AN INITIAL OVERVIEW OF UN SYSTEM ACTORS, PROCESSES AND ACTIVITIES ON ICT-RELATED ISSUES OF INTEREST TO THE OEWG, BY THEME

The Open-Ended Working Group (OEWG) established pursuant to resolution 73/27 is mandated to study the possibility of establishing regular institutional dialogue on the theme of information and communications technologies (ICTs) and international security.

This theme touches upon the work of many parts of the Principle Organs of the United Nations, including the General Assembly, the Security Council, and the Economic and Social Council. Several delegations at the first session of the OEWG suggested that existing bodies and processes might be suitable for this role of regular dialogue and noted the importance of not duplicating the work or mandates of other bodies. In order to inform consideration of this issue in advance of the OEWG’s second session, Part I of this paper identifies actors, processes and activities that directly address ICTs and international security and international law (or existing bodies which could do so if requested).

In addition, at the first session of the OEWG many delegations acknowledged the interplay between the international security dimension of ICTs with other key priorities of the United Nations such as sustainable development, human rights and counter-terrorism—and expressed an interest in learning more about UN system activities outside of the First Committee’s remit in order to situate their deliberations on regular dialogue within this wider ecosystem. Thus, Part II of this paper contains a sampling of UN system actors, processes and activities that address ICTs and other themes that are outside the purview of the First Committee yet have been mentioned by delegates at the first session of the OEWG or have been acknowledged in previous reports of the Groups of Governmental Experts. These include the topics of: Cybercrime; Counter-Terrorism; Human Rights; Sustainable Development; Internet Governance; Technical Standards and Best Practices; and Training.

Within each thematic section, entries are grouped by main bodies and committees of the UN system, followed by UN departments/offices or specialized agencies, and concluding with other entities, stand-alone initiatives or reports.

This is not an exhaustive compendium of all UN initiatives concerning digital technologies, nor does each entry reflect the entirety of an entity’s activities or a resolution’s content. It is merely an initial thematically organized overview of a broad range of existing UN actors, processes and activities addressing various facets of ICTs of interest to the OEWG to help inform discussions at its second session.

---

1 Selection for inclusion was informed by the direct relevance to issues within the OEWG’s mandate and interest expressed by delegations at the first session of the OEWG. This overview is not exhaustive.
2 See preambular paragraphs in the resolutions cited for earlier and related resolutions and decisions.
Part I
International Security, including International Law

Principal organs, main bodies and committees

**General Assembly First Committee—Disarmament and International Security**

The issue of developments in the field of ICTs in the context of international security was first introduced to the agenda of First Committee in 1998 via resolution 53/70, and presented annually thereafter. These First Committee resolutions established five Groups of Governmental Experts (GGEs, 2004–2005; 2009–2010; 2012–2013; 2014–2015; and 2016–2017), three of which produced consensus reports. In 2018, Member States decided to establish a sixth GGE and an Open-Ended Working Group (OEWG), both of which commenced work in 2019.

The mandates of the two processes both consider existing and potential threats; capacity-building; confidence-building measures; norms, rules and principles for responsible State behaviour; and the application of international law to the use of ICTs. The mandate of the OEWG includes an additional element: to study the possibility of establishing regular institutional dialogue under the auspices of the United Nations. The OEWG will conclude its work in mid-2020; the GGE in mid-2021.

The annual resolution on ICTs and international security (most recently resolutions 73/27 in 2018 and A/C.1/74/L.50/Rev.1 of 2019) invites Member States to submit their national views on the subject, which are issued as reports by the Secretary-General.

https://www.un.org/disarmament/ict-security/

OEWG: https://www.un.org/disarmament/open-ended-working-group/

GGE: https://www.un.org/disarmament/group-of-governmental-experts/

For a summary of recommendations of the three consensus GGE reports, on law and norms: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-International-Law.pdf


**General Assembly Sixth Committee—Legal**

The Sixth Committee is the General Assembly’s forum for consideration of legal questions by all Member States. The annual report of the International Law Commission (see below) is discussed in Sixth Committee. The Sixth Committee has yet to take up the topic of ICTs and international security.


