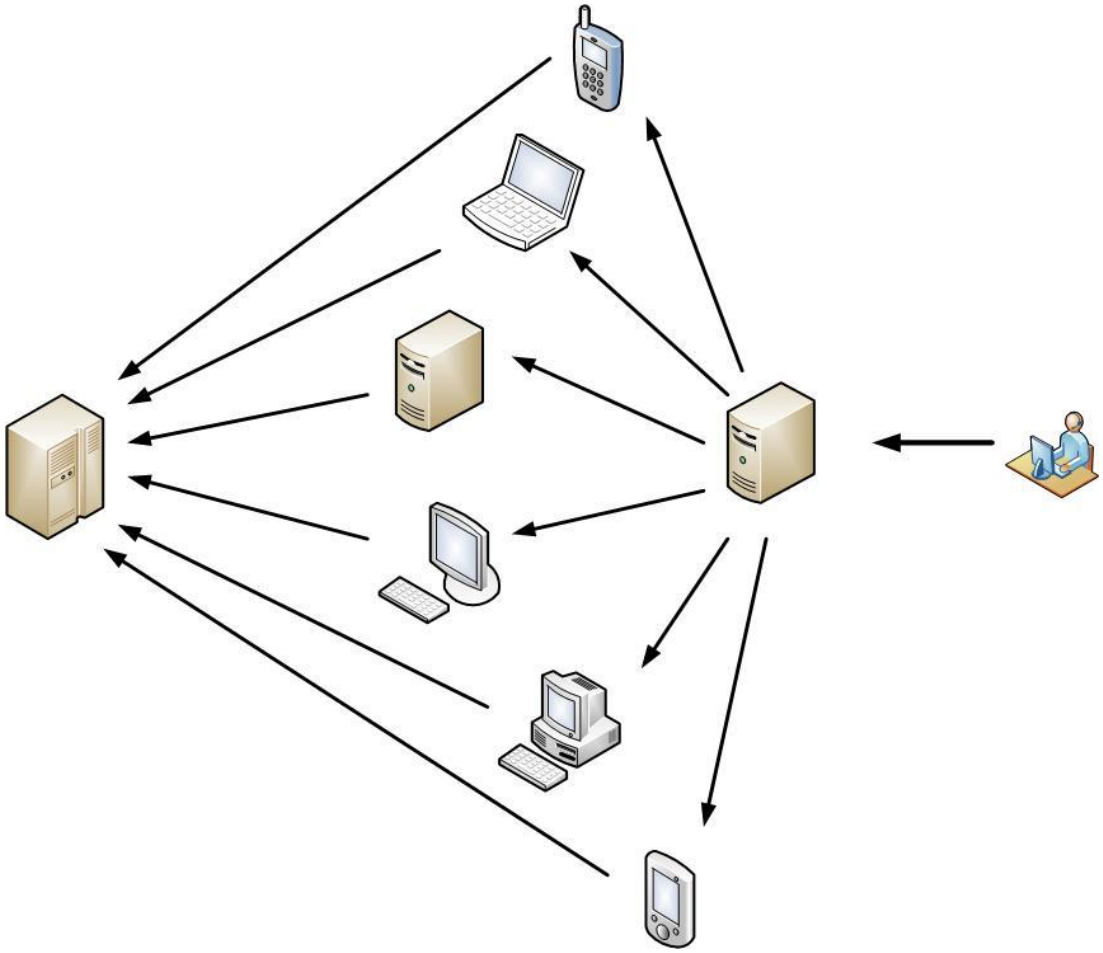
ICTs

- Information and Communications Technologies – inseparable part of modern society
- Rapid development of new applications and slow changes of fundamental principles
- New technologies: IoT, 5G, autonomous vehicles…
- Risk of open and always available cyberspace

Characteristics of cyber attacks

- Asymmetry
- Each country can be a source, a target, or a transit country
- Attribution problem

Botnet



Problems

- National solutions alone are not enough for transnational problems
- Insufficiently defined and non-binding framework for international cooperation
- Lack of technical knowledge
- Lack of trust between states
- Limited control over “patriotic hackers”

