Code: GA/1/1
Committee: General Assembly First Committee
Topic: The Role of Information and Communication Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Affirming the work of the offices concerned with the illicit trade of arms, such as the United Nations Office on Drugs and Crime (UNODC) with their Monitoring Illicit Arms Flows Initiative, and the United Nations Office for Disarmament Affairs (UNODA),

Deeply concerned about the illegal seizure of legally-produced arms by criminal actors for their illicit purposes, with said legally produced arms finding themselves being traded in the dark web,

Recognizing the pre-existing framework concerning the tracing of and registry of arms under the International Tracing Instrument (ITI) and the United Nations Register of Conventional Arms (UNROCA),

Calling attention to the absence of a consolidated framework or set of international norms towards addressing the illicit trade of arms over the internet, as encouraged under the Sustainable Development Goals (SDGs) for 2030 to create international collaboration between Member States for a better world,

Aware of the recent growth of private military companies, consultants, and trainers who provide and deliver military services and supplies, as noted by the UNODC,

Realizing the importance of the *Programme of Action to Prevent, Combat, and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects* (PoA SALW),

Having considered the specific and different educational needs of each country and their current knowledge of the internet and media,

Noting the *Arms Trade Treaty* (ATT) (2013) and the *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition supplementing the Convention against Transnational Organized Crime* (Firearms Protocol) (2001) and their emphasis on preventing the illicit trade of arms globally, regulating the international trade of conventional weapons, and discouraging weapons sales to malicious actors, such as terrorist groups and organized crime actors, in order to protect international security and defend against crime and terror,

Bearing in mind feminist foreign policies and that, in line with General Assembly resolution 65/69 (2010) on “Women, disarmament, nonproliferation, and arms control,” the implementation of women in the disarmament and arms control process continues to have positive effects in strengthening the arms control infrastructure, contributes to lower numbers of arms in circulation, and advances the goal of international peace, to solution strategies that have positive effects in strengthening arms control and advocate international peace,

Believing in the role of efficient firearms tracing systems like the eTrace System employed by the United States of America in providing critical data for law enforcement agencies, aiding in the prevention of firearms tracking and related criminal activities,

Guided by the “Panel Discussion on Digital, Media, and Information Literacy” held by the Office of the United Nations, recognizing the importance of digital literacy globally for citizen safety and security, and of inclusive and accessible educational programs to empower individuals, bridge societal gaps, and enhance international cooperation,

Stressing the need to reinforce and enhance existing national infrastructures to effectively address evolving challenges and to promote global stability,

Keeping in mind the need for fostering inclusive and effective partnerships with non-governmental organizations (NGOs),

Fully aware of the cruciality of the *2030 Agenda for Sustainable Development* (2030 Agenda) and the Sustainable Development Goals 3 (Good health and well-being), 5 (Gender equality), and 16 (Peace, justice, and strong institutions), in combating the illicit trade and proliferation of arms, maintaining safe and secure information and communication technologies (ICT) usage, and uplifting ICT infrastructure,

Deeply concerned with the negative impacts of the illicit trade of arms on society, such as deaths, injuries, and psychological harm, as shown by Security Council resolution 2117 (2013) on “Small arms and light weapons,” and Security Council resolution 2220 (2015) on “Small arms”,

Guided by the Global Education Monitoring (GEM) Report, published annually by the United Nations Educational, Scientific. and Cultural Organization (UNESCO), which assesses progress toward global education as well as targets and identifies gaps and challenges,

Emphasizing efforts that are made to enhance the quality of teaching and teacher training programs worldwide using information from the United Nations Office of Counter-Terrorism (UNOCT) to specialize the education on ICTs and their role in the illicit trade of arms,

Reaffirming Education for Sustainable Development, as promoted by UNESCO through education that fosters sustainable development, helping individuals acquire the knowledge, skills, attitudes, and values necessary to shape a sustainable future,

Recognizing the importance of regulating the international trade of legal conventional weapons and how ICTs contribute to increased illicit arms trade and exacerbate the issue further,

Emphasizing the benefit of working in line with Security Council resolution 2616 (2016) on “Maintenance of international peace and security,” which recognizes that the illicit trade of arms endangers Member States' security and the safety of civilians as it intensifies crime and terror, and Security Council resolution 2370 (2017) on “Preventing terrorists from acquiring weapons,” which discusses collaboration between Member States to interrupt the online supply of weapons to terrorist groups,