**International Court of Justice (ICJ)**

One of the six principal organs of the UN, the ICJ’s role is to settle legal disputes submitted by States and to give advisory opinions on legal questions referred to it by authorized UN organs and specialized agencies, such as the request by the General Assembly in resolution 49/75K on the legality of the threat or use of nuclear weapons. The topic of ICTs and international security has yet to be referred to the ICJ.

https://www.icj-cij.org/en
International Law Commission (ILC)

The ILC is mandated by the General Assembly to encourage the progressive development and codification of international law. The 34 seats on the ILC are distributed by regional groups for five-year terms. The annual ILC report is discussed in Sixth Committee. Although the ILC has yet to take up the topic of ICTs and international security directly, at its seventy-first session (2019), the topic “Protection of personal data in transborder flow of information” was added to the ILC’s programme of work. When considering adding new topics to its work programme the ILC uses the following criteria: “(i) the topic should reflect the needs of States in respect of the progressive development and codification of international law; (ii) the topic should be at a sufficiently advanced stage in terms of State practice to permit progressive development and codification; (iii) the topic should be concrete and feasible for progressive development and codification; and (iv) the Commission should not restrict itself to traditional topics, but should also consider those that reflect new developments in international law and pressing concerns of the international community as a whole.”

https://legal.un.org/ilc/
https://legal.un.org/ilc/programme.shtml#a53

Security Council

Under Chapter VII of the UN Charter, a Member State could bring an ICT incident to the attention of the Security Council, although this has yet to happen. Under Article 39, the Council shall determine the existence of any threat to the peace, breach of the peace or act of aggression and determine measures to maintain or restore international peace and security.

In 2017 the Security Council adopted resolution 2341 on the protection of critical infrastructure against terrorist attacks, which recognizes cybersecurity as an important element of protection. The Security Council was briefed on the use of ICTs and international security for the first time in 2016, through an “Arria formula” meeting.³ The objective of the meeting, which involved the participation of representatives from governments, regional organizations, the private sector, and civil society, was to consider the potential of State use of ICTs in fuelling political or military tensions and the importance of the protection of ICT-dependent critical infrastructure.⁴ A second Arria-formula meeting organized in April 2017 on the topic of “hybrid wars as a threat to international peace and security” focused on the changing character of warfare driven by the “increasing use of new technologies and strategies”, and in this regard cited “cyber technologies, interference with political processes, and systematic dissemination of propaganda domestically and internationally, among the means to achieve political objectives”.⁵

https://www.un.org/securitycouncil/

United Nations Disarmament Commission (UNDC)

³ “The ‘Arria-formula meeting’ are very informal, confidential gatherings which enable Security Council members to have a frank and private exchange of views, within a flexible procedural framework, with persons whom the inviting member or members of the Council (who also act as the facilitators or conveners) believe it would be beneficial to hear and/or to whom they may wish to convey a message.” See http://www.un.org/en/sc/about/methods/bgarriaformula.shtml.
The UNDC is a deliberative body that considers and makes recommendations on disarmament-related issues. Meeting for three weeks each year, the UNDC’s agenda comprises two substantive items that are discussed for three consecutive years. Outputs of the UNDC have included consensus principles, guidelines and recommendations which are then transmitted to the General Assembly. Topics are determined by Member States and agreed via a resolution in the First Committee. The Commission’s current topics are under consideration through 2020. The UNDC has yet to take up the topic of ICTs and international security.

https://www.un.org/disarmament/institutions/disarmament-commission/

Departments/offices and specialized entities

Department of Political and Peacebuilding Affairs (DPPA)
The Mediation Support Unit of DPPA has developed a report and accompanying Toolkit on “Digital Technologies and Mediation in Armed Conflict”. In addition to exploring practical applications of technology in mediation contexts, the report and Toolkit also highlight how digital technologies impact mediation efforts. DPPA has a leading role in supporting the Secretary-General’s offer to make available his good offices to contribute to the prevention and peaceful settlement of conflicts stemming from malicious activity in cyberspace (Action 30 of the Secretary-General’s Agenda for Disarmament).