International cooperation

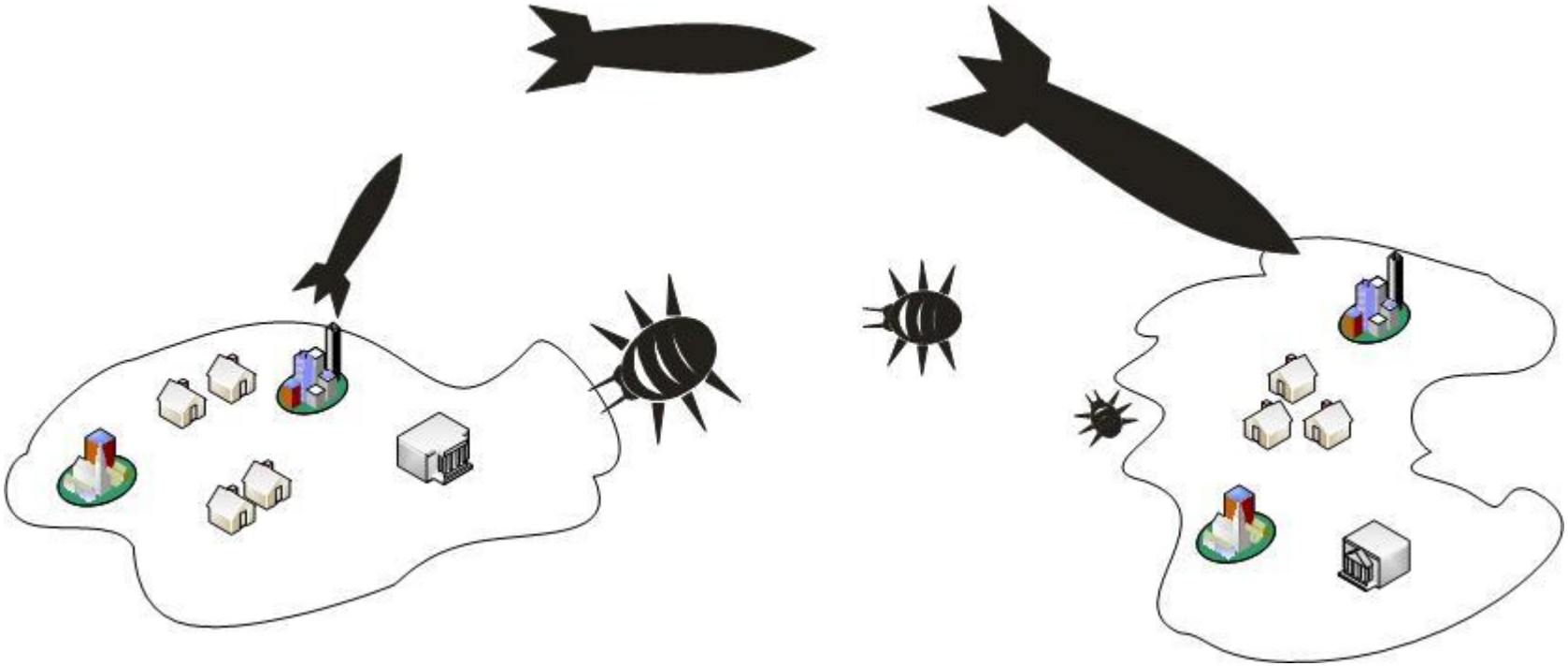
- GGE UN recommendations
- OEWG
- Regional cooperation
- IWG OSCE and CBMs