Having considered small Member States’ and least-developed countries’ (LDCs) demand for global cooperation in funding technological and cybersecurity education,

1. *Recommends* a partnership between the UNODC and the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE) under the UNODA in order to:

a. Research and examine ICTs by identifying gaps in current frameworks and ways to leverage ICTs;

b. Use the findings of civil society organizations on emerging trends and technologies used within the online illicit trade of arms to develop strategies for such establishments;

c. Revise the Illicit Arms Flows Questionnaire (IAFQ) to include SALW, developed by Member States, intergovernmental organizations (IGOs), and experts in the field;

2. *Encourages* the implementation of the GGE to spread cybersecurity to all Member States and prevent the effects of cybercrime globally, as well as foster the collaboration of all Member States in this effort by:

    a. Directing the Open-ended Working Group on security and use of ICTs (OEWG) to research the setting of a global cybersecurity standard to prevent the further spread of the illicit trade of arms and cybercrime, allowing for inter-operability;

    b. Stimulating the sharing of cybersecurity methods and technology for a more coherent, unified, and stronger cyberspace;

    c. Following data protection regulations to prevent leakage of sensitive information;

    d. Further encouraging Member States to continue to deliver annual reports on their implementation of the PoA SALW;

    e. Encouraging Member States to consider increasing security assets in ports and logistical hubs and the examination manifests as well as using cyber-based safeguards to prevent system compromise;

    f. Reminding that the program will target the dark web and trade of illicit arms and will be an expansion of the already existing educational program GEM, with the appropriate funding from UNESCO;

    g. Sharing the use of ideas regarding education on cyberattacks, cyberwar crimes, cyber trade and the dark web;

3. *Encourages* Member States to uphold and reinforce existing frameworks for the tracing of weapons and international databases for information sharing on SALW, while still respecting the national sovereignty of Member States, by:

    a. Increasing involvement in capacity-building efforts to improve the marking and tracing of weapons using the ITI to negate the diversion of weapons from official channels to non-state actors to work to prevent any further illicit arms trading;

    b. Expanding the pre-existing UNROCA database to include illicit weapons from tracing efforts for the purpose of sharing intelligence on transnational crime while incorporating techniques from the Stockholm International Peace Research Institute (SIPRI) and the Illicit Arms Records and Tracing Management System (iARMS) by implementing various

technologies, including but not limited to blockchain verification, artificial intelligence, and machine learning;

c. Considering implementation of various technologies including but not limited to blockchain verification, artificial intelligence, and machine learning;

4. *Welcomes* the implementation of policy reform and collaboration between Member States to prevent the illicit trafficking of arms and weapons, such as:

    a. Increasing border control, and monitoring crossings and shipments through the use of x-ray scanners and drones;

    b. Sharing databases between Member States to facilitate reforms;

5. *Encourages* member states to commit to a shared security standard in the implementation of their ICT infrastructure in order to:

    a. Deter and limit the effectiveness of illicit arms trafficking operations and planning through Member State ICT capabilities;

    b. Enhance cooperation between Member States in developing and fulfilling ICT security protocols;

6. *Emphasizes* the need for communication of educational programs by:

    a. Focusing on early-age education;

    b. Funding provided by the United Nations Children's Fund (UNICEF);

7. *Strongly encourages* the establishment of country-specific assessments to identify the distinct educational needs and levels of internet literacy in each Member State by utilizing existing data such as literacy rates, highest education levels, and standardized test scores if available;

8. *Invites* Member States to develop tailored educational strategies that consider the unique challenges and opportunities within their borders, with a particular emphasis on addressing existing gaps in internet literacy;

9. *Strongly advises* all Member States to invest in educational programs promoting internet literacy with the aid of UNESCO and UNICEF, to provide training and employment opportunities for teachers involved in academic initiatives aimed at improving media knowledge by:

    a. Encouraging Member States to participate in the Education for Justice initiative led by the UNODC;

    b. Additionally endorsing Member States' engagement with the World Wide Web Foundation to integrate their expertise into national educational programs;

    c. Providing equitable access to the internet for rural and marginalized groups;

d. Establishing of online, accessible, and free computer science education;

e. Teaching safe internet practices;

