



The [General Assembly First Committee](#) addresses the disarmament of conventional weapons, weapons of mass destruction and related international security questions. The First Committee makes recommendations on the regulation of these weapons as they relate to international peace and security. The First Committee does not consider legal issues surrounding weapons possession nor does it address complex peace and security issues addressed by the Security Council. The First Committee also adheres to the purview guidelines of the [General Assembly](#) as a whole.

Topics:

I. Developments in the field of information and telecommunications in the context of international security.

Governments, businesses and the general public around the globe increasingly rely on information and communication technologies (ICTs) in almost every aspect of life and work. From their role in providing government services and communicating public safety information, to enabling digital commerce and keeping friends and families connected worldwide amid a global pandemic, ICTs will continue to be a constant fixture of 21st century society. Governments have also used ICTs as instruments in [maintaining international peace and security](#), yet these same tools can be used maliciously by State and non-State actors, presenting a bevy of risks. High-profile cyber attacks, such as the targeting of [Iranian](#) and [Indian](#) nuclear power plants, as well as an abundance of [foreign electoral interventions](#) in recent memory, illustrate the international cybersecurity implications of ICTs. The early months of the coronavirus pandemic [unleashed a wave of cyber attacks](#) targeting healthcare organizations and medical research facilities for informational and financial gain. As malicious actors work to hack States' digital infrastructure to gain access to high-level information and state secrets, States have progressively joined the discussion around the need for an international framework for advancing peace and security in cyberspace.

The United Nations first addressed information security in 1998, when the Russian Federation [added the topic](#) to the agenda of the First Committee. In addition to recognizing the importance of information and telecommunications in the context of international security, [Resolution 53/70](#) called for States to submit [reports](#) articulating their stances on the issues of information security to the Secretary-General, initiating an iterative process that has become a key confidence-building measure for understanding where States stand on this ever-evolving subject. Subsequent resolutions on this topic recurred in the First Committee year after year with minimal changes until 2004, when [Resolution 58/32](#) authorized the first Group of Governmental Experts (GGE)—experts from 15 States, appointed by the Secretary-General yet working in their personal capacities—to consider existing and potential threats in the sphere of information security, potential measures for cooperation, and international information security issues. Experts—on behalf of their States—[brought different perspectives and priorities](#) to the GGE, with Russia, China, Brazil and Belarus promoting the right of States to ensure their own information security and the adoption of a

new international legal regime, and the United States and European countries rejecting calls for cyber disarmament. These fundamental differences resulted in the failure of the first GGE to adopt a consensus report, an outcome that stifled progress on this topic until different circumstances permeated the political and security environment as a new GGE convened in 2009.

Cyber-related national security incidents instigated by Russia against [Estonia in 2007 and Georgia and Lithuania in 2008](#) tempered the contentious political climate as participating experts from both West and East [brought compatible priorities](#) to the table as the second GGE convened between 2009 and 2010. Finding common ground on some aspects of this topic, the second GGE produced a [consensus report](#), which the General Assembly adopted without a vote, demonstrating the body's support for the process. The report's contents mostly amounted to early cyber confidence-building measures, but experts recognized the gravity of threats posed in the sphere of information security, agreed to continue discussing norms pertaining to State use of ICTs, and noted a need to explore measures to reduce collective security risks and protect national and international infrastructure from cyber attacks. The subject of international law's application in cyberspace has proven to be a stumbling block in negotiations, given that most of the existing body of international law lacks specialized rules for regulating cyberspace. The [United States](#) and [several Western countries](#) have argued for international law's applicability in cyberspace, while [Russia and China](#) have called for a new international cyber convention. The third GGE in 2013 addressed the longstanding open question by bringing the experts together in [agreement](#) that the existing framework of international law—in particular the United Nations Charter—is applicable to cyberspace, and that future forums could discuss how it does so with greater granularity. The [consensus report](#) produced by the fourth GGE, now expanded to 20 experts, included for the first time a separate section listing 11 voluntary norms of responsible State behavior in their cyber activities. These include norms that States should cooperate in developing and applying measures to increase stability and security in the use of ICTs, States should consider how best to cooperate in exchanging information and assisting each other to address terrorist and criminal uses of ICTs, and States should take appropriate measures to

protect their critical infrastructure from ICT attacks in pursuit of creating a global culture of cybersecurity.