https://dppa.un.org/en
https://peacemaker.un.org/digitaltoolkit

Office for Disarmament Affairs (UNODA)
UNODA’s mandate on ICT security is derived from the priorities established in relevant General Assembly First Committee resolutions. As such, it supports the Chairs and the Members of both the OEWG and the GGE. As part of the UN Secretariat, UNODA also supports the Secretary-General and his Executive Office on matters pertaining to international ICT security. In this capacity, it pursues the implementation of the relevant commitments included in the Secretary-General’s Agenda for Disarmament. UNODA, in partnership with Member States, also contributes to awareness raising and capacity-building, such as through the online training course on Cyberdiplomacy. UNODA’s work on ICT security is closely coordinated with its work on other matters related to science and technology in the context of international security, as well as with broader work strands on emerging technologies within the Secretariat and the wider UN system.

https://www.un.org/disarmament/ict-security/

Office for the Coordination of Humanitarian Affairs (OCHA)
In 2014, OCHA issued a policy paper entitled “Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies”, which recommended advocating for a “humanitarian cyberspace”. In 2017 OCHA established The Centre for Humanitarian Data, with the objective of helping to ensure that those in humanitarian situations have access to the data they need, when and how they need it, to make responsible and informed decisions. The Centre is focused on four areas: data services; data literacy; data policy; and network engagement.

https://www.unocha.org/publication/policy-briefs-studies/humanitarianism-age-cyber-warfare
https://centre.humdata.org/
United Nations Institute for Disarmament Research (UNIDIR)

UNIDIR conducts independent research and analysis, convenes multistakeholder expert workshops and conferences, and develops resources for policymakers on cybersecurity-related issues. Within its Security and Technology Programme cyber workstream, UNIDIR focuses on supporting the implementation of specific norms and recommendations previously agreed in multilateral processes and explores options to strengthen cyber stability and crisis management mechanisms. UNIDIR holds an annual multistakeholder Cyber Stability Conference, and maintains the Cyber Policy Portal, an online reference tool with cyber policy profiles of all 193 Member States. Through its role as Consultant, UNIDIR also supports intergovernmental processes such as the UN GGEs and OEWG.

www.unidir.org

CyberPolicyPortal.org


Other

Conference on Disarmament (CD)

Since the First Special Session on Disarmament in 1978, the 64 Member CD has been considered “the single multilateral disarmament negotiating forum of the international community”. In recent years, the Members of the Conference have raised ICT-related issues in discussions on “New types of weapons of mass destruction and new systems of such weapons”. In 2018, substantive discussions were held in CD Subsidiary Body 5 on the security dimensions of ICTs and artificial intelligence/machine learning.


Global Pulse

Global Pulse is an innovation initiative of the Secretary-General on big data. Its mission is to accelerate discovery, development and scaled adoption of big data innovation for sustainable development and humanitarian action. In 2018 Global Pulse produced a study “Experimenting with Big Data and Artificial Intelligence to Support Peace and Security”.


Secretary-General’s Agenda for Disarmament

In 2018, with the objective of placing disarmament and non-proliferation at the centre of the work of the United Nations, the Secretary-General launched his Agenda for Disarmament “Securing Our Common Future”. In it, the Secretary-General commits to make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace (Action 30) and to engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace (Action 31). Other action items in the Agenda include promoting
multistakeholder dialogue and engagement on emerging technologies (Actions 27, 39 and 40), encouraging responsible innovation (Action 28), and keeping humans in control over the use of force (Action 29).


Secretary-General’s High-Level Panel on Digital Cooperation (HLP)

The multistakeholder HLP was convened by the Secretary-General in 2018 to consider how to collectively realize the potential of digital technologies for humanity while mitigating their risks. The HLP delivered its report “The Age of Digital Interdependence” in June 2019, containing recommendations on inclusive digital economies and societies; developing capacity; protecting rights and agency; promoting trust, security and stability; and fostering global cooperation.

Of particular interest to the OEWG is the recommendation to mark the UN’s 75th anniversary in 2020 with a Global Commitment on Digital Trust and Security “to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.” (See recommendation 4).

https://digitalcooperation.org/

Part II
Other themes

Part II of this paper contains actors, processes and activities that address ICTs and other themes that are outside the remit of the First Committee of the General Assembly yet have been mentioned by delegates at the first session of the OEWG or have been acknowledged in previous reports of the Group of Governmental Experts as significant. These include the topics of Cybercrime; Counter-Terrorism; Human Rights; Sustainable Development; Internet Governance; Technical Standards and Best Practices; and Training.