10. *Considers* an additive virtual program through UNESCO, educating young minds on the dangers of illicit trade of arms, preventing the participation of such illegal activities in future generations through the inclusion of a large scope of topics stemming from operations off the dark web using insights from the UNOCT regarding the trading of illicit arms through illegal platforms, and the societal consequences of these illegal trades;

11. *Encourages* Member States to increase knowledge of digital skills through funding from UNESCO by:

    a. Emphasizing education on cybersecurity so that members of the public are able to respond to cyber incidents;

    b. Bringing more ICT specialists to their labor markets;

12. *Emphasizes* the importance of the need for Member States to adopt and adhere to the ATT and the Firearms Protocol;

13. *Reaffirms* the essentiality of ensuring that legal arms are marked for tracing, kept on record, tracked through the process of transfer, and the risk of transfer is assessed by:

    a. Encouraging Member States to implement the PoA SALW in all Member States;

    b. Making use of its supplementary ITI in order to bolster the legality and safety of arms transfers and ensure transparency of the status of arms in circulation internationally.

Code: GA1/1/2
Committee: General Assembly First Committee
Topic: The Role of Information and Communication Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Taking note of the devastating effects of the illegal arms trade, including stalling the process of achieving Sustainable Development Goal (SDG) 3 (Good Health and Well-being), SDG 5 (Gender Equality), SDG 16 (Peace, Justice, and Strong Institutions), and SDG 17 (Partnerships for the Goals),

Restating the importance of international standards on small arms and light weapons (SALW) that the United Nations has implemented, such as disarmament, demobilization, safety and security, trade of weapons, and curbing illicit trade, all done through collaboration with other organizations that also have implemented educational workshops,

Affirms that vulnerable populations, often in Member States lacking well-developed Information Communications and Technology (ICT) frameworks, benefit from strategic communication campaigns that deter participation in the illicit trade of arms with the support of the United Nations Department of Global Communications within the Office of Counter-Terrorism,

Recognizing the critical role that global law enforcement organizations and personnel play in the maintenance of international security,

Considering the transformative potential of emerging technologies, like blockchain and crypto-currencies, and the need to recognize their significance in preventing and detecting illicit trades as outlined in Security Council resolution 2117 (2013) on “Small arms and light weapons”,

Recalling General Assembly resolution 74/247 adopted in 2019 on “Countering the use of information and communications technologies for criminal purposes, which suggests a new treaty on cybercrime”,

Acknowledging advancements in ICTs, specifically artificial intelligence (AI), and the continued progress needed to be made in both developed and developing countries,

Understanding the Illicit Arms Transfers Database (IATD) is an ever-evolving source of information that can be used to great benefit,

Bearing in mind the International Tracing Instrument (ITI) to ensure that all weapons are properly marked and traced,

Recalling Security Council resolution 2616 (2021) on “Maintaining international peace and security,” which emphasizes the critical importance of countering the diversion of arms, as well as their illicit transfer and their destabilizing accumulation for the maintenance of international peace and security,

Recognizing the importance of the creation of initiatives that tackle cyber threats and cybercrimes as they relate to arms trafficking,

Having reviewed United Nations Institute for Disarmament Research and United Nations Office of Drugs and Crime (UNODC) 2022 reports that highlight that conflict increases the demand for illicit arms in a

population, thereby increasing state fragility and providing opportunities for the diversion of arms to the illicit market, including through and to criminal groups,

1. *Recommends* the expansion of existing regional forums to include the public and non-governmental organizations in order to facilitate cooperation among Member States to raise awareness of threats related to the security and use of ICTs:

    a. Extending to local communities, and especially to vulnerable and developing populations to increase cybersecurity literacy and awareness of developments in ICTs, and a special focus on SDGs 3, 15, and 16;

    b. Including Member State collaboration to incorporate resources and information centralized into the Universal Basic Education framework and monitored in partnership with the United Nations Development Programme (UNDP), to promote information sharing that addresses the following:

    c. Extending learning mechanisms to local populations about ICT development and processing information accurately from a civilian perspective by knowing the goals of the government in which they reside;

    d. Including education on the dangers of the dark web and tactics on how to avoid its misuse;