The second, third and fourth GGEs established the foundation for today's discussions on State behavior in cyberspace, but [gridlock and backsliding](#) characterized the fifth GGE that met between 2016 and 2017. Some States appeared to change their positions on the applicability of international law in cyberspace. The applicability of international humanitarian law and the question of whether States could respond to cyber attacks using non-cyber means created friction points that prevented consensus. One attributed cause for this dysfunction is the nature of the GGEs' [closed proceedings and their limited participation list](#) involving only 25 Member States at this point, which failed to create a global environment that encouraged widespread, transparent implementation of the consensus reports' voluntary norms and principles. Separately, the complex geopolitical environment of 2016 and 2017 made negotiations on this delicate subject more difficult to broach among the great power participants. In 2018, debate arose in the General Assembly First Committee over the next iteration of working groups, with Western interests backing a sixth GGE in [Resolution 73/266](#), while the Russian Federation proposed a novel [Open-Ended Working Group](#) (OEWG) in [Resolution 73/27](#). In contrast to the GGEs of years past, the OEWG would be open to any and all interested United Nations Member States. Although this might address some of the perceived issues with the GGE's limited membership, some watchdog groups [noted](#) that the resolution establishing the OEWG omitted references to the past GGEs' consensus reports on the applicability of existing international law in cyberspace. Ultimately, the General Assembly [adopted both resolutions](#), with a majority of Member States voting in favor of both.

Although [pessimism](#) filled the air as the two working groups set out to fulfill their mandates, both the [sixth GGE](#) and the [OEWG](#) submitted final consensus reports in 2021 that now await adoption in the General Assembly First Committee, marking important milestones and highlighting existing gaps in State capacity. Rather than acting as two groups with competing mandates, each [carved out unique roles](#) for themselves. The sixth GGE—comprised of 25 Member States—created an ecosystem where a fewer number of States could deliberate some of the more complicated and politically contentious

aspects of this topic, while the OEWG—open to all interested Member States—served as a forum to build capacity and diffuse technical knowledge among the States who were not as involved with the previous GGEs. These dynamics came to pass as the bodies grappled with the quarrelsome topic of international law’s application to State behavior in cyberspace. The GGE actively engaged in [sophisticated discussions](#) concerning international law, including the role of international humanitarian law, State sovereignty, due diligence and State countermeasures. In contrast, the OEWG only [commented](#) on the applicability of international law in cyberspace at a high level—reaffirming the third and fourth GGE reports—and urged further capacity building on the subject. The vast majority of States [did not issue a position concerning international law](#), potentially out of political considerations or due to a lack of legal capacity to understand and contribute to the topic. With the adoption of [Resolution 75/240](#) in January 2021, deciding to convene a second OEWG from 2021–2025, questions abound of how the OEWG can continue to build capacity among and broaden the conversation to more Member States.

The ability of the sixth GGE to produce a consensus report that built upon past reports, when the fifth GGE failed, marks a step toward the implementation of norms and principles concerning State behavior in cyberspace. Absent from the report, however, is any mention of accountability in the context of State behavior, a difficult subject that [could limit implementation](#) unless the international community reaches consensus around ways to follow through on and enforce their commitments. So far, [47 Member States have called for the creation](#) of a [Programme of Action for advancing responsible State behavior in cyberspace](#), an action-oriented international framework and political commitment to address challenges related to the use of ICTs in the context of cybersecurity that States and other stakeholders face. Both of the recent reports from the GGE and OEWG recommended that the topic of a potential Programme of Action be added to the agenda of the second OEWG in order to ensure that the interests and concerns of all Member States are taken into account through equal State participation. As discussions trend toward establishing some form of Programme of Action, a [natural point of reference](#) will be the 2001 [Programme of Action on Small Arms and Light Weapons](#), also

established under the auspices of the General Assembly First Committee. A cyber Programme of Action could be an effective bridge between calls for a legally binding treaty and the current voluntary normative framework established through the two working groups. Applying lessons from the 2001 Programme of Action could inform a new Programme of Action concerning cyberspace. Some civil society organizations [are already encouraging](#) the United Nations to be ambitious, focus on action and accountability, and ensure all stakeholders are engaged throughout all phases of negotiation and implementation in order to secure responsible State behavior in the context of international peace and security.

Questions to consider from your country's perspective:

- How should the enforcement of international law be changed to effectively regulate State behavior in cyberspace and preserve international peace and security?
- How can the United Nations and the international community help build capacity and knowledge among Member States concerning the role of ICTs in the context of international security?
- What measures should Member States include in a new Programme of Action to ensure States remain accountable to their commitments to responsible behavior in cyberspace?
- What lessons from the 2001 Programme of Action on Small Arms and Light Weapons can be applied to a new Programme of Action on cyberspace? What concerns and recommendations will civil society organizations offer?

