# United Nations (UN)

Last Updated: October 2019

**Member States**

## POLICY

### Strategy Documents

**ICT Strategy (A/69/517)**

General Assembly, Office of Information and Communications Technology

- Comprises a section on information security: states that the Office of Information and Communications Technology has established a comprehensive information security framework for the Secretariat, building on the interim initiatives identified in the report of the Secretary-General in the areas of prevention, incident detection and response, and governance, risk and compliance
- Aligned with A/RES/69/262 (stressing the need to harness the potential of information and communications technology to support the work of the United Nations in the areas of peace and security, development, human rights and international law)
- Key activity areas include reinforced importance of information security and need for central control and governance
- Information Security elements of the Strategy include:
    - Transparency, including continious monitoring and vulnerability management
    - InfoSec policy development, compliance and enforcement, including
        - Incident response coordination and intelligence sharing
        - Privacy
        - Security architecture and application development
        - Enhancements to the security infrastructure, including regions
    - Full detailed assessment of ICT assets, services, and systems
    - Correction of critical issues

Source Source 2

*10 October 2014*

### Other Documents

**Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/72/327)**

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

- Report of the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- No consensus was reached on a final report

Source

*14 August 2017*

**Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)**

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Source

*22 July 2015*

**Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)**

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

# United Nations (UN)

Last Updated: October 2019

Source

*24 June 2013*

**Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)**

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Source

*30 July 2010*

**Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/60/202)**

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Source

*5 August 2005*

**Report of the Secretary-General: Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity**

UN Secretary-General

Includes section on High-technology and computerrelated crime, which cites findings of Resolution 56/121 and Report on Effective Measures to Prevent and Control Computer-Related Crime (E/CN.15/2002/8)

Source

*2 July 2002*

**Report of the Secretary-General: Effective measures to prevent and control computer-related crime**

UN Secretary-General

Provides a brief overview of ongoing efforts to prevent and control high technology and computer-related crime, highlighting general trends and developments within and outside the United Nations

Source

*29 January 2002*

**Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (A/HRC/27/37)**

Human Rights Council

- Report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council
- Mandated by the General Assembly through the adoption of Resolution 68/167

Source Source 2

*30 June 2014*

**Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children**

UNODC

- Prepared pursuant to Economic and Social Council resolution 2011/33 on Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children
- Based primarily on open source research and the outcomes of an informal expert group meeting on ICT-facilitated abuse and exploitation of children

# United Nations (UN)

Last Updated: October 2019

- Includes four Chapters:
  - *Chapter I*: identifies and defines key terms in analysing the problem of ICT-facilitated child abuse and exploitation and describes the most common types and forms of related behaviour
  - *Chapter II*: evaluates the effects of ICTs on common forms of child abuse and exploitation; provides a brief overview of the main risk factors for victims as well as possible offender profiles; describes organized groups of offenders and the role of organized criminal networks in child abuse and exploitation
  - *Chapter III*: identifies the main international and regional instruments relevant to combating the ICT-facilitated sexual abuse and exploitation of children
  - *Chapter III (additional section):* provides an overview of different practices and policies adopted to combat ICT-facilitated child sexual abuse and exploitation, as well as opportunities to enhance the fight against such crimes
- Includes Glossary or terms related to the Study's scope and subject

Source Source 2

*May 2014*

**Comprehensive Study on Cybercrime**

UNODC

- Mandated by UN General Assembly Resolution 65/230 to "examine options to strengthen existing and to propose new national and international legal or other responses to cybercrime"
- The focus is limited to the crime prevention and criminal justice aspects of preventing and combating cybercrime; the Study represents a 'snapshot' in time of crime prevention and criminal justice efforts to prevent and combat cybercrime
- Prepared by the Open-Ended Intergovernmental Expert Group (IED)
- Addresses the following topics covered in 8 chapters:
  1. Connectivity and cybercrime
  2. The global picture
  3. Legislation and frameworks
  4. Criminalization
  5. Law enforcement and investigations
  6. Electronic evidence and criminal justice
  7. International cooperation, and
  8. Prevention
- Information was received from 69 Member States, and also from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations
- Comments from States to the Comprehensive Study were requested from the Secretariat by the Commission on Crime Prevention and Criminal Justice