Cybercrime

Principal organs, main bodies and committees

General Assembly Third Committee—Social, Humanitarian and Cultural Issues

On 18 November 2019, Third Committee delegates voted to adopt the resolution “Countering the use of information and communications technologies for criminal purposes” (A/C.3/74/L.11/Rev.1), which establishes an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes. An organizational session will be held in August 2020.

In an earlier resolution (73/187) the General Assembly requested the Secretary-General to seek the views of Member States on the challenges that they faced in countering the use of ICTs for criminal purposes and issue a report. The Report of the Secretary-General prepared pursuant to General Assembly resolution 73/187, entitled “Countering the use of information and communications technologies for criminal purposes” (A/74/130) reflects the responses of over 60 Member States.

https://undocs.org/A/C.3/74/L.11/Rev.1
https://undocs.org/A/74/130

On the basis of ECOSOC’s recommendation (see below), Third Committee adopted the resolution “Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing” (A/C.3/74/L.5), which encourages States to implement measures to ensure that cybercrime can be investigated and prosecuted at the national level and facilitate effective international cooperation; urges training of relevant law enforcement and judiciary officials; and encourages appropriate technical assistance and capacity building, as well as cooperation with the private sector and civil society.

https://undocs.org/A/C.3/74/L.5

Economic and Social Council (ECOSOC)

One of the six principal organs of the United Nations, the 54 member Council coordinates the economic and social fields of the UN’s work and serves as a forum for discussing and formulating policy recommendations for States and the UN system.
In July 2019, ECOSOC adopted the resolution “Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing” (E/RES/2019/19), recognizing the important work of the Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of Cybercrime (see entry below) as an “important platform for the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses for cybercrime”. The resolution also encourages Member States to implement effective international cooperation on cybercrime investigation and prosecution; training of officials to equip them to “effectively carry out their respective roles in investigating, prosecuting and adjudicating cybercrime offences”, and provide, upon request and based on needs, “appropriate technical assistance and sustainable capacity-building to strengthen the ability of national authorities to deal with cybercrime”.


ECOSOC Functional Commission: Commission on Crime Prevention and Criminal Justice (CCPCJ)

The CCPCJ is the UN’s principal policymaking body in the field of crime prevention and criminal justice. The CCPCJ offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies, and to identify priorities for combating crime. CCPCJ is the governing body of the United Nations Office on Drugs and Crime (UNODC).

Thematic discussion at the 27th CCPCJ session (May 2018) focused on “Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels”.

http://www.unodc.org/unodc/commissions/CCPCJ/

Specialized entities

United Nations Office on Drugs and Crime (UNODC)

The UNODC Global Programme on Cybercrime provides focused technical assistance for capacity building, prevention and awareness raising, international cooperation and analysis, principally in developing countries.


Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of Cybercrime

Via resolution 65/230 the CCPCJ established an open-ended intergovernmental expert group to conduct a comprehensive study of 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 international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. At its fourth meeting in 2018, the expert group adopted its workplan for the period 2018–2021. In 2020, the group will discuss international cooperation and prevention.

UNODC Cybercrime Repository

The cybercrime repository is 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. It includes databases on cybercrime case law, legislation and lessons learned from national practices.

https://sherloc.unodc.org/clv3/cybrepo/

United Nations Interregional Crime and Justice Research Institute (UNICRI)

The UNICRI project “Security through Research, Technology and Innovation” aims at increasing knowledge and information sharing on supply chain security, cybersecurity, artificial intelligence, blockchain and big data analytics. The project is focused on enhancing awareness on emerging risks and possible policy responses; fostering cooperation, exchange and sharing of good practices and informational resources.

http://www.unicri.it/special_topics/SIRIO_Security_and_Innovation/

Counter-Terrorism

Principal organs, main bodies and committees

Through the UN Global Counter-Terrorism Strategy (adopted by consensus via resolution 60/288) Member States have committed to “work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to: (a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard”. The strategy is reviewed every two years. In its most recent review in 2018 (resolution 72/284), Member States noted the importance of developing the most effective means to counter terrorist propaganda, incitement and recruitment, including through the Internet; the urgent need for the international community to counter terrorists’ exploitation of ICTs to craft distorted narratives; and noted the importance of multistakeholder cooperation to implement the Strategy.

https://undocs.org/en/A/RES/72/284

Security Council

The use of the Internet and ICTs for terrorist purposes is addressed by the Security Council and its subsidiary bodies. Security Council resolution 2129 (2013) directs the Counter-Terrorism Committee Executive Directorate (CTED, see below) to continue to address the use of ICTs for terrorist activities, in consultation with Member States, international, regional, and subregional organizations, the private sector, and civil society, and to advise the Committee on further approaches. Security Council resolution 2178 (2014) on foreign terrorist fighters calls on Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications, and resources to incite support for terrorist acts.

