General Assembly First Committee:

Disarmament and International Security Committee (DISEC)

Background Guide

2026-2027

Cleveland Council on WORLD AFFAIRS



General Assembly First Committee: Disarmament and International Security Committee (DISEC) Background Guide

Written by: Marie Chuparkoff, University of Virginia

Written May 2026

The Disarmament and International Security Committee (DISEC), typically referred to as the First Committee, aims to counter international threats to peace, pursue disarmament, and strengthen the international security regime. It was established as the first of six committees of the UN General Assembly by the 1945 UN Charter, and the committee functions under the principles of cooperation in the interest of international peace and security, specializing in disarmament and the regulation of armaments as a means for strengthening stability.[1]

The First Committee reports to two main bodies: the Disarmament Commission (UNDC) and the Conference on Disarmament (CD). Some of the issues these bodies regularly discuss are the following: the cessation of the nuclear arms race; prevention of nuclear war; and regulation of new types of weapons of mass destruction. In addition to disarmament, DISEC addresses a myriad of other issues such as cyberterrorism and state-sponsored cyberwarfare, the trade of conventional arms, and the arms race in outer space. The objective of the First Committee is to promote stability and peace in the international community by responding to threats, from nuclear to cyber weapons, whether originating from state or non-state actors.

Topic I: Preventing State-Sponsored Cyberwarfare

Statement of the Issue:

An evolving form of transnational crime, cybercrime is any criminal act committed in cyberspace. Cyberwarfare is a form of cybercrime, and although it lacks a single agreed upon definition, cyberwarfare is broadly understood as the use of technology to engage in hostile acts in cyberspace against an identified target. According to the UN Office on Drugs and Crime,

[1] UN. "Disarmament and International Security (First Committee)." United Nations: General Assembly of the United Nations. Accessed May 21, 2026. https://www.un.org/en/ga/first/.

cyberwarfare is different from cybercrime because cyberwarfare describes "cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack."[2] A relatively new medium of warfare, cyberwarfare lacks sufficient international regulation, which is further complicated by the lack of a specific standardized definition. Generally, state-sponsored cyberwarfare is any planned or executed cyberattack congruent with the previous definition originating from a foreign government, which either directly or indirectly executes or finances the attack.

States turn to cyberwarfare instead of, or in addition to, conventional military operations because cyberattacks pose significantly fewer risks to the attacking state and can impact systems that are difficult to access through conventional means. It can also be more difficult to identify the perpetrator of a cyberattack. For example, the United States and Israel were allegedly responsible for Stuxnet, a malicious computer worm used to sabotage Iran's uranium enrichment program; cyberwarfare was a more covert and less risky means of preventing Iranian nuclear progress, and compared to conventional military, it was more effective with a computer virus accessing systems a military campaign would not be able to destroy. Another example involves Russia and Ukraine; while Russian cyberaggression began with interference in the 2014 Ukrainian presidential election, Russia's cyberwarfare against Ukraine includes power grid hacks, the paralysis of Ukraine's State Treasury, and the hacking of government websites.

International legal norms governing cyberwarfare are limited. Perpetrators are difficult to hold accountable due to challenges in identifying and attributing attacks, which hinders the application of international norms and laws to cyberwarfare. While state-sponsored cyberwarfare can be associated with targeting another state government, the consequences of these digital attacks are also felt by its citizens. In May 2017, a cybercrime syndicate allegedly sponsored by North Korea perpetrated the WannaCry ransomware cyberattack. The cyberattack spread to more than 200,000 computers across over 150 countries, impacting hospitals, schools, fuel pipelines,

[2] UNODC. "Cyberwarfare." UN Office on Drugs and Crime. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html. Accessed July 6, 2026.

government buildings, and more.[3] Whether actors intend to or not, state-sponsored cyberwarfare wreaks havoc on the lives of innocent civilians.[4]

In 2024, the UN General Assembly adopted the UN Convention against Cybercrime, otherwise known as the Hanoi Convention. Effectively strengthening international cooperation in response to cybercrime, the Hanoi Convention is the first comprehensive global treaty written to address transnational cybercrime. While cyberwarfare was outside the scope of the Hanoi Convention, the Open-Ended Working Group (OEWG), established by DISEC, specializes in constructing norms of responsible state behavior regarding cyberwarfare specifically. The OEWG has agreed on eleven UN cyber norms, including an agreement to "cooperate to increase stability and security in cyberspace," "report ICT vulnerabilities in a responsible manner," and "prevent criminal and terrorist use of information and communications technologies."[5]