2. *Encourages* the creation of a regional capacity-building program under UNODC in collaboration with expert organizations, relevant working groups, and other UN bodies to provide workshops to local leaders on how to responsibly use ICTs by:

    a. Stressing the need for human resource capacity development to prevent global cybersecurity attacks and threats;

    b. Sharing best practices relevant to the maintenance of regional peace and stability by preventing the dissemination of SALWs in global markets;

3. *Proposes* that the Office of Disarmament Affairs, UNDP and, SDG-Education 2030 Steering Committee jointly develop a comprehensive, encompassing curriculum cognizant of Member States' individual needs with the intention of promoting resilience against violent extremism and conflict resulting in the illicit trade of arms, preventing misuse of ICTs, and advancing worldwide digital literacy;

4. *Encourages* Member State collaboration with non-governmental organizations and the United Nations Children's Fund, to amplify voices of those victimized by online recruitment to violent groups, in order to prevent and discourage participation in illicit activities by:

    a. Working with third-party social media management platform companies to create campaigns with maximum impact;

    b. Publishing multimedia content, including but not limited to factsheets, infographics, videos;

5. *Calls upon* the UN Secretary-General to issue a report outlining recommendations for the formation of collaborative task forces involving International Criminal Police Organization (INTERPOL) and relevant UN bodies, particularly the First Committee, on the topic of the use of ICTs in the illicit trade of arms;

6. *Encourages* Member States to unite in facilitating the sharing of knowledge on cybersecurity and advocating for robust training and education programs for law enforcement and security personnel to enhance their collective capabilities in combating cyber threats associated with the illicit arms trade;

7. *Recommends* the sharing of capacity and knowledge across Member States on a voluntary basis in regard to law enforcement training, focusing on cybercrime prevention, digital forensics, and the identification of illicit arms transactions facilitated by emerging technologies;

8. *Emphasizes* the significance of promoting awareness regarding emerging technologies, like blockchain and crypto-currencies, and urges Member States to incorporate educational camps and training programs to empower relevant stakeholders, including civilians, law enforcement and security personnel, and policymakers, with the necessary knowledge to tackle the changing landscape of the illicit arms trade;

9. *Encourages* partnerships between Member States and public technology companies to increase international cooperation between private media-based entities and UN entities to monitor the illicit trade of arms through online platforms, with attention to:

    a. Such companies like the Meta social media (Instagram and Facebook), which partake in international programs in which they develop cybersecurity, including regulating the spread of trading 3-D blueprints of weapons throughout the dark web;

    b. Efficient communication between borders and maintaining a better understanding of what illegal weapons are being traded (smuggling through countries or from the use of the internet);

    c. Strengthening cooperation between law enforcement agencies and international organizations, such as UNODC and INTERPOL, to combat the illicit arms trade;

    d. Engaging with civil society organizations and private sector partners to leverage their expertise and resources in combating the illicit trade of arms;

10. *Suggests* collaboration between Member States to create a global cyber task force, enhancing international cooperation, building trust between Member States by sharing information and technology with customs agencies and border control, and ceasing the spread of small arms and explosives across international borders, via:

    a. The creation of software that monitors borders and transport between countries;

    b. Funding from the International Monetary Fund (IMF) and other capable bodies;

    c. Encouragement of Member States to utilize and share informants found through cyber-baiting to collect demographic information and inform Member States who are most at risk with illicit arms trading such as fake arms websites on the dark web;

11. *Encourages* Member States to use ICTs to fight ICTs and utilize AI technologies to enhance education platforms and accurately track and analyze where weapons, and the materials used to make such weapons, are at any given moment;

12. *Further encourages* cooperation and enhanced transparency to form a database on the trade of illicit arms to ensure that all Member States have access to information required to stop and prosecute the illicit trade in arms;

13. *Recommends* that Member States, especially developing Member States, utilize information exchange platforms to facilitate real-time sharing of intelligence and best practices among Member States and to enhance international cooperation in combating illicit arms trade, in line with previous action by the international community;

14. *Further recommends* improving the PoA SALW and the ITI as well as encouraging the IMF to finance meaningful efforts;

15. *Suggests* that Member States support global initiatives aimed at addressing the challenges posed by the illicit arms trade and enhancing cybersecurity measures, which could include:

    a. Resource allocation, information sharing, and technology transfer, particularly from developed, economically advanced states;

    b. The creation of an expert group to conduct studies and research on preventing accessibility to confidential information;

16. *Promotes* the building upon the ITI to focus on mitigating cyber threats related to arms trafficking through international cooperation and advanced cybersecurity measures with support from:

    a. The IMF to dedicate funding;

    b. The UNODC and Member States.