Source Source 2

*February 2013*

## Communications

**Compendium on the High Level Review of United Nations Sanctions**

UN Secretariat

Contains five recommendations for tackling issues of cybercrime, including:

- 147: The Security Council should enhance investigative capacities and strengthen international cooperation to determine which countries and/or individuals or entities are responsible for abuses of cyberspace affecting international peace and security, facilitating the imposition of UN sanctions

Source Source 2

*November 2015*

**The Mapping of International Internet Public Policy Issues**

Intersessional Panel of the Commission on Science and Technology for Development, ECOSOC

Aims to create a more comprehensive set of information on international public policy issues pertaining to the Internet, the mechanisms dealing with these issues, and potential gaps in those mechanisms

Source

# United Nations (UN)

Last Updated: October 2019

*21 November 2014*

**Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects, Working Group Compendium**

UN Counter-Terrorism Implementation Task Force

Details strategic approaches (and provides recommendations) to addressing challenges of terrorist use of the internet, including:

- Applying existing cybercrime legislation
- Applying existing (non Internet specific) terrorism legislation
- Developing specific legislation dealing with terrorist use of the internet

Source

*May 2011*

## STRUCTURE

### Specialized Agencies

**United Nations Office for Disarmament Affairs**

- Established in January 1998 as the Department of Disarmament Affairs, the United Nations Office for Disarmament Affairs provides substantive and organizational support for norm-setting in the area of disarmament through the work of the General Assembly and its First Committee, the Disarmament Commission, the Conference on Disarmament and other bodies.
- Provides support for multilateral discussions, including the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which has been on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly.

Source

*1998*

**International Telecommunications Union**

Based on the guidance of the World summit on the Information Society and the ITU Plenipotentiary Conference, tasked with building confidence and security in the use of information and communication technologies.

Source

**United Nations Institute for Disarmament Research**

- Voluntarily funded autonomous institute within the United Nations that generates ideas and promotes action on disarmament and security
- The Institute's Security and Technology (SecTec) Programme was launched in 2019 and currently encompasses several workstreams, including:
  - Cyber Security
  - Autonomous Technologies and Artificial Intelligence
  - International Peace and Security Implications of Emerging Technologies
- Has supported in the past the work of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security (2009-2010; 2012-2013; 2014-2015; 2016-2017)
- Launched the Cyber Policy Portal in January 2019 as a universal reference tool on cyber policy issues for diplomats, policy makers and the expert community, and conducts its maintenance and development

Source Source 2

*1980*

**United Nations Office on Drugs and Crime**

Draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, interantional cooperation, and data collection, research and analysis on cybercrime.

# United Nations (UN)

Last Updated: October 2019

Source

**Office of Information and Communications Technology (OICT)**

- Responsible for defining strategic direction for ICT to the UN Secretariat
- Provides oversight of ICT programmes, budgets and decision-making to ensure alignment with the Secretariat's overall ICT strategy
- Submitted the Strategy on ICTs in the United Nations (A/69/517) in 2015, defining the roadmap for ICT for five years, providing a common vision for ICT delivery in the UN through modernization, transformation and innovation
- Was tasked with establishing an information risk management regime and supporting policies for the Secretariat; in 2013, developed an action plan to address the most urgent shortcomings and mitigate specific risks
- Relevant guiding documents with regard to ICT security activities include Report of the Secretary -General (A/68/552) and UN GA Resolution (A/RES/68/247)
- Coordinates the Digital Blue Helmets (DBH) programme intended to serve as a common platform for rapid information exchange and better coordination of protective and defensive measures against IT security incidents for the UN, including agencies, funds and programmes