Bibliography

- Achten, Nele (2019). [New U.N. Debate on Cybersecurity in the Context of International Security](#). *Lawfare*.
- CyberPeace Institute (2021). [The OEWG Final Report: New Milestone in Global Cyber Diplomacy, Collective Efforts Still Needed to Close the Accountability Gap and Achieve CyberPeace](#).
- CyberPeace Institute (2021). [The UN GGE Final Report: A Milestone in Cyber Diplomacy, but Where Is the Accountability?](#)

- Digital Watch Observatory (2018). [Developments in the Field of Information and Telecommunications in the Context of International Security \(A/RES/73/27\)](#).
- Digital Watch Observatory (2017). [Digital Watch Newsletter—Issue 22—June 2017](#).
- Digital Watch Observatory (2020). [France and Partners Propose a Programme of Action for Advancing Responsible State Behaviour in Cyberspace](#).
- Farnsworth, Timothy (2011). [China and Russia Submit Cyber Proposal](#). *Arms Control Association*.
- France, et al (2020). [The Future of Discussions on ICTs and Cyberspace at The UN](#).
- Global Commission on the Stability of Cyberspace (2021). [Statement from the GCSC on the Final Draft of the Substantive Report of the UN Open-ended Working Group](#).
- Hollis, Duncan (2021). [A Brief Primer on International Law and Cyberspace](#). *Carnegie Endowment for International Peace*.
- Iasiello, Emilio (2019). [OEWG or GGE—Which Has the Best Shot of Succeeding?](#) *Technative*.
- Kaspar, Lea, and Sheetal Kumar (2019). [Cyber Norms in NYC: Takeaways from the OEWG Meeting and UNIDIR Cyber Stability Conference](#). *Global Partners Digital*.
- Koh, Harold Hongju (2012). [International Law in Cyberspace](#). *Harvard International Law Journal*.
- [The Latest: UN Warns Cybercrime on Rise During Pandemic](#) (2020). *Associated Press*.
- Lowe, Christian (2009). [Kremlin Loyalist Says Launched Estonia Cyber-attack](#). *Reuters*.
- Moynihan, Harriet (2019). [The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention](#). *Chatham House Royal Institute of International Affairs*.
- Nakashima, Ellen, and Joby Warrick (2012). [Stuxnet Was Work of U.S. and Israeli Experts, Officials Say](#).
- Ruhl, Christian, et al. (2020). [Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads](#). *Carnegie Endowment for International Peace*.

- Schmitt, Michael N. (2021). [Foreign Cyber Interference in Elections](#). *International Law Studies*.
- Tikk-Ringas, Eneken (2012). [Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012](#). *ICT4Peace Foundation*.
- Tikk-Ringas, Eneken, et al. (2010). [International Cyber Incidents: Legal Implications](#). *The NATO Cooperative Cyber Defense Centre of Excellence*.
- United Nations Group of Governmental Experts (2021). [Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security](#).
- United Nations Institute for Disarmament Research (2017). [The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century](#).
- United Nations Office for Disarmament Affairs (2021). [Developments in the Field of Information and Telecommunications in the Context of International Security](#).
- United Nations Office for Disarmament Affairs (2021). [Open-ended Working Group](#).
- United Nations Office for Disarmament Affairs (2021). [Programme of Action on Small Arms and Its International Tracing Instrument](#).
- Women’s International League for Peace & Freedom (2021). [Programming Action: Observations from Small Arms Control for Cyber Peace](#).
- Zetter, Kim (2014). [An Unprecedented Look at Stuxnet, the World’s First Digital Weapon](#). *Wired*.

[Top ↑](#)

United Nations Documents:

- United Nations, General Assembly (2021). [Open-ended Working Group on developments in the field of information and telecommunications in the context of international security: Final substantive report](#). A/AC.290/2021/CRP.2.
- United Nations, General Assembly (2020). [Developments in the field of information and telecommunications in the context of international security](#). A/RES/75/240.

- United Nations, General Assembly (2018). [Advancing responsible State behavior in cyberspace in the context of international security](#). A/RES/73/266.
- United Nations, General Assembly (2018). [Developments in the field of information and telecommunications in the context of international security](#). A/RES/73/27.
- United Nations, General Assembly (2015). [Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security](#). A/70/174.
- United Nations, General Assembly (2013). [Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security](#). A/68/98.
- United Nations, General Assembly (2010). [Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security](#). A/65/201.
- United Nations, General Assembly (2003). [Developments in the field of information and telecommunications in the context of international security](#). A/RES/58/32.
- United Nations, General Assembly (1999). [Developments in the field of information and telecommunications in the context of international security](#). A/RES/53/70.