The UN Office of Counter-Terrorism (UNCT) has focused specifically on cyberattacks carried about by terrorists; UNCT has launched several initiatives to strengthen law enforcement as well as mitigate the impact of cyberattacks through improvements to defense and recovery systems.[6] Along with UNCT's partnership with organizations like INTERPOL, the UNCT works to strengthen law enforcement by equipping agencies with new technologies, biometric tools, and border screening systems. Despite these advancements in strengthening the international community's cybersecurity as well as affirming UN authority in cyber space, the issue remains of how the UN should identify, punish, and deter state-sponsored perpetrators of cyberattacks.

History:

Cybersecurity was first addressed at the UN in 1998 because of the emergence of malware in the 1980s, but a temporary committee was not established until 2004 when the Group

---

[3] "What Was the WannaCry Ransomware Attack?" Cloud Flare. https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed July 6, 2026.

[4] IMI. "State Sponsored Cyber Warfare." Identity Management Institute, May 9, 2023. https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/.

[5] Hogeveen, Bart. "The UN Cyber Norms." *The Cyber Defense Review*, Fall 2022. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/08_Hogeveen.pdf?ver=BYnHYWAYLrW_PpP4lljm5A%3D%3D.

[6] UN. "Cybersecurity and New Technologies." United Nations: Office of Counter-Terrorism. Accessed May 21, 2026. https://www.un.org/counterterrorism/en/cybersecurity.

of Governmental Experts (GGE) was mandated to advance responsible state behavior in cyberspace in response to international security threats. In 2016, the UN established the OEWG, which operated under a format different from the GGE, albeit pursuing the same objectives. In 2025, the OEWG agreed to establish the UN Global Mechanism, which permanently institutionalized UN discussions on cybersecurity starting in 2026.[7]

As state-sponsored acts of cyberwarfare have increased, the need for global governance of cyber space has grown. In 1986, the first known case of state-sponsored cyberwarfare took place in the form of cyber espionage, when a German hacker targeted computers at US military bases and then sold information to the KGB. Between 1996 and 1998, Moonlight Maze, a grave data breach of classified US government documents by Russian-based cyber-espionage group Turla, brought cyber espionage to the forefront of global politics. In 2010, the United States and Israel allegedly launched a piece of malware known as Stuxnet to obstruct Iranian nuclear weapons progress. Stuxnet exploited the zero-day vulnerabilities of Programmable Logic Controllers, which were used to run and monitor the Iranian uranium enrichment program. Soon after, a hacker sponsored by the Iranian government carried out a similar cyberattack against the Saudi Arabian energy sector. Each of those operations was immensely complex, requiring years of intelligence gathering beforehand.[8]

Citizens have also been targeted through cyberattacks on infrastructure. In 2015 and 2016, following Russian's annexation of Crimea, the Russian government sponsored immense cyberattacks on Ukraine's power grid, which caused widespread blackout and severe economic and social consequences. State-sponsored cyberattacks are relatively low-cost, low-risk ways to harm civilians compared to conventional military means. In 2017, Ukraine was again targeted by NotPetya, the most destructive malware deployed up to that time. NotPetya infiltrated most Ukrainian networks, costing the state $10 billion in damages, and it continued to spread across other European networks. The malware paralyzed global shipping giant Maersk and caused outages and blackouts in 22 banks, six power companies, two airports, four hospitals, and several government agencies across Ukraine. This forced the cancellation of medical procedures, created

---

[7] Rupp, Christina. "The UN's New Global Mechanism on Cybersecurity." Interface, March 6, 2026. https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity.