Source Source 2

## LEGISLATION

### Regulations and Directives

**Resolutions and Reports on Developments in the field of information and telecommunications in the context of international security**

United Nations General Assembly

- Resolutions: A/RES/73/266 and A/RES/73/27 (2018); A/C.1/72/L.44 (2017); A/RES/71/28 (2016); A/RES/70/237 (2015); A/RES/69/28 (2014); A/RES/68/243 (2013); A/RES/67/27 (2012); A/RES/66/24 (2011); A/RES/65/41 (2010); A/RES/64/25 (2009); A/RES/63/37 (2008); A/RES/62/17 (2007); A/RES/61/54 (2006); A/RES/60/45 (2005); A/RES/59/61 (2004); A/RES/58/32 (2003); A/RES/57/53 (2002); A/RES/56/19 (2001); A/RES/55/28 (2000); A/RES/54/49 (1999); A/RES/53/70 (1998)

- Annual Reports of the Secretary-General with the views of UN Member States on the issue: A/72/315 (2017); A/71/172 (2016); A/70/17 (2015); A/69/11 and A/69/112/Add.1 (2014); A/68/156 and A/68/156/Add.1 (2013); A/67/167 (2012); A/66/152 and A/66/152/Add.1 (2011); A/65/154 (2010)

Source

*1998 (since)*

**Resolution on The right to privacy in the digital age (A/RES/68/167)**

General Assembly

• Reaffirms the right to privacy;
• Affirms that the same rights that people have offline must also be protected online.

Source

*18 December 2013*

**Resolution on the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (A/RES/64/211)**

General Assembly

• Invites Member States to use the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity;
• Encourages sharing of best practices and measures

Source

# United Nations (UN)

Last Updated: October 2019

*21 December 2009*

**Resolution on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures (A/RES/58/199)**

General Assembly

• Invites Member States to use the annexed elements in developing their strategies for reducing risks to critical information infrastructures
• Encourages sharing of best practices and measures

Source

*30 January 2004*

**Resolution on the Creation of a global culture of cybersecurity (A/RES/57/239)**

General Assembly

• Invites Member States to use annexed elements in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies
• Encourages sharing of best practices and measures

Source

*31 January 2003*

**Resolution on Combating the criminal misuse of information technologies (A/RES/56/121)**

General Assembly

Invites Member States to take into account the work and achievements of the commission on Crime Prevention and Criminal Justice and of other international and regional organizations, as well as the measures set forth in Resolution 55/63

Source

*23 January 2002*

**Resolution on Combating the criminal misuse of information technologies (A/RES/55/63)**

General Assembly

Identifies measures aimed to combat the criminal misuse of information technologies, including information exchange, law enforcement cooperation and training, mutual assistance regimes, and others.

Source

*22 January 2001*

## COOPERATION

### Meetings

**Annual Cyber Stability Conference**

United Nations Institute for Disarmament Research (UNIDIR)

- The Annual Cyber Stability Conference presents an ongoing opportunity for stakeholders to discuss how to take pragmatic steps towards a more stable and predictable cyber security environment, with a specific focus on the risks of escalation in times of conflict, and the implementation of transparency and confidence-building measures
- The 2019 theme, "Strengthening Global Engagement", focuses on building international commitment and cooperation to address the risks stemming from the malicious use of ICTs
- The Conference aims to bring together to representatives of the UN Member States, as well as other major stakeholders, including international and regional organizations, multistakeholder frameworks with focus on cyber security policy issues, private industry, technical community, civil society and the academia