Security Council Counter-Terrorism Committee (CTC)

CTC supports Member States to prevent terrorist acts both within their borders and across regions. The Committee has organized special meetings on “Preventing terrorists from exploiting the Internet and social media to recruit terrorists and incite terrorist acts, while respecting human rights and fundamental freedoms” and “Preventing the exploitation of ICT for terrorist purposes, while respecting human rights and fundamental freedoms.”

https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/

Security Council Counter-Terrorism Committee Executive Directorate (CTED)

CTED carries out the policy decisions of the Counter-Terrorism Committee, conducting expert assessments of each Member State and facilitating counter-terrorism technical assistance to countries. It has conducted significant work in cooperation with INTERPOL and the UN Office of Counter-Terrorism, on protecting critical infrastructure against terrorist attacks, through capacity-building activities and promotion of best practices—including the Compendium of Good Practices on the Protection of Critical Infrastructures Against Terrorist Attacks. CTED has engaged with the private sector and civil society to further understanding of industry responses to the use of ICTs for terrorist purposes and identify good practices. CTED also works with the International Association of Prosecutors and UNODC to strengthen cooperation among national prosecutors engaged in counter-terrorism issues.

CTED launched and supports the project Tech Against Terrorism to help the global tech industry protect itself from terrorist exploitation, while respecting freedom of expression and human rights.

https://www.un.org/sc/ctc/


https://www.techagainstterrorism.org/

Departments/offices and specialized entities

Office of Counter-Terrorism (OCT)

OCT is mandated to, inter alia, enhance coordination and coherence across the 38 Global Counter-Terrorism Coordination Compact Task Force entities to ensure the balanced implementation of the four pillars of the UN Global Counter-Terrorism Strategy; strengthen the delivery of United Nations counter-terrorism capacity-building assistance to Member States; and ensure that due priority is given to counter-terrorism across the UN system.

The United Nations Counter-Terrorism Centre helps to develop national and regional Counter-Terrorism Strategy implementation plans in support of the Global Counter-Terrorism Strategy; promotes cooperation and collaboration between national, regional and international counter-terrorism centres and organizations; and helps build capacity of Member States to strengthen their counter-terrorism capability. The UNCCT 5-Year Programme includes a specific output helping Member States to be better able to prevent terrorist cyber-

6 In 2017, the Counter-Terrorism Implementation Task Force (CTIFT) and the UN Counter-Terrorism Centre, initially established in the Department of Political Affairs, were moved into the newly established OCT.
attacks, and mitigate the effects and expedite recovery should they occur. The **Integrated Assistance on Countering Terrorism (I-ACT) Initiative** aims to enhance the capacity within the UN to help interested Member States, upon their request and in a user-friendly way, to implement the Global Counter-Terrorism Strategy.

https://www.un.org/counterterrorism/ctitf/

**United Nations Office on Drugs and Crime (UNODC)**

In 2012, UNODC in cooperation with the United Nations Counter-Terrorism Implementation Task Force, conducted the study “Use of the Internet for Terrorist Purposes” in order to provide guidance regarding legal frameworks and practice at the national and international levels relating to the criminalization, investigation and prosecution of terrorist cases involving the Internet.


**Human Rights**

**Principal organs, main bodies and committees**

**General Assembly Third Committee—Social, Humanitarian and Cultural Issues**

Similar to the Human Rights Council resolution of 2017 on the same theme (see below), the Third Committee resolution A/C.3/73/L.49 "**The right to privacy in the digital age**“ affirms that the same rights that people have offline must also be protected online; that any interference with the right to privacy must be consistent with the principles of legality, necessity and proportionality; and encourages all States to promote an open, secure, stable, accessible and peaceful ICT environment based on respect for international law, including the obligations enshrined in the Charter and human rights instruments.

https://undocs.org/A/C.3/73/L.49/Rev.1

**Report of the Secretary-General on Strengthening the Role of the United Nations in Enhancing the Effectiveness of the principle of periodic and genuine elections and the promotion of democratization (A/74/285)**