Code: GA1/1/3
Committee: General Assembly First Committee
Topic: The Role of Information and Communications Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Alarmed with the violence and concerns that the illicit trade of arms creates, resulting in an estimated 200,000 deaths globally each year between 2010-2015, according to Security Council Meeting Coverage SC/14098 (2020),

Deeply concerned by the detrimental impacts of corruption within law enforcement agencies, which exacerbates the challenges in effectively addressing the illicit trade of arms facilitated by Information and Communication Technologies (ICT),

Noting with regret the augmentation of illicit arms trafficking by ICTs through the use of digital transaction technologies, as criminal organizations laundered over 1.6 billion USD in 2021 globally with the assistance of ICTs to fund their operations through these untraceable transactions,

Bearing in mind the need to implement and fund new technology in providing new tools and increase productivity between Member States while also achieving the committee's goal of Sustainable Development Goal (SDG) 8 (Decent work and economic growth),

Aware of the major role of information and technologies in the security of all Member States, as they can facilitate the operations of illicit arms trade groups in all Member States,

Recognizing that building trust is a necessity in maintaining transparent arms transfers between Member States,

Acknowledging the significant challenges faced by inadequately trained law enforcement officials in countering the sophisticated use of ICTs for the illicit trade of arms and properly handling illegally seized arms,

Reaffirming the need for internationally accessible language referring to the responsible implementation of ICTs,

Recognizing Member States' concerns regarding cybersecurity internationally while also keeping in mind that the illicit trading of arms is more susceptible to occur through commonly used and shared borders,

Endorsing the work of the Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime towards developing an international convention on countering the use of ICTs for criminal purposes,

Fully aware of the UN Ad Hoc Committee's efforts to pass a Global Cybercrime Treaty, whose important efforts should be observed,

Emphasizing its commitment to working with Member States to strengthen international cooperation and to welcome globally interconnected networks to combat the illicit trade of arms,

Understanding the gravity of an unregulated and ever-evolving illegal arms market,

Referencing Security Council resolution 2462 (2019) on “Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism,” and Security Council resolution 2482 (2019) on “Threats to international peace and security,” which concern the involvement of the International Criminal Police Organization (INTERPOL) in anti-weapons trafficking efforts,

Observing the Global Program against Money Laundering, which emphasizes the importance of international cooperation in combating illicit flows, which often fund illegal arms trade,

Deeply concerned by the necessity to regulate and monitor access to illicit internet portals,

Contemplating the need to have a sense of collaboration between all Member States concerning ICTs, developing an intense and intricate network to safeguard cybersecurity and approve new strict laws,

Observing the need to implement heightened security for Member States’ citizens,

Encouraged by the effectiveness and broad acceptance of the *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition supplementing the Convention against Transnational Organized Crime* (Firearms Protocol) (2001), International Tracing Instrument (ITI), and *Programme of Action to Prevent, Combat, and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects* (PoA SALW),

Guided by SDG 8 by working towards implementing, funding, and providing new technological tools to increase productivity between Member States in order to achieve increased levels of economic productivity and technological innovation,

1. *Calls for* the United Nations Development Program to build upon the ITI by creating an international database that tracks the imports and exports of SALW to combat the illicit arms trade, by:
    a. Urging ICT-capable Member States to advise and assist less ICT-capable Member States in the implementation of a database, security standards, and infrastructure;
    b. Advocating for the importance of information sharing and transparency in arms control efforts to the United Nations Office for Disarmament Affairs (UNODA), through the increased monitoring of the import and export of arms across Member States’ borders;
    c. Suggesting the economic and educational efforts required for the database’s construction to be advanced and promoted by Member States with ICT experience;
    d. Utilizing blockchain technology, streamlining information sharing between Member States regarding the exchange of cryptocurrencies;
2. *Further requests* that Member States participate in their implementation of the aforementioned database by:
    a. Sharing its use to Member States internationally by providing access to all Member States who choose to partake in the database;
    b. Facilitating transparency between all Member States using the collaborative database, reporting consistently to the UNODA;