[8] O'Brien, Dick. "A Short History of Cyber Espionage." Medium, July 27, 2017. https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec.

food shortages, delayed shipping, and prevented citizens from withdrawing cash or using cards from certain banks.[9]

Ukraine is not Russia's only target when it comes to cyberwarfare. In November 2023, Russian hackers targeted 22 Danish power companies to decentralize Denmark's power grid, responsible for the largest cyberattack against Denmark on record. The same year, Iranian hackers similarly targeted infrastructure by launching a cyberattack against Israel's railroad network. Research conducted in 2025 has concluded that between 2023 and 2024 alone, the quantity of cyberattacks in interstate conflicts has increased significantly. In 2024, Russian cyberattacks on Ukraine surged by about 70%, with 4,315 attack targeting critical infrastructure such as government services, power companies, and defense-related entities. Similarly, Chinese cyberattacks on Taiwan doubled between 2023 and 2024, and the number of successful attacks rose by 20%.[10]

State-sponsored cyberwarfare is not novel; rather, it has grown rapidly in global conflicts this past decade. There is still uncertainty of how cyberattacks are regarded under international law, and it is the responsibility of international governments such as the UN to interpret and resolve conflicts related to cyberwarfare. Despite rapid technological advancement alongside surging cyberattack rates in the 21st century, there are still major obstacles to responding to and regulating state-sponsored cyberwarfare as an international community.

Analysis:

There are three primary challenges the UN faces in preventing state-sponsored cyberwarfare: lack of an agreed-upon definition; the problem of attribution; and the offense-defense balance.

While there have been many attempts to define cyberwarfare, no single definition has been agreed that comprehensively describes the issue and how it affects states. The ambiguity

---

[9] "Five Facts to Know About History's Most Destructive Cyberattack." HYPR. https://www.hypr.com/security-encyclopedia/notpetya. Accessed July 6, 2026.

[10] CSIS. "Significant Cyber Incidents." Center for Strategic and International Studies. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed July 6, 2026.

allows states to frame their cyber actions as more positive and socially acceptable on the international stage. For instance, the Russian government developed the term "information warfare" for their own use to describe "mass psychological campaigns against the population of a State in order to destabilize society and the government."[11] This definition describes potential forms of cyberwarfare as more acceptable and less severe with the word "destabilize," which is a much weaker description of the grave harm cyberwarfare may pose to society. "Information warfare" also seems more passive than "cyberwarfare," which would hold a perpetrator of "information warfare" to a lower standard of accountability than a perpetrator of cyberwarfare. Disguising acts of cyberwarfare as mere "information warfare" hinders the international community from reprimanding Russia. The lack of a standard definition also makes the application of international norms and laws to cyber warfare more difficult. Since cyberwarfare is such a broad form of aggression of varying intensities, it can be challenging to identify the appropriate retaliation or the proportionate armed attack to which it could be analogous under international law.

A second issue with state-sponsored cyber warfare is the problem of attribution. Attribution and identification are more difficult with the perpetrators of cyber-attacks than with perpetrators of hostile acts not in cyber space. Even when states are identified as the source of the attack, they often deny affiliation because attribution is hard to prove concretely. This deters states from retaliating because if a state cannot confirm who perpetrated the cyber-attack, it is more difficult to justify retaliation.

The final issue with handling state-sponsored cyberwarfare is the offense-defense balance. When applied to cybersecurity, this term describes the balance between the relative ease of an attack against a proportionately weak defensive system. For example, the United States generally prioritizes cyber offense over defense which has made it more susceptible to cyberattacks. Most scholars agree that cyberspace favors the offense, rendering cyberattacks much easier to commit than defend. One aspect of cyberwarfare that demonstrates the efficacy of an attack is advanced persistent threats (APTs). APTs are highly organized nation-state cyber

[11] The Ministry of Foreign Affairs of the Russian Federation, "Convention on International Information Security," Foreign Policy Fundamental Documents. Accessed May 22, 2026. https://www.mid.ru/en/foreign_policy/official_documents/-/assetpublisher/CptICkB6BZ29/content/id/191666.

actors, as opposed to lone actors, that can gain unauthorized access to a network while undetected for months or years; Stuxnet is a prime example of an APT. Another aspect of cyber warfare that makes cyberattacks so effective is the existence of zero days. A zero day is a software or hardware flaw for which there is no known patch; zero-day vulnerabilities are easily exploitable by both lone hackers and state actors. While zero-day vulnerabilities are relatively rare, their exploitation is highly dangerous and threat intelligence groups regularly track up to a hundred zero-day exploits that are actively used each day.

Within the domain of cybersecurity, there is a great disparity between capabilities of the five biggest government players—United States, China, Russia, North Korea, and Iran—and other countries such as Ukraine or Estonia that, albeit developed, lack the same cybersecurity capabilities to defend themselves or retaliate against attacks.[12] While a major concern is limiting these countries' cyberwarfare capabilities, it is within DISEC's interest to improve and develop cybersecurity for all countries to preserve international peace and stability.