The report includes a reflection on some of the “complex issues emerging around the growing influence in elections of the Internet and social media, being both enablers of participation and tools for spreading disinformation and hate speech, including against women, and to incite violence.” The report references the Paris Call on Trust and Security in Cyberspace as well as the recommendations of the Secretary-General’s High-Level Panel on Digital Cooperation and the importance of seeking “universal and multi-stakeholder commitments with respect to digital trust and security”, which are “critical for addressing such threats, including in elections.” The resolution welcoming the Secretary-General’s report (A/C.3/74/L.46/Rev.1) expresses concern over “the spread of disinformation by both internal and external actors on traditional and
social media, as well as efforts to manipulate voting systems and the blocking of the Internet and social media in the framework of elections, constitute an increasing problem for democracies around the world.”


https://undocs.org/A/C.3/74/L.46/Rev.1

Human Rights Council

The 2018 Report of the High Commissioner on The right to privacy in the digital age (A/HRC/39/29) provides an overview of the international legal framework, the obligations of States and the responsibility of the private sector, and addresses the collection of personal data by governments and businesses, as well as State surveillance and communications interception. The report builds on the 2014 report A/HRC/27/37.

Recent Human Rights Council (HRC) resolutions addressing human rights in the digital domain include:

2019 Resolution on the right to privacy in the digital age (42/15)

Affirms that the same rights that people have offline must also be protected online; that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality; and encourages all States to promote an open, secure, stable, accessible and peaceful ICT environment based on respect for international law, including the obligations enshrined in the Charter and human rights instruments. The resolution specifically notes that human rights considerations must be taken into account in the design, development, deployment and use of artificial intelligence.


https://undocs.org/A/HRC/39/29

https://undocs.org/A/HRC/RES/42/15

2018 Resolution on the promotion, protection and enjoyment of human rights on the Internet (A/HRC/38/L.10/Rev.1)

This consensus resolution, inter alia, calls upon all States to bridge the digital divides, including the gender digital divide, in order to promote the full enjoyment of human rights; to address security concerns on the Internet in accordance with their international human rights obligations to ensure the protection of all human rights online; urges States to enact laws, regulations, policies and other measures concerning personal data and privacy protection online; and “condemns unequivocally measures, in violation of international human rights law, that prevent or disrupt an individual’s ability to seek, receive or impart information online.”

The resolution also encourages the private sector “to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States’ obligations under international human rights law.”

https://undocs.org/A/HRC/38/L.10/Rev.1
Special Rapporteurs on:

- **Promotion and protection of the right to freedom of opinion and expression** have produced recent reports on online hate speech (A/74/486), artificial intelligence (A/73/348); surveillance (A/HRC/41/35), online content regulation (A/HRC/38/35), roles of private actors engaged in the provision of Internet and telecommunications access (A/HRC/35/22); mapping the ways in which the information and communications technology sector implicates freedom of expression (A/HRC/32/38) and encryption and anonymity tools (A/HRC/29/32)

- **Right to privacy:** In 2015, the HRC decided to appoint a Special Rapporteur on the right to privacy, to examine inter alia alleged violations of the right to privacy including in connection with the challenges arising from new technologies. See, in particular, on big data and open data (A/73/45712)

- **Promotion and protection of human rights and fundamental freedoms while countering terrorism** have addressed the use of digital surveillance for counter-terrorism purposes (see, for example, A/69/397, section III and A/HRC/34/61)

Specialized agency

**UNESCO**

UNESCO’s Knowledge Societies Division (KSD) is responsible for coordination of UNESCO’s follow up to WSIS, including “information ethics”, which are the ethical, legal and societal aspects of using information and communication technologies derived from the Universal Declaration on Human Rights. Among other activities, KSD promotes free and open source software and open standards, and through the Information for All Programme, assists states to develop national information policy frameworks.

https://en.unesco.org/themes/building-knowledge-societies

https://en.unesco.org/themes/information-ethics

Other

**Secretary-General’s High-Level Panel on Digital Cooperation (HLP)**

The HLP’s recommendation 3 on human rights and human agency underscored that human rights apply fully in the digital world. It urged the Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. The HLP also stressed that life and death decisions should not be delegated to machines.