3. *Recommends* the structural expansion of the INTERPOL and the United Nations Office on Drugs and Crime (UNODC) joint Operation Trigger programs by:

    a. Mobilizing INTERPOL's efforts as a non-UN entity with regard to weapons trafficking;

    b. Providing additional training services (i.e., courses) for the government officials of Member States;

4. *Calls upon* the Secretary-General to outline a report on collaboration between INTERPOL and the General Assembly First Committee regarding the illicit trade of arms;

5. *Suggests* a report by the UNODA every five years that surveys and voluntarily evaluates a country on its cybersecurity between Member States, rating their cybersecurity strength based on the following:

    a. Levels of preparedness;

    b. Unidentified devices on internal networks;

    c. Intrusion attempts on networks;

    d. Security incidents;

    e. The average time to detect, contain, and resolve cyberattacks;

6. *Further requests* that the United Nations Office of Outer Space Affairs coordinates and reaches an agreement with the private sector to implement new data matrix codes, radio frequencies, and biometrics to fund new technologies for state authorities;

7. *Requests* that the ITI increases the promotion of intelligence-sharing between Member States, specifically regarding the sale of used weapons that occur between Member States and outside groups by:

    a. Advocating for Member State disclosure of sales of previously used weapons;

    b. Encouraging a decrease in sales of used weapons to non-member states to prevent illicit organizations from obtaining weapons;

8. *Endorses* the expansion of the PoA SALW to add increased emphasis on used weapons sales between Member States and outside groups;

9. *Calls upon* Member States to enhance the capabilities of their law enforcement and security personnel in addressing the cybersecurity and enforcement challenges associated with firearms trafficking through measures such as:

    a. Exploring the development and implementation of a standardized curriculum for law enforcement training on topics such as cybercrime prevention, digital forensics, and digital techniques for identifying illicit arms transactions facilitated by emerging technologies;

    b. Encouraging collaboration with INTERPOL's resources and expertise in developing and disseminating best practices in cybersecurity and digital investigation techniques;

c. Considering the development and adoption of clear guidelines and protocols based on best practices for the secure management of seized weapons;

d. Suggesting the utilization of the UNODC's Global eLearning platform, which offers training on various aspects of international security threats such as cybercrime, firearms trafficking, intelligence analysis, and border control;

10. *Encourages* Member States to utilize anti-corruption measures within law enforcement, suggesting disciplinary practices against corrupt practices and promoting transparency and accountability in arms trafficking investigations and enforcement;

11. *Welcomes* the cooperation of non-governmental organizations and government authorities to find solutions that regulate the possession, trade, and use of SALW;

12. *Reaffirms* the need for governmental protocols regarding the illegal trafficking of arms between Member States' borders, as well as facilitation of cooperation between government agencies concerned with the issue of the illicit trade of arms;

13. *Encourages* the UNODC and the open-ended Working Group on Firearms and the Use of ICTs 2021-2025 to establish a standardized common language between all Member States in combating and tracking the arms trade in order to properly define and trace arms and illicit arms to consistently evaluate and transform dialogue surrounding the Firearms Protocol to ensure the compliance of all Member States.

Code: GA1/1/4
Committee: General Assembly First Committee
Topic: The Role of Information and Communication Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Emphasizing the importance of the International Criminal Police Organization (INTERPOL), consisting of an information trade of statistics regarding illicit arms, a cutting-edge instrument that makes it easier for law enforcement organizations to collaborate on investigations and share information regarding the international trafficking of illegal guns known as the Illicit Arms Records and Tracing Management System (iArms),

Finding that the United Nations Office of Drugs and Crime (UNODC) aims at strengthening the capacity of Member States in arms tracing through the program that focuses on the development of databases and tools to enhance the tracing of illicit arms, and develop technical assistance tools for the daily collection and analysis of illicit trafficking flow, as discussed in the Conference of Parties to the United Nations Convention against Transnational Organized Crime and the Protocols,