Source Source 2

*Since 2012*

**World Summit on the Information Society (WSIS) Forum**

ITU, UNCTAD, UNDP, UNESCO

# United Nations (UN)

Last Updated: October 2019

- Global multi-stakeholder platform facilitating the implementation of the WSIS Action Lines for advancing sustainable development
- Serves as a key forum for discussing the role of ICTs as a means of implementation of the Sustainable Development Goals (SDGs) and targets, with due regard to the global mechanism for follow-up and review of the implementation of the 2030 Agenda for Sustainable Development (ASD)
- Co-organized by ITU, UNESCO, UNDP and UNCTAD, in close collaboration with all WSIS Action Line co-/facilitators and other UN organizations
- Provides an opportunity for information exchange, knowledge creation and sharing of best practices, while identifying emerging trends and fostering partnerships, taking into account the evolving Information and Knowledge Societies
- Aims to constantly evolve and strengthen the alignment between the WSIS Action Lines and the SDGs in follow up to the outcomes of the UN GA Overall Review of the Implementation of WSIS Outcomes (Res. A/70/125) and with the adoption of the 2030 ASD (Res. A/70/1)

Source Source 2

*Annually since 2006*

**UN Groups of Governmental Experts on developments in the field of ICTs in the context of international security (2004-2017)**

United Nations General Assembly

- The issue of information security was put on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly (adopted A/RES/53/70)
- 5 GGEs were conducted over the period from 2004 to 2017:
  - *1st GGE*: 2004-2005, mandated by UNGA A/RES/58/32, produced Report A/60/202; no consensus on the Report was achieved
  - *2nd GGE*: 2009-2010, mandated by UNGA A/RES/60/45, produced a consensus Report A/65/201 with recommendations on dialogue on norms for State use of ICTs; confidence-building and risk-reduction measures, information exchanges; and capacity-building in less-developed countries
  - *3rd GGE*: 2012-2013, mandated by UNGA A/RES/66/24, produced aconsensus-based Report A/68/98*, in which the Group agreed on a number of principles and other points
  - *4th GGE*: 2014-2015, mandated by UNGA A/RES/68/243, produced a substantive consensus Report A/70/174 on norms, rules or principles of the responsible behaviour of States in the cyber-sphere as well as confidence building measures, international cooperation and capacity building, which could have wider application to all States
  - *5th GGE*: 2016-2017, mandated by UNGA A/RES/70/237, produced Report A/72/327; no consensus on the Report was achieved
- A new UN GGE on Advancing responsible State behaviour in cyberspace in the context of international security is to conduct its work in 2019-2021 as enshrined in the UN General Assembly Resolution (A/RES/73/266 adopted on 22 December 2018)

Source Source 2

*2004-2005; 2009-2010; 2012-2013; 2014-2015; 2016-2017*

**Open-Ended Intergovernmental Expert Group (IEG) to conduct a Comprehensive Study on the Problem of Cybercrime**

UNODC

- Mandated by the Economic and Social Council (Resolution 2010/18) and the General Assembly (Resolution 65/230) to conduct a comprehensive study on the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and interntional cooperation
- Aims to examine options to strengthen existing and to propose new national and international legal or other responses to cybercrime
- 5 Meetings of the IEG took place in Vienna, Austria, as of 2019:
  - 5th IEG Meeting, 27-29 March 2019
  - 4th IEG Meeting, 3-5 April 2018
  - 3rd IEG Meeting, 10-13 April 2017
  - 2nd IEG Meeting, 25-28 February 2013
  - 1st IEG Meeting, 17-21 January 2011

Source Source 2

*17-21 January 2011; 25-28 February 2013; 10-13 April 2017; 3-5 April 2018; 27-29 March 2019*

**Arria-Formula Meeting on Threats to Peace and Security Caused by Terrorist Acts (Cybersecurity)**

UN Security Council

- Chaired by Senegal and Spain, with participants representing Telefonica Internacional USA, ICT4Peace Foundation, FireEye iSIGHT Intelligence, among others
- Conducted to discuss the challenges resulting from the use of information and communications technologies (ICTs) that can threaten international peace and security
- Aimed at broadening the discussion to include the potential role of ICTs in fueling political or military tensions, as well as the importance of the protection of ICT-dependent critical infrastructure
- Raised the issue of whether the UN Security Council is receiving appropriate contextual information on the possible security implications of the use of ICTs in the event of emerging political or military tensions, and how it can contribute to mitigating these