https://digitalcooperation.org/


Sustainable Development

**Principal organs, main bodies and committees**

**General Assembly**

In 2018 the General Assembly adopted resolution 73/17 on the “Impact of rapid technological change on the achievement of the Sustainable Development Goals and their targets”. The resolution recognizes that the spread of ICTs and global interconnectedness has great potential to accelerate human progress, to bridge the
digital divide and to develop knowledge societies, and inter alia, calls on all UN Member States and agencies to implement public policies and share best practices so that the new technologies help achieve the 2030 Agenda.

https://undocs.org/A/RES/73/17

**General Assembly Second Committee—Economic and Financial Committee**

Over 15 years ago, the Second Committee adopted its first resolution on the “Creation of a global culture of cybersecurity” (57/239) identifying 9 complementary elements: awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment. The 2004 resolution “Creation of a global culture of cybersecurity and the protection of critical information infrastructures” (58/199) contains an annex “Elements for protecting critical information infrastructures”. The 2010 resolution “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures” contains in annex a “Voluntary self-assessment tool for national efforts to protect critical information infrastructures”.

https://undocs.org/A/RES/58/199
https://undocs.org/A/RES/64/211

At its 74th Session, Second Committee adopted the resolution “Science, technology and innovation for sustainable development” (A/C.2/74/L.58), which emphasizes, inter alia, “the need to effectively harness technology to bridge the digital divides within countries and between developed and developing countries”. It also notes that there is a “gender digital divide”, urges “Member States to mainstream a gender perspective in legislation, policies and programmes”, and emphasizes the importance of the participation of women and girls in science, technology and innovation.

https://undocs.org/A/C.2/74/L.58

It also adopted the annual resolution “Information and communications technologies for sustainable development” (A/C.2/74/L.70), which recognizes that a lack of access to affordable and reliable technologies and services remains a critical challenge in many developing countries and that there is a pressing need to “address the major impediments that developing countries face in engaging with and accessing new technologies, such as an appropriate enabling environment, sufficient resources, infrastructure, education, capacity, investment and connectivity, as well as issues related to technology ownership, setting standards and technology flows, and in this regard urges all stakeholders to consider ensuring appropriate financing of digital development and adequate means of implementation, including strengthened capacity-building of developing countries, particularly the least developed countries, towards a digitally empowered society and knowledge economy;”. The resolution also recognizes the importance of enhanced cooperation in order for governments to carry out their roles and responsibilities in international public policy issues pertaining to the Internet.

https://undocs.org/A/C.2/74/L.70

ECOSOC Functional Commission: **Commission on Science and Technology for Development (CSTD)**

The CSTD is an annual intergovernmental forum for discussion of the nexus of science, technology and development. It is a forum for the examination of science and technology questions and their implications for development; promoting understanding on science and technology policies, particularly in respect of developing countries; and formulating recommendations and guidelines on science and technology matters
within the United Nations system. The CSTD encourages collaboration between Member States, the private sector, academia, and civil society. In addition, the CSTD is mandated by ECOSOC to serve as the focal point in the system-wide follow-up to the outcomes of WSIS. The Secretariat of CSTD is hosted by the United Nations Conference on Trade and Development (UNCTAD).


**Technology Facilitation Mechanism (TFM)**

The TFM supports implementation of the Sustainable Development Goals (SDGs), by facilitating multi-stakeholder collaboration and partnerships through the sharing of information, experiences, best practices and policy advice among Member States, civil society, the private sector, the scientific community, United Nations entities and other stakeholders. The TFM has three components: an Interagency Task Team on Science, Technology and Innovation for the SDGs (IATT), including the 10-Member Group of representatives from civil society, the private sector and the scientific community; the Multi-stakeholder Forum on Science, Technology and Innovation for the SDGs (see below); and an online clearinghouse on existing STI initiatives, mechanisms and programs.

https://sustainabledevelopment.un.org/tfm

**Multistakeholder Forum on Science, Technology and Innovation for the SDGs**

The President of ECOSOC convenes the annual meeting of the Multistakeholder Forum on Science, Technology and Innovation for the SDGs (part of the Technology Facilitation Mechanism mandated by the 2030 Agenda, see above). The Forum provides “a venue for facilitating interaction, matchmaking and the establishment of networks between relevant stakeholders and multi-stakeholder partnerships in order to identify and examine technology needs and gaps, including with regard to scientific cooperation, innovation and capacity-building, and also in order to help facilitate development, transfer and dissemination of relevant technologies for the sustainable development goals.”