[Top ↑](#)

II. Women, disarmament, non-proliferation and arms control

With the adoption of the [Convention on the Elimination of all Forms of Discrimination Against Women](#) in 1979, the United Nations recognized the importance of complete disarmament in achieving full equality between men and women. Since then, the international community has increasingly examined the unique, nuanced and diverse ways in which armed conflict disproportionately affects women, and often in gender-specific ways. In 2019, [96 percent of conflict-related sexual violence](#) targeted women and girls. Explosive weapons also often target marketplaces, the second highest location for civilian casualties, which [disproportionately affects women](#), who

are often responsible for buying food and household necessities at markets. Despite carrying many of the burdens of the consequences of conflict, women tend to be underrepresented in decisions that are made regarding disarmament, with only [three out of every 10](#) peace agreements between 1992 and 2019 including any women in their negotiation or signing. Ensuring the equitable representation of women's voices on the issues of disarmament, non-proliferation and arms control is necessary to promote collective security and stability for all Member States, as research has shown that peace talks which meaningfully involve women yield a [greater likelihood](#) of lasting peace.

In 2000, the Security Council [passed a resolution](#) encouraging Member States to include the perspective of women in all fields of operations, including in peace negotiations, post-conflict reconstruction and disarmament. Subsequently, the Office of Disarmament Affairs adopted a [Gender Action Plan](#) in 2003 to explore the connection between disarmament and gender equality, incorporate gender into its ongoing work, and advocate for including gender perspectives and advocates in disarmament discussions. Progress in implementing this plan was slow and uneven; by 2004 the [Secretary-General noted](#) that women's participation in developing policies and guidelines had increased, while substantial gaps remained in directly including women in conflict resolution processes. The ad hoc nature of voluntary financial contributions for initiatives focused on increasing attention to gender perspectives, protecting the human rights of women and promoting women's participation in the arms control space have contributed to slow progress in the resolution's implementation. In 2006, the United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects convened and established [concrete recommendations](#) for gender mainstreaming and including women in the implementation of the original 2001 United Nations [Programme of Action](#) (PoA), a foundational policy document in arms control. While the original PoA provided detailed policy recommendations, it did not discuss how the illicit small arms trade affects women or what their role is in addressing disarmament. The report created a set of guidelines focused on four areas: women's relevance in combating the illicit trade of

small arms and light weapons; planning and implementation of disarmament, demobilization and reintegration; national and regional foci; and civil society and public awareness initiatives. These guidelines were reviewed again in [2010](#) and [2016](#) and have served as references for efforts moving forward.

The General Assembly passed a [resolution](#) in 2010 focused solely on women's role in disarmament, non-proliferation and arms control, the first of its kind, and adopted the [Arms Trade Treaty](#) (ATT) in 2013, now the primary international agreement regulating the legal movement and transfer of arms. Articles Six and Seven of the ATT call on States to assess the risk of arms being used to commit violence against women and children and deny any arms transfer if there is an overriding risk that the arms may be used to commit or facilitate gender-based violence, finally formalizing the need to address gender in armed conflict. While the ATT marks a step toward progress in the women and arms control space, a lack of accountability mechanisms for States that violate the treaty, as well as the failure of many States to provide their assessed financial contributions for implementation efforts, may be [limiting the agreement's potential](#) to address gender-based violence.

With the adoption of the [Sustainable Development Goals](#) (SDGs) in 2015, the United Nations continued its efforts to address women's participation in disarmament, non-proliferation and arms control, notably through [Goal 5](#) on gender equality and eliminating gender-based violence and [Goal 16](#) on reducing illicit arms trafficking. In 2018, the Secretary-General [reported](#) that some progress had been achieved among Member States in increasing female representation within their disarmament efforts. The United Nations has seen increased funding to the [United Nations Entity for Gender Equality and Empowerment of Women](#). Many countries have reported increased numbers of women in government and armed forces positions. Women increasingly participate in peace negotiations. The Office of Disarmament Affairs also implemented the [Women Scholarship for Peace initiative](#) to train young female professionals on peace, disarmament and non-proliferation, [leading to 170 early career female professionals](#) from the global South receiving scholarships in the program's first year. Despite this progress, [as of 2019](#), women still only account for 32 percent of the

participants at disarmament meetings, and account for 24 percent of delegation heads in the General Assembly First Committee, the Conference on Disarmament and the Non-Proliferation Treaty preparatory committee meetings.