# United Nations (UN)

Last Updated: October 2019

Source Source 2

*28 November 2016*

**United Nations Open-Ended Working Group (OEWG) on developments in the field of ICTs in the context of international security**

United Nations General Assembly

- The OEWG, open to all UN Member States, was established through UNGA Resolution A/RES/73/27, entitled "Developments in the field of information and telecommunications in the context of international security", adopted on 5 December 2018
- The mandate of the OEWG also includes the possibility of holding, from within voluntary contributions, intersessional consultative meetings with interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the Group's mandate
- Ambassador Jürg Lauber of Switzerland was elected by acclamation to Chair the Open-ended Working Group
- The Group held its first organizational session on 3-4 June 2019, followed by its first substantive session on 9-13 September 2019 in New York, USA
- Further schedule of the OEWG actitivities includes:
    - Intersessional meeting with Industry Partners and NGOs – New York, 2-4 Dec 2019 (CR1)
    - Second substantive session – New York, 10-14 February 2020
    - Third (and final) substantive session – New York, 6-10 July 2020, and reporting back to the UN General Assembly in 2020
- The UN ODA is providing support to the Open-Ended Working Group process (as well as to the UN GGE process)

Source Source 2

*5 December 2018 (established); 6-10 July 2020 (final substantive session scheduled)*

**UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE)**

United Nations General Assembly

- The Group was established through the UN General Assembly Resolution (A/RES/73/266) adopted on 22 December 2018 with its mandate including continued study of:
    - possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence -building measures and capacity-building, and
    - how international law applies to the use of ICTs by States
- The Group's mandate also includes consultations on the subject to be held with regional organizations, such as :
    1. the African Union
    2. the European Union
    3. the Organization of American States
    4. the Organization for Security and Cooperation in Europe and
    5. the Regional Forum of the Association of Southeast Asian Nations
- The Group will hold its first substantive session in December 2019 in New York, and is to submit its final report to the UN General Assembly in 2021The Group will hold its first substantive session in December 2019 in New York, and is to submit its final report to the UN General Assembly in 2021
- Also, the Group's Chair will hold two informal consultations with all UN Member States in between its sessions
- The Group comprises experts from 25 States working in their personal capacity
- The UN ODA has provided substantive support to the expert Groups and has acted as the secretariat assisting in the preparation of the Groups' Reports

Source Source 2

*22 December 2018 (established)*

## Activities

**Secretary-General's High-level Panel on Digital Cooperation**

UN Secretary-General

- Convened by the UN Secretary-General on 12 July 2018 to advance proposals to strengthen cooperation in the digital space among Governments, the private sector, civil society, international organizations, technical and academic communities and other relevant stakeholders
- Expected to raise awareness about the transformative impact of digital technologies across society and the economy, and contribute to the broader public debate on how to ensure a safe and inclusive digital future for all, taking into account relevant human rights norms
- The Panel has a total of 20 members, representing a cross-section of expertise from government, private industry, civil society, academia and the technical community
- Deliverables: in June 2019 the Panel will submit a report that will provide a high-level independent contribution to the broader public debate on digital cooperation frameworks and support Member States in their consultations on these issues

# United Nations (UN)

Last Updated: October 2019

- The HLP's final Report is expected to:
    1. raise awareness about the transformative impact of digital technologies across society and the economy
    2. identify policy, research and information gaps as well as ways to improve interdisciplinary action on digital technologies, and
    3. present concrete proposals to strengthen cooperation in the digital space in an effective and inclusive manner

Source Source 2

*12 July 2018*

**"Combatting Cybercrime: Tools and Capacity Building for Emerging Economies" Toolkit**

ITU, UNCTAD, UNICRI, UNODC

Includes resources aimed at building capacity among policy-makers, legislators, public prosecutors & investigators, and civil society in developing countries in the policy, legal and criminal justice aspects of the enabling environment to combat cybercrime

Source

*2016*

**Global Cybersecurity Index**

ITU

• Multi-stakeholder initiative to measure the commitment of countries to the ITU's Global Cybersecurity Agendathrough surveys;
• Aims to instigate international cooperation and promote knowledge exchange on this topic;
• Iterations of the project result in reports (third iteration currently in progress).