**Departments/offices or specialized entities**

**Department of Economic and Social Affairs (DESA)**

DESA’s Division for Public Institutions and Digital Government supports Member States in e-government development and supporting implementation of the SDGs. In addition, DESA hosts the Secretariat of the Internet Governance Forum (see below).


**Other**

**Secretary-General's High-Level Panel on Digital Cooperation (HLP)**

The HLP’s recommendation 1 on **an inclusive digital economy and society** emphasizes affordable access to digital networks, creation of a sharing platform, and the adoption of policies for digital inclusion and digital equality, including development of metrics for digital inclusiveness and the collection of sex disaggregated data. Recommendation 2 on **human and institutional capacity** urges the development of capacity related to social and economic impacts of digital technologies.
World Summit on the Information Society (WSIS)

The global multistakeholder summit was convened to address harnessing the developmental benefits of the digital revolution, while narrowing the digital divide. The initial phase of WSIS (2003) resulted in the Geneva Declaration of Principles and Geneva Plan of Action. The second phase in Tunis two years later addressed operationalizing the Plan of Action as well as consideration of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents. The Action Lines contained in the Plan of Action address, inter alia, ICT infrastructure, capacity building, confidence building and cooperation. The annual WSIS Forum is a global multi-stakeholder platform facilitated by the UN that aims towards the implementation of the WSIS Action Lines.

Internet Governance

Other

Internet Governance Forum (IGF)

The IGF is a global multi-stakeholder platform to facilitate discussion of policy issues related to the Internet. It holds an annual meeting where delegates exchange information, share good practices, and develop a common understanding of how to maximize the opportunities of the Internet, while addressing the risks and challenges. Based on the Tunis Agenda for the Information Society, current capacity building efforts focus on strengthening capacity of developing countries to participate in Internet governance arrangements. Intersessional “Best Practice Forums” focus on cyber security; gender and access; IoT, big data and AI; and local content. Regional and sub-regional IGFs are organized by multistakeholder organizing teams. These IGFs create a space where different stakeholders from the region can discuss issues pertaining to the Internet, reflecting the need of their respective communities. IGF is supported by DESA.

Secretary-General’s High-Level Panel on Digital Cooperation (HLP)

The HLP’s recommendation 5 on Global Digital Cooperation includes proposals to strengthen multi-stakeholder cooperation on digital issues.
Technical Standards and Best Practices

Specialized agency

International Telecommunication Union (ITU)

The ITU is a specialized agency of the UN focused on ICT operations and services. Its membership includes 193 Member States as well as over 900 companies, universities and other organizations. It focuses on three “sectors”: Radiocommunications, Standardization (including standards for ICT network operation and new technologies such as 5G, distributed ledger and AI), and Development (including bridging the “digital divide” in order to meet the connectivity targets set by WSIS). The ITU convenes conferences, meetings and study groups to develop systems, share best practices and formulate principles and guidelines. The ITU also engages in capacity building, through toolkits, guides and meetings; organizing drills for incident response, offering assistance to establish CERTs, etc. The ITU also publishes the Global Cyber Index, a ranking of countries, based on an assessment and aggregated score on national ICT development across five pillars: legal measures; technical measures; organizational measures; capacity building; and cooperation.

https://www.itu.int/en/Pages/default.aspx
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
https://www.itu.int/en/ITU-D/Conferences/connect/Pages/default.aspx
https://www.itu.int/en/action/internet/Pages/default.aspx

Training

Departments/offices and specialized entities

Office for Disarmament Affairs (UNODA)

In 2019 UNODA launched the online training course “Cyberdiplomacy” to encourage greater understanding of the use of ICTs and its implications for international security. The course addresses threats, international law, norms, CBMs, and capacity building.

https://cyberdiplomacy.disarmamenteducation.org/home/

United Nations Institute for Training and Research (UNITAR)

UNITAR occasionally offers courses on “Digital and Cyberdiplomacy” for diplomats and governmental officials, and staff of intergovernmental and non-governmental organizations. The course presents the range of challenges that arise from cyberspace and how diplomacy can be applied to managing them.

https://www.unitar.org/event/