Conclusion:

DISEC, alongside UNCT and other UN bodies, has already made efforts to regulate and prevent state-sponsored cyberwarfare. From the official recognition of cyberspace under the UN Charter, to the establishment of the OEWG which specializes in cybersecurity concerns, DISEC has designated state-sponsored cyberwarfare and its regulation as the UN's responsibility. While DISEC has already laid out a framework for state-sponsored cyberwarfare under international law, there is much more ground to cover regarding the specificity of regulations and the enforcement of international law in cyberspace.

State-sponsored cyberwarfare escalates global conflicts and damages critical infrastructure, worsening standard of living for civilians around the globe. Although it is not treated with the same gravity as physical military action, cyberwarfare has caused irreparable damage to both interstate relations and the many individual lives caught in the global crossfires. Cyberspace, now recognized under the jurisdiction of the UN Charter and International

[12] Nason, Alanna. "What Are State-Sponsored Cyberattacks?" Coro Cybersecurity, January 30, 2024. https://www.coro.net/blog/what-are-state-sponsored-cyberattacks.

Humanitarian Law, is under the authority of DISEC and related bodies, and it is up to this committee to prevent state-sponsored cyberwarfare and inevitably respond to it.

Questions to Consider:

1. How should cyberwarfare be defined under international law? How should it differ from traditional warfare in terms of regulations and repercussions?
2. How can UN bodies prevent and deter future acts of state-sponsored cyberwarfare?
3. How can the global community alter the offense-defense balance of cybersecurity that gives perpetrators such an advantage?

Bibliography

Hogeveen, Bart. “The UN Cyber Norms.” *The Cyber Defense Review*, Fall 2022. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/08_Hogeveen.pdf?ver=BYnHYWAYLrW_PpP4lljm5A%3D%3D.

IMI. “State Sponsored Cyber Warfare.” Identity Management Institute, May 9, 2023. https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/.

The Ministry of Foreign Affairs of the Russian Federation, “Convention on International Information Security,” Foreign Policy Fundamental Documents. Accessed May 22, 2026.

“Moonlight Maze.” Wikipedia, February 16, 2026. https://en.wikipedia.org/wiki/Moonlight_Maze.

Nason, Alanna. “What Are State-Sponsored Cyberattacks?” Coro Cybersecurity, January 30, 2024. https://www.coro.net/blog/what-are-state-sponsored-cyberattacks.

O’Brien, Dick. “A Short History of Cyber Espionage.” Medium, July 27, 2017. https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec.

Ohlin, Jens David. "Did Russian Cyber Interference in the 2016 Election Violate International Law?," 95 Texas Law Review 1579 (2017).

Rosenberger, Laura, and Jamie Fly. “Lessons from France for Fighting Russian Interference in Democracy.” GMF. Accessed May 22, 2026. https://www.gmfus.org/news/lessons-france-fighting-russian-interference-democracy.

Rupp, Christina. “The UN’s New Global Mechanism on Cybersecurity.” Interface, March 6, 2026. https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity.

UN. “Disarmament and International Security (First Committee).” United Nations: General Assembly of the United Nations. Accessed May 21, 2026. https://www.un.org/en/ga/first/.

UN. “Cybersecurity and New Technologies.” United Nations: Office of Counter-Terrorism. Accessed May 21, 2026. https://www.un.org/counterterrorism/en/cybersecurity.

“What Is NotPetya? 5 Fast Facts: Security Encyclopedia.” HYPR, April 28, 2025. https://www.hypr.com/security-encyclopedia/notpetya.

Topic II. Preventing Illicit Trade and Trafficking of Small Arms and Light Weapons

Statement of the Issue:

The illicit trade of small arms and light weapons (SALWs) is a major cause of global conflict, terrorism, and organized crime. Illicit arms trade is the diverting of weapons from national stockpiles to non-state armed groups. It is often used interchangeably with the term illicit arms trafficking, which is the smuggling of illegal arms across borders without the knowledge or consent of the state. The UN's International Tracing Instrument defines small arms and light weapons as "any man-portable lethal weapon that expels or launches, is designed to expel or launch, or may be readily converted to expel or launch a shot, bullet or projectile by the action of an explosive." Small arms include revolvers and self-loading pistols, rifles and carbines, shotguns, sub-machine guns, assault rifles, and light machine guns. Light weapons refer to machine guns, grenade launchers, mortars, and other crew-served shoot explosive munitions.[13]