Charter of the UN, Chapter VII

Article 51:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

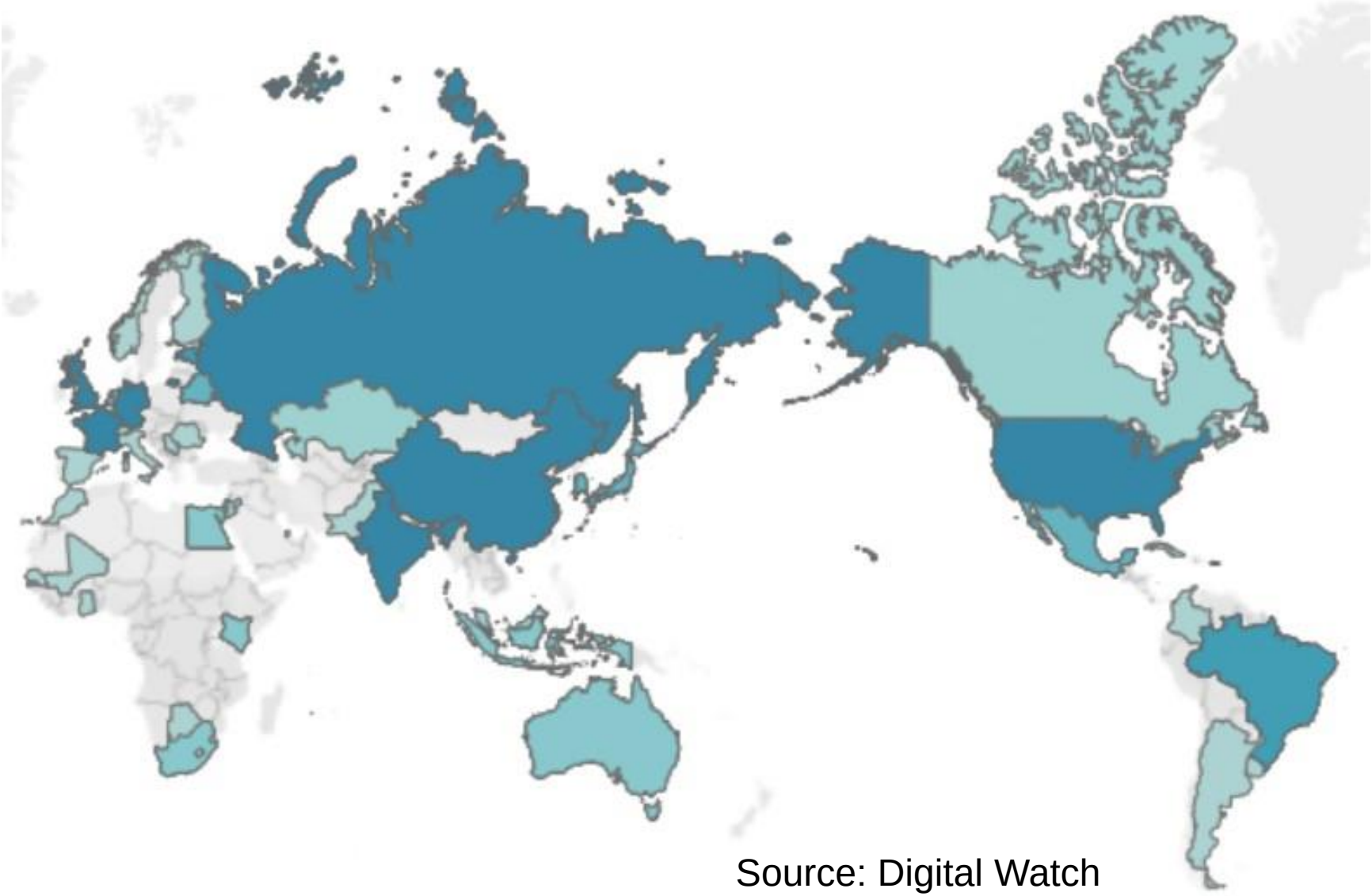
DANGER!



UN GGE

- GGE process: six goups
- Selection: 'on the basis of equitable geographical distribution'
- Five permanent members of the Security Council have a seat on all GGEs
- The UN Office for Disarmament Affairs (UNODA) serves as the Secretariat to the cyber GGEs
- Decisions, including decisions on the final Report, are made by consensus

Members of the UN GGE



Source: Digital Watch

Groups of Governmental Experts

- 2004 – 2005
- 2009 – 2010
- 2012 – 2013
- 2014 – 2015
- 2016 – 2017
- 2019 – 2021

Recommendations 2013

- International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment
- The application of norms derived from existing international law is an essential measure to reduce risks to international peace, security and stability
- State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory

Recommendations 2013

- State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms
- States should intensify cooperation against criminal or terrorist use of ICTs
- States must meet their international obligations regarding internationally wrongful acts attributable to them
- States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs
- Member States should consider how best to cooperate in implementing the above norms and principles of responsible behavior

Recommendations 2013

- Voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception.
  - The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation
  - The creation of bilateral, regional and multilateral consultative frameworks for confidence-building
  - Enhanced sharing of information among States on ICT security incidents
  - Exchanges of information and communication between national Computer Emergency Response Teams (CERTs)
  - Increased cooperation to address incidents that could affect ICT or critical infrastructure
  - Enhanced mechanisms for law enforcement cooperation

Recommendations 2013

- States should consider the following measures:
  - Supporting bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and ICT infrastructures
  - Creating and strengthening incident response capabilities, including CERTs, and strengthening CERT-to-CERT cooperation
  - Supporting the development and use of e-learning, training and awareness-raising
  - Increasing cooperation and transfer of knowledge and technology for managing ICT security incidents
  - Encouraging further analysis and study by research institutes and universities on matters related to ICT security