One outstanding issue is the lack of access and resources allocated to address the specific challenges facing women. [Disarmament, demobilization and reintegration](#) (DDR) programs provide support in many forms—including services, cash incentives, healthcare, training, travel remittance, small business grants or housing support—to halt conflict and reintegrate people and groups involved in armed conflict into society at large, contributing toward peace, security and disarmament. One barrier is that women [do not register for DDR programs](#) at a high level. Prevailing gender norms in some countries may prevent women from declaring themselves as members of an armed force out of fear for social stigma. Some DDR programs also [fail to sufficiently address the gender-specific needs](#) of either women and girls or men and boys, and how gender-specific needs fluctuate as gender norms change. Inhibiting access for women and girls to DDR support packages [makes it less likely](#) that they will make it to the negotiation table, and diminishes the likelihood that the economic and physical needs of women affected by armed conflict will be acknowledged, hindering the success of disarmament efforts.

Questions to consider from your country's perspective:

- What steps can the international community take to further implement the Arms Trade Treaty and reduce the risk of arms being used to perpetuate violence against women?
- How can the United Nations and Member States increase women's participation, at all levels, in the field of disarmament?
- How can Member States improve women's access to disarmament, demobilization and reintegration programs? How can DDR programs be more responsive to the gender-specific needs of women?

Bibliography

- [Arms Trade Treaty](#) (2013).

- Bigio, Jamille, and Rachel Vogelstein (2016). [How Women's Participation in Conflict Prevention and Resolution Advances U.S. Interests](#). *Council on Foreign Affairs*.
- [Convention on the Elimination of All Forms of Discrimination Against Women](#) (1979).
- Council on Foreign Relations (2020). [Women's Participation in Peace Processes](#).
- Dwan, Renata (2019). [Women in Arms Control: Time for a Gender Turn?](#) *Arms Control Association*.
- LeGrone, Owen (2019). [ATT Confronts Gender-Based Violence](#). *Arms Control Association*.
- Norwegian Peacebuilding Resource Centre (2016). [Women in Armed Groups and Fighting Forces: Lessons Learned from Gender-Sensitive DDR Programmes](#).
- UN Women (2020). [Facts and Figures: Women, Peace, and Security](#).
- United Nations Development Fund for Women (2004). [Getting it Right, Doing it Right: Gender and Disarmament, Demobilization and Reintegration](#).
- United Nations Institute for Disarmament Research (2021). [Gendered Impacts of Explosive Weapons in Populated Areas](#).
- United Nations Inter-Agency Working Group on Disarmament, Demobilization and Reintegration (2012). [How-to Guide: Gender-Responsive Disarmament, Demobilization and Reintegration](#).
- United Nations Office for Disarmament Affairs (2021). [Small Arms and Light Weapons](#).
- United Nations Office for Disarmament Affairs (2020). [Scholarship for Peace and Security 2020](#).
- United Nations Office for Disarmament Affairs (2016). [Gender Mainstreaming Action Plan](#).
- United Nations Office for Disarmament Affairs (2003). [Gender Mainstreaming Action Plan](#).
- United Nations Peacekeeping (2017). [Disarmament, Demobilization and Reintegration](#).
- United Nations Small Arms Review Conference (2006). [United Nations Conference to Review Progress Made in the Implementation of the](#)

[Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All its Aspects.](#)

[Top ↑](#)

United Nations Documents:

- United Nations, General Assembly (2020). [Women, disarmament, non-proliferation and arms control](#). A/RES/75/48.
- United Nations, General Assembly (2020). [Women, disarmament, non-proliferation and arms control: Report of the Secretary-General](#). A/75/133.
- United Nations, General Assembly (2018). [Women, disarmament, non-proliferation and arms control](#). A/RES/73/46.
- United Nations, General Assembly (2018). [Women, disarmament, non-proliferation and arms control: Report of the Secretary-General](#). A/73/115.
- United Nations, General Assembly (2010). [Women, disarmament, non-proliferation and arms control](#). A/RES/65/69.
- United Nations, Security Council (2004). [Women and peace and security: Report of the Secretary-General](#). S/2004/814.
- United Nations, Security Council (2000). [Women and peace and security](#). S/RES/1325 (2000).