SALWs significantly drive global violence and instability because of their portability, durability, and low cost. They are easy to replicate and conceal, which is why illegal SALWs are more successfully trafficked compared to larger firearms. According to the Small Arms Survey, there are more than one billion SALWs in the world. Even though the majority of SALWs are in the hands of civilians, small arms are responsible for about a half million deaths every year and are used to facilitate human rights violations and acts of terror among other crimes.[14]

Historically, DISEC has been instrumental in global efforts to reduce the illicit arms trade of SALWs by creating global standards for the tracking and regulating of small arms. Treaties such as the Firearms Protocol and the Arms Trade Treaty have been especially effective in reducing illicit arms trade by constructing regulations and criteria for the exporting of all arms

---

[13] "Small Arms and Light Weapons (SALW)." World Customs Organization. https://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/security-programme/small-arms-and-light-weapons.aspx. Accessed July 6, 2026.

[14] Moses, Mandu. "Small Arms and Light Weapons: Why Do They Matter?" Cedar Mill, September 15, 2023. https://cedarmillfirearms.com/pages/blog/small-arms-and-light-weapons-why-do-they-matter/?srsltid=AfmBOoo1Cnb-UVXng63Q55uBPhbW9_4gFdG65xPyLoXgG5g3up_dC-Ps.

and ammunition. Nevertheless, the circumvention of these preventative measures has still allowed for the trafficking of illegal SALWs, inflaming conflicts in each continent.

History:

In the 16th century, arms became central to warfare, and governments faced conflicting demands. While arms manufacturers were financially successful during wartime, they faced a lack of demand during times of peace. Governments, fearful of the consequences of weapons sales to their own civilians, encouraged gun makers to sell their products abroad. Thus, as early as the 18th century, international trade in SALWs began and continued to grow with increased globalization. By the middle and late 19th century, powerful anticolonial movements emerged, and British officials were unable to prevent British guns from falling into the hands of pro-independence groups in Ireland, India, and elsewhere, significantly increasing the spread of SALWs to non-state actors.[15] Illicit arms trading continued to expand with the fall of the Soviet Union, which led to an immense increase in the supply of weapons flowing from former Soviet stockpiles.[16]

Up until this point, states' primary concern with illicit arms trade was the possibility that manufacturers were indirectly supplying the enemies of their state. However, the rise of terrorist groups in the 1990s made the illicit trade of SALWs even more dangerous. For instance, terrorist attacks in Mumbai in 2008, Paris in 2015, and Sri Lanka in 2019 all involved a combination of small arms and light weapons with assault rifles as well as explosives used.[17]

The first time the UN Security Council (UNSC) addressed the issue of small arms was in 1999 by explicitly recognizing the threat of the proliferation of small arms. In 2001, countries adopted the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small

---

[15]DeLay, Brian, Priya Satia, Ron Hassner, and Daniel Sargent. "Arms Trafficking: Its Past, Present, and Future." American Academy of Arts & Sciences, 2020. https://www.amacad.org/news/arms-trafficking-its-past-present-and-future.

[16] Ivanova, Kate. "Illicit Arms Trade: Analyzing the Unobservable." Mershon Center for International Security Studies, 2011. https://mershoncenter.osu.edu/illicit-arms-trade-analyzing-unobservable.

[17] Spapens Antonius and Nils Duquet. "Terrorists' Acquisition of Firearms and Explosives: Criminal, Legal, and Grey Sources." Tilburg University, February 2022. https://repository.tilburguniversity.edu/server/api/core/bitstreams/aab948a0-a2a2-4278-b0e1-daa57fea5665/content.

Arms and Light Weapons in All Its Aspects. This agreement mandated that state governments "improve national small arms regulations, strengthen stockpile management, ensure that weapons are properly and reliably marked, improve cooperation in weapons tracing, and engage in regional and international cooperation and assistance."[18] In 2005, the General Assembly adopted the International Tracing Instrument (ITI) to improve global cooperation in weapons tracing. In 2013, the UNSC specifically focused on the illicit transfer of small arms with the adoption of Resolution 2117, and two years later, the Council implemented UN arms embargoes to support the Arms Trade Treaty (ATT). The ATT was created to combat illicit arms trade by establishing common standards for international trade in conventional arms; in an effort to reduce armed conflict and violence, the ATT puts prohibitions on types of arms transfers, sets criteria for assessment of exports, and encourages countries to develop and report on their export and import control system.[19] As for SALWs specifically, the UN Coordinating Action on Small Arms acts as the platform for global coordination surrounding legislation of small arms and light weapons. While these treaties successfully establish legally binding global standards, they are largely ineffective due to lack of enforcement, vague criteria, and reliance on self-reporting.