Acknowledging the United Nations *Programme of Action on Small Arms and Light Weapons* (PoA SALW), its subprograms like the “Cyber PoA” based on General Assembly resolution on “Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security” and the adopted International Tracing Instrument (ITI), which assist on arms tracing, providing a framework of information on the identified traded illicit arms,

Observing that the relevant authorities such the United Nations institute of Disarmament Affairs, the United Nations Office of Counter-Terrorism, and the United Nations Office on Drugs and Crime (UNODC),

Supporting the role of Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, designed to resolve issues within all regions, including the role of information and communication technologies and cybersecurity in the illicit trade of arms, within an intergovernmental committee,

Deeply concerned about the lack of precision to target the transactions of illicit arms which is caused by the lack of reliable cybersecurity and cyber monitoring systems that inhibits the development of less developed countries,

Recognizing the importance of transparency in this area of concern and in the reliability of data collection exchanges among each nation as well as ensuring reliable and safe policies, actions, and goals,

1. *Invites* UNODC to build on information sharing, while expanding on information on the transaction of the illicit arms through the deep web, allowing UNODC to decipher what strategy is being used to facilitate these transactions, which allows Member States to take action within their own state, such as:

    a. Promoting the UNODC to be in charge of tracking which exact cryptocurrencies, blockchains, and other currencies are involved in the transactions of illicit arms and report them to the program, allowing states to track the movement of these transactions, with the following considerations:

i. This could be done by the use of reverse search of crypto-wallets or consultation of blockchain ledgers;

ii. The Member States could have the right to consult the UNODC to use different methods in order to track these cryptocurrencies, blockchains, and other currencies;

b. Tracking the movement of the illicit arms, and the regions they are moving between, through the use of the PoA SALW and ITI, which require states to ensure that weapons are properly marked and records are kept, and with attention to which sites on the dark web are responsible for the trading of illicit arms;

2. *Requests* updates from the common blockchains being used in different regions, to allow Member States the opportunities to combat the root of the transaction, limiting purchasing abilities;

3. *Promotes* the establishment by the UNODC of a knowledge-sharing platform, accessible to Member States, where best practices, research findings, and analytical tools for addressing unknown risks in the illicit arms trade are disseminated;

4. *Encourages* the leading nations in the ambit of information security professionals and their resources in order to filtrate through the shadow sites, such as the dark web, to gain information on the process of purchasing the illicit arms through the efforts of the UNODC, allowing access to knowledge-sharing platforms in regards to the purchasing of the illicit arms and the unknown risks associated with the purchasing of illicit arms through blockchains;

5. *Strongly reaffirms* the establishment of advanced technologies, such as artificial intelligence and data analysis, in identifying and disrupting illicit arms trade networks to identify the currency through the UNODC;

6. *Recommends* the UNODC to implement a universal accord through the use of the Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, suggesting limitations of software and platforms which are open for public use in reducing criminal threats of illicit trades, which will aid in the discovery of dark web platforms where the illicit purchases of arms are conducted;

7. *Strongly commends* the efforts of the UNODC to allow access to knowledge-sharing platforms in regards to the purchasing of the illicit arms and the unknown risks associated with the purchasing of illicit arms through blockchains;

8. *Calls for* cyber tracking by “The Cyber PoA” program established by the UN outlined in resolution General Assembly resolution 77/37 on “Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security” (2022) in order to track currencies, crypto-currencies, or blockchains used in the purchase of illicit arms, upon the request of the nations that need it;

9. *Proclaims* relevant cybersecurity resources that patch cyber vulnerabilities through collaboration with cybersecurity analyst agencies will ensure a robust and safer approach to the illicit trade of arms, leading Member States to filtrate through the dark web and gain information on the process of purchasing the illicit arms through PoA SALW and the national report Member States send every two years.