Source

*2013-2014 (first iteration)*

**Digital Blue Helmets Programme**

Office of Information and Communications Technology

- The Programme is intended to serve as a common platform for rapid information exchange and better coordination of protective and defensive measures against information technology security incidents for the United Nations, including agencies, funds and programmes
- Serves as a platform for rapid information exchange; the core of the UN’s cyber defense; the designer of resiliency; and the leader of coordinated protective measures against cybersecurity incidents
- Long-term measures:
    - Continue to build the UN’s defenses against external threats
    - Enrich national cybersecurity defenses for Member States, on demand
    - Mitigate the effects of “zero-day” vulnerabilities Establish additional cybersecurity ground rules
    - Promote digital IDs and encourage the shift to biometrics
    - Encourage stronger encryption
    - Combat online trafficking Improve the ability of the UN to deliver on its mandates through secured ICT
- Key action lines:
    1. Help prevent and combat cyberwarfare
    2. Protect critical infrastructure - including food chains, supply networks, and commodities markets - from cyber-attacks
    3. Facilitate dialogue to ensure a peaceful, open, secure, and cooperative cyberspace
    4. Prevent and stop human trafficking and online exploitation of people
    5. Counter cyberthreats to human and economic development

Source Source 2

*2017*

**Global Programme on Cybercrime**

UNODC

- Mandated by the UNGA and the Commission on Crime Prevention and Criminal Justice to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance
- Comprises as part of the Programme the Cybercrime Repository, a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance
- Main geographic nexus (as of 2017): Central America, Eastern Africa, MENA and South East Asia & the Pacific
- Key aims:
    - Increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime, especially online child sexual exploitation and abuse, within a strong human-rights framework

# United Nations (UN)

Last Updated: October 2019

- Efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence
- Strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks

Source Source 2

**United Nations Group on Cybercrime and Cybersecurity**

ITU, UNODC

• To address programme policy aspects of the work and to foster coordination and collaboration within the United Nations system
• Offered report to the High-Level Committee on Programmes at its 28th session in November 2014

Source

*17 October 2013*

**International Security Cyber Issues Workshop Series**

UNIDIR, Center for Strategic and International Studies (CSIS)

- The goal is to promote common understandings among governments, academics and technologists on problems for peace and stability in cyberspace and on a range of possible solutions at the regional and multilateral levels
- The Workshop Series was organized by UNIDIR and CSIS in two Phases:
  - Phase I (2015-2016): a series of three expert workshops to help identify areas of common understandings and of divergence on number of cybersecurity issues, including on norm development, legal measures and possible approaches to the malicious use of cyber tools
  - Phase II: (2017-2019): a series of three expert workshops to involve regional audiences to help to identify areas of common understandings on cybersecurity issuesl; the major goal to to promote common understandings among governments, academics and technologists on problems for peace and stability in cyberspace and on a range of possible solutions at the regional and multilateral levels
- The Workshop Series was successfully concluded with the workshop on the Role of Regional Organizations in Strengthening Cybersecurity and Stability on 24 January 2019 in Geneva, Switzerland

Source Source 2

*2015-2016 (Phase I); 2017-2019 (Phase II)*

## External Cooperation

**Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust**

Security Council Counter-Terrorism Committee and ICT4Peace Foundation

Goal is to identify the emergence of norms of voluntary self-regulation amongst the private sector in their responses to terrorist use of their products and services, highlight multi-stakeholder and public-private initiatives aimed at supporting efforts in this area, identify persisting challenges, and recommend further areas for engagement

Source

*December 2016*