Analysis:

The main danger surrounding illicit arms trade is the ease at which SALWs can be bought by terrorist groups. Most literature supports the claim that terrorist groups are net purchasers of weapons, most often from organized criminal groups (OCGs). Typically, the largest demand for SALWs comes from terrorist groups aimed at territorial control, which they use to defeat state militaries and other groups seeking control. The mass production of SALWs has been realized by "ghost guns," which are 3D-printed small arms without serial numbers. Ghost guns make the illicit arms trade more widespread and accessible, particularly in Western Europe and Latin America, and they are easily smuggled because of their lack of serial numbers.[20]

---

[18] UN. "Small Arms and Light Weapons." United Nations: Office for Disarmament Affairs. Accessed May 27, 2026. https://disarmament.unoda.org/en/our-work/conventional-arms/small-arms-and-light-weapons.

[19] UN. "Arms Trade Treaty." United Nations: Office for Disarmament Affairs. Accessed May 27, 2026. https://disarmament.unoda.org/en/our-work/conventional-arms/legal-instruments/arms-trade-treaty.

[20] Mishru, Vibhu. "Illicit Weapons Fueling Conflicts Worldwide, Officials Warn." UN News, November 10, 2025. https://news.un.org/en/story/2025/11/1166324.

In Haiti, the trafficking of illegal arms, including ghost guns, has empowered Haitian gangs, who now have more firepower than the police. The sniper attacks, mass lootings, kidnappings, and prison breaks, all facilitated by the trafficking of illegal weapons of OCGs, have displaced more than 362,000 Haitians and have exacerbated a growing food crisis.[21] In 2022, the UNSC placed an arms embargo on Haiti tentatively until October of 2026; originally, the embargo only applied to SALWs, but it was updated in 2024 to include arms and related equipment of all types unless they are supplies to the Government of Haiti or a UN-authorized mission. Despite the embargo, there is an estimated 270,000 to 500,000 illegal arms in circulation. Haitian OCGs are circumventing the UN arms embargo through several ways. Well-established trafficking routes from Miami and New York, via the Dominican Republic, are often exploited because of the reportedly weak customs enforcement and corruption. Additionally, there are reports of arms being shipped from South American countries, with Venezuela in particular. To evade inspection, small arms are usually hidden with mixed cargo or declared as humanitarian or commercial goods. Additionally, some assault rifles belonging to private security companies based in Haiti are also ending up in the hands of Haitian gangs. Some ways the embargo could be strengthened are optimizing Haiti's capacity to detect and investigate illicit arms as well as improving maritime and port security.[22]

In Europe, there are major links between OCGs and terrorist groups. Cooperation between the Italian Mafia and ISIS groups involve trafficking illegal arms as well as cultural goods; there is evidence that the Italian Mafia sells rifles to ISIS leaders in Libya in exchange for archeological artefacts. The Italian Mafia, working with Camorra, one of Italy's oldest OCGs, also purchases SALWs such as rifles and grenade launchers smuggled out of Ukraine and Moldova by the Russian Mafia.[23] Regarding terrorism, SALWs are the third most frequently used weapon in terrorist attacks (after larger explosives and incendiary devices). According to a study conducted by Tessler and colleagues, in the United States, Canada, European countries,

---

[21] UN. "Haiti: Gangs Have 'More Firepower than the Police.'" United Nations: Office on Drugs and Crime. Accessed May 28, 2026. https://www.unodc.org/unodc/frontpage/2024/April/haiti_-gangs-have-more-firepower-than-the-police.html.

[22] Dickinson, Daniel. "Haiti Is under a UN Arms Embargo: So Why Are 500,000 Illegal Weapons in Circulation? | UN News." UN News, October 17, 2025. https://news.un.org/en/story/2025/10/1166121.