Recommendations 2015

- States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security
- In case of ICT incidents, States should consider all relevant information, the challenges of attribution in the ICT environment and the nature and extent of the consequences
- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats
- States should respect Human Rights Council resolutions on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions on the right to privacy in the digital age

Recommendations 2015

- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public
- States should take appropriate measures to protect their critical infrastructure from ICT threats
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts
- States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products
- States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies
- States should not conduct or knowingly support activity to harm the information systems of the authorized CERTs of another State

Recommendations 2015

- To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:
  - The identification of appropriate points of contact at the policy and technical levels
  - The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations
  - Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels
  - The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure

Recommendations 2015

- Additional confidence-building measures:
  - Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests
  - Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations
  - Establish a national computer emergency response team
  - Expand and support practices in computer emergency response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks
  - Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory

OEWG

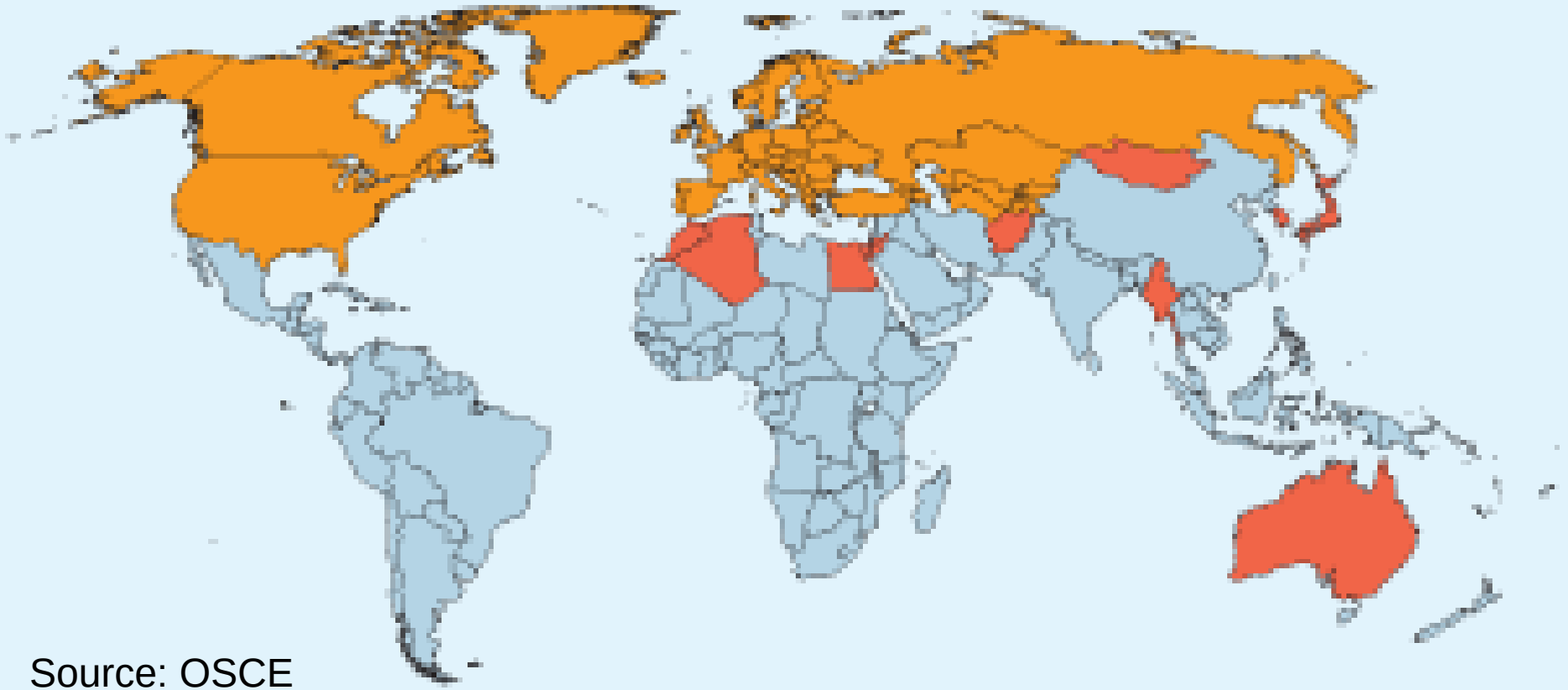
- The composition is open, allowing all UN member states that express a desire to participate
- Issues for discussion:
  - Existing and potential threats;
  - International law;
  - Rules, norms and principles;
  - Regular institutional dialogue;
  - Confidence building measures;
  - Capacity building.