[23] UN. "Firearms Module 7 Key Issues: Interconnections between organized criminal groups and terrorist groups in relation to firearms trafficking." Sharing Electronic Resources and Laws on Crime. Accessed May 28, 2026. https://www.unodc.org/cld/en/education/tertiary/firearms/module-7/key-issues/terrorist-groups.html.

Australia, and New Zealand from 2002 to 2016, even though arms, mostly SALWs, account for 10% of terrorist attacks in the given timeframe, they account for about 55% of the fatalities as well.[24] Not only are SALWs a direct method to effectively cause harm, but they can also be used to facilitate main attacks by terrorist groups; kidnappings, drug trafficking, and attacks against military personnel are a few examples of main attacks that use SALWs to facilitate and enable their execution.[25] In South America, the Peruvian terrorist organization Sendero Luminoso similarly benefits from illicit arms trade.[26] One of their weapons of choice is the *tiracha*, or homemade gun, which is more difficult for law enforcement to track than manufactured firearms. In Northern Africa, the illicit arms trade has empowered terrorist groups such as Boko Haram through the recirculation of SALWs after wars have ended. Following the collapse of Libya in 2011, massive stockpiles of SALWs were similarly looted and diverted to arm insurgent factions and terrorist organizations.

Along with supplying terrorist organizations, the trafficking of illegal SALWs exacerbates ongoing political conflict. In Sudan, illicit arms trade has fueled and perpetuated the conflict between the Sudanese Armed Forces and the Rapid Support Forces, worsening the civil war and humanitarian crisis. Even though the UN placed an arms embargo on the Darfur region of Sudan in 2004, the embargo has remained inadequate and does not cover the entirety of Sudan. There are weapons from Russia, Serbia, Turkey, the United Arab Emirates, and Yemen being imported in large quantities to Sudan and then transferred to Darfur, effectively evading Darfur's arms embargo.[27] In Colombia, the Revolutionary Armed Forces of Colombia have trafficked illegal SALWs in addition to producing their own weapons in illegal factories both in Colombia and abroad. Another creative problem regarding the circulation of illegal arms is deactivated weapons, which can be sold for use as film and theatre props and face fewer restrictions with a lack of common EU rules. These are easily bought and are more difficult to

---

[24] Tessler RA, Mooney SJ, Witt CE, et al. Use of Firearms in Terrorist Attacks: Differences Between the United States, Canada, Europe, Australia, and New Zealand. *JAMA Intern Med.* 2017;177(12):1865–1868. doi:10.1001/jamainternmed.2017.5723.

[25] UN. "Firearms Module 7 Key Issues: Terrorist Groups." Sharing Electronic Resources and Laws on Crime. Accessed May 28, 2026. https://www.unodc.org/cld/en/education/tertiary/firearms/module-7/key-issues/terrorist-groups.html.

[26] McCormick, Gordon. "The Shining Path and Peruvian Terrorism." Santa Monica, CA: RAND Corporation, 1987. https://www.rand.org/pubs/papers/P7297.html.

[27] "Sudan: Constant Flow of Arms Fuelling Relentless Civilian Suffering in Conflict – New Investigation." Amnesty International, July 26, 2024. https://www.amnesty.org/en/latest/news/2024/07/sudan-constant-flow-of-arms-fuelling-relentless-civilian-suffering-in-conflict-new-investigation/.

trace due to a lack of standard regulations. The illicit trade of deactivated weapons poses a problem for European states and can easily diffuse the problem across the entire continent.

Conclusion:

The illicit trade and trafficking of SALWs have been detrimental to countries all over the globe—most dangerous because of their benefiting terrorist groups and OCGs alike. The UN has worked to reduce the circulation of illegal arms through actions such as the establishment of arms embargoes, encouragement of gun registration and tracking, and setting of global criteria for assessments of imports. However, non-state actors have still been able to circumvent these regulations and purchase hundreds of thousands of illegal SALWs.

Although the illicit arms trade originated to support countries' gun manufacturing industries, it now empowers enemies and enables more military conflict. Similarly, the trafficking of illegal arms has fueled global conflicts, from civil wars to acts of terrorism. SALWs, although used in about 10% of terrorist attacks in the Western world, are responsible for about half of all fatalities caused by terrorism. Illicit arms trade and trafficking supply terrorists and other non-state actors, sparking new conflicts and adding fuel to the fire of ongoing ones. It is the First Committee's responsibility to work with other UN bodies such as the UNODC and UNSC to prevent illicit arms trade and trafficking either by strengthening actions already taken or finding new ways to address the burgeoning issue.

Questions to Consider:

1. How can the UN address non-traditional elements of illicit arms trafficking such as the circulation of ghost guns and deactivated weapons?
2. How can the UN strengthen arms embargoes and/or prevention non-state actors from circumventing them in the interest of your country's regional stability?
3. How can the UN reduce collaboration between OCGs and terrorist groups?

Bibliography

DeLay, Brian, Priya Satia, Ron Hassner, and Daniel Sargent. “Arms Trafficking: Its Past, Present, and Future.” American Academy of Arts & Sciences, 2020. https://www.amacad.org/news/arms-trafficking-its-past-present-and-future.

Dickinson, Daniel. “Haiti Is under a UN Arms Embargo: So Why Are 500,000 Illegal Weapons in Circulation? | UN News.” UN News, October 17, 2025. https://news.un.org/en/story/2025/10/1166121.

Ivanova, Kate. “Illicit Arms Trade: Analyzing the Unobservable.” Mershon Center for International Security Studies, 2011. https://mershoncenter.osu.edu/illicit-arms-trade-analyzing-unobservable.

McCormick, Gordon. “The Shining Path and Peruvian Terrorism.” Santa Monica, CA: RAND Corporation, 1987. https://www.rand.org/pubs/papers/P7297.html.

Mishru, Vibhu. “Illicit Weapons Fueling Conflicts Worldwide, Officials Warn.” UN News, November 10, 2025. https://news.un.org/en/story/2025/11/1166324.

Moses, Mandu. “Small Arms and Light Weapons: Why Do They Matter?” Cedar Mill, September 15, 2023. https://cedarmillfirearms.com/pages/blog/small-arms-and-light-weapons-why-do-they-matter/?srsltid=AfmBOoo1Cnb-UVXng63Q55uBPhbW9_4gFdG65xPyLoXgG5g3up_dC-Ps.

Spapens Antonius and Nils Duquet. “Terrorists’ Acquisition of Firearms and Explosives: Criminal, Legal, and Grey Sources.” Tilburg University, February 2022. https://repository.tilburguniversity.edu/server/api/core/bitstreams/aab948a0-a2a2-4278-b0e1-daa57fea5665/content.

“Small Arms and Light Weapons (SALW).” World Customs Organization. https://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/security-programme/small-arms-and-light-weapons.aspx. Accessed July 6, 2026.

“Sudan: Constant Flow of Arms Fuelling Relentless Civilian Suffering in Conflict – New Investigation.” Amnesty International, July 26, 2024. https://www.amnesty.org/en/latest/news/2024/07/sudan-constant-flow-of-arms-fuelling-relentless-civilian-suffering-in-conflict-new-investigation/.

Tessler RA, Mooney SJ, Witt CE, et al. Use of Firearms in Terrorist Attacks: Differences Between the United States, Canada, Europe, Australia, and New Zealand. *JAMA Intern Med.* 2017;177(12):1865–1868. doi:10.1001/jamainternmed.2017.5723.

UN. "Arms Trade Treaty." United Nations: Office for Disarmament Affairs. Accessed May 27, 2026. https://disarmament.unoda.org/en/our-work/conventional-arms/legal-instruments/arms-trade-treaty.

UN. "Haiti: Gangs Have 'More Firepower than the Police.'" United Nations: Office on Drugs and Crime. Accessed May 28, 2026. https://www.unodc.org/unodc/frontpage/2024/April/haiti_-gangs-have-more-firepower-than-the-police.html.

UN. "Firearms Module 7 Key Issues: Interconnections between organized criminal groups and terrorist groups in relation to firearms trafficking." Sharing Electronic Resources and Laws on Crime. Accessed May 28, 2026. https://www.unodc.org/cld/en/education/tertiary/firearms/module-7/key-issues/terrorist-groups.html.

UN. "Firearms Module 7 Key Issues: Terrorist Groups." Sharing Electronic Resources and Laws on Crime. Accessed May 28, 2026. https://www.unodc.org/cld/en/education/tertiary/firearms/module-7/key-issues/terrorist-groups.html.

UN. "Small Arms and Light Weapons." United Nations: Office for Disarmament Affairs. Accessed May 27, 2026. https://disarmament.unoda.org/en/our-work/conventional-arms/small-arms-and-light-weapons.