Regional cooperation

- African Union
- Association of Southeast Asian Nations (ASEAN) Regional Forum
- Asia Pacific Economic Cooperation Forum
- Council of Europe
- Economic Community of West African States
- European Union
- League of Arab States
- Organization of American States
- Shanghai Cooperation Organization
- Organization for Security and Cooperation in Europe (OSCE)

OSCE participating States

OSCE Geographical Area



Source: OSCE

Participating States Partners for Co-operation

OSCE Decision 1039

- The Permanent Council decides to step up individual and collective efforts to address security in the use of information and communication technologies
- OSCE Chairmanship tasked to establish an open-ended, informal OSCE working group (IWG)
- IWG tasks:
  - To elaborate a set of draft Confidence-Building Measures (CBMs) to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs;
  - To help build consensus for the adoption of CBMs;
  - To provide progress reports.

OSCE CBMs

- OSCE Permanent Council Decision 1106 (2013)
- OSCE Permanent Council Decision 1202 (2016)

OSCE CBMs

- **Objective:** To reduce tensions between States by promoting exchanges of information and communication between **policy/ decision makers and the technical community**.

- **The CBMs will not stop an intentional conflict but they can stop an unintentional conflict** by stopping or slowing down the spiral of escalation.

- The 16 voluntary CBMs can be broadly categorized in three clusters:
  - **Posturing** - CBMs which allow States to “read” another State’s posturing in cyberspace
  - **Communication** - CBMs which offer opportunities for timely communication and co-operation including to defuse potential tensions
  - **Preparedness** - CBMs which promote national preparedness and due diligence to address cyber/ICT challenges

OSCE CBMs

Posturing

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.

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

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.

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.*

OSCE CBMs

Communication

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.

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.

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.

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.

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.

OSCE CBMs

Preparedness

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.

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.

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.

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.

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.

Implementation of CBMs

In 2018, the Chair of the IWG launched the **"Adopt-a-CBM"** initiative, which saw participating States volunteering, alone or in groups, to explore how CBMs can be usably implemented.

As of today, 8 CBMs have been adopted in such a way:

- **CBM 3**, regarding consultations to prevent tensions;
- **CBM 4**, regarding information exchange taken to ensure open, interoperable, secure and reliable Internet;
- **CBM 5**, where States volunteer to exchange information, including on capacity-building, through the OSCE;
- **CBM 9**, whereby States agree to volunteer national terminologies to reduce the risks of misunderstanding;
- **CBM 13**, whereby States can further explore how to make the OSCE Communications Network for cyber/ICT security more fit-for-purpose;
- **CBM 14**, regarding promotion of PPP;
- **CBM 15**, for the protection of critical infrastructure;
- **CBM 16**, for encouraging co-ordinated (responsible) vulnerability disclosures.

Serbian contribution

- Participation in IWG
- Sponsorship of the Confidence Building Measure No. 9, which refers to national terminologies and definitions of terms in the field of cyber security:
  - "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. "

Serbian contribution

- Action plan:
    1) The list of defined terms shall be taken from the legislation of each Member State, together with the definition of each term in the language in which the legal act is written;
    2) If a Member State has made a legal act public in English, the term and definition in English shall be added to the table;
    3) If the Member State has not officially published the legal act in English, the translation of the term into English shall be entered into the table without translation of the definition;
    4) A complete list of terms and their definitions will be published on the OSCE POLIS platform;
    5) Member States will be kindly requested to review the published list of terms from their legislation and submit comments, as well as to provide translations of definitions where English translation is not available;
    6) After completing the entry of terms and definitions, a list of all terms defined by any Member State will be made.

- Based on the obtained results, an analysis of the used terminology and similarities will be made
- Serbia does not intend to work on a common dictionary.

Serbian contribution

Database fields:

- Member State
- Term in the national language
- Term in the English language
- Definition in the national language
- Definition in the English language
- Title of the legal act in the national language
- Title of the legal act in the English language
- Link to the legal act in the national language
- Link to the legal act in the English language

Serbian contribution

website:

https://cbm9.gov.rs

Serbian contribution

Future plans:

- Regular updates of terms and definitions
- Improvement of the website
- Cooperation with member States
- Analysis of the obtained results

Republic of Serbia
Ministry of Interior

Thank you for your attention!