Code: GA1/1/5
Committee: General Assembly First Committee
Topic: The Role of Information and Communication Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Noting the adoption of the International Tracing Instrument (ITI) (2005) to enable Member States to identify and trace, in a timely and reliable manner, illicit trade of small arms and light weapons (SALW),

Acknowledging the rise of digital banking, especially in African Member States, in most of which this is the main form of banking used, and the cyber security measures that can be implemented to better ensure that digital transactions are being done safely and legally,

Reaffirming the framework provided by the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA),

Fully alarmed by the lack of cooperation between Member States-led efforts to combat the innovations in the illicit arms trade,

Recognizing Article 11 of the *Charter of the United Nations* (1945) and the vested interest that the General Assembly has in the issue of disarmament,

Applauding Member States' recent achievements in overcoming civic and historical disagreements to facilitate the expansion of bilateral treaties such as the *Arms Trade Treaty* (ATT) (2013) and the *United Nations Convention against Transnational Organized Crime* (2000), targeted at intelligence agreements on illicit arms deals,

Guided by the United Nations International Computing Centre (UNICC) and the outline of norms on state responsibilities in regard to cyberspace behaviors of the United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (GGE),

Emphasizing the importance of the *Budapest Convention on Cybercrime* (2001), the *African Union Convention on Cyber Security and Personal Data Protection* (2014), and the *Agreement Between the Governments of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security* (2009) as regional treaties and their promotion of a global approach that seeks to integrate national laws, enhance investigative abilities, and enable international cooperation for the purpose of defining criminal offenses for cybercrimes,

Acknowledging the significance of promoting international cooperation and knowledge exchange as essential components in enhancing cybersecurity measures across Member States, specifically through mechanisms of the United Nations Office on Drugs and Crime (UNODC) and the draft *Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* (Cybercrime Convention),

Bearing in mind the disparity in access to information and communication technology (ICT) resources between more developed and developing Member States,

Affirming the work of the United Nations Office for Disarmament Affairs (UNODA) in facilitating information-sharing and transparency in arms control efforts,

Recognizing the need for additional education programs to ensure the proper use of ICT and cyber security, as outlined in General Assembly resolution 77/71 on “The illicit in small arms and light weapons in all its aspects” (2022),

Cognizant of the detrimental impact of the illicit trade in arms on advancing progress towards Sustainable Development Goals (SDGs) 3 (Good health and well being) and 17 (Partnerships for goals), including progress through global partnerships such as the North Atlantic Treaty Organization’s Cooperative Cyber Defence Center of Excellence and its efforts to support interdisciplinary research, training, and exercises on cyber defense,

Deeply concerned about increasing risks caused by cybersecurity tension between non-state actors,

Stressing the importance of the achievement of SDG 9 (Industry, innovation and infrastructure) due to its connection to the internet as a free-flowing source of information,

Calling attention to SDG 16.4 (“By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime”) and its importance in reminding us to continually work towards the reduction of the flow of illicit arms,

Deeply concerned about the facilitation of crimes through encrypted forms of communication like Encrochat, which, according to Europol, has led to over 6,500 arrests worldwide,

Acknowledging the need for monitoring the use of blueprints for 3D printing arms in illicit trade, as there is a lack of research surrounding that technology,

Reaffirming General Assembly resolution 77/298 on “The United Nations Global Counter-Terrorism Strategy: eighth review” (2023) and its goal to enact counter-terrorism strategies and renew its unwavering commitment to pursuing international cooperation,

Acknowledging the escalating threat posed by the dark web to international peace and security through its facilitation of the illicit arms trade,

Recalling General Assembly resolution 76/19 on “Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behavior in the use of information and communications technologies” (2021) and its emphasis on the promotion and use of information and communications technologies for peaceful purposes,

Guided by the *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition supplementing the Convention against Transnational Organized Crime* (Firearms Protocol) (2001), as it is the only legally binding instrument to counter the illicit manufacturing and trafficking of firearms at the international level,

Recalling the importance of existing regional and interregional forums, such as the European Union – League of Arab States Project and the Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies of the Association of Southeast Asian Nations’ Regional Forum and their effectiveness in furthering collaboration between Member States,

Further recalling Security Council resolution 1540 (2004) on “Non-proliferation of weapons of mass destruction” and its condemnation of the proliferation of weapons within Member State and its connection to non-state actors,

1. *Encourages* transparency in information sharing between Member States by:

    a. Leveraging SDG 16.4 to encourage and highlight the importance of transparency in the repossession of stolen or illegally produced arms, and of returning them to their State of origin;

    b. Promoting awareness of possible malware attacks over ICTs by utilizing partnerships between Member States to share prevention and defense tactics;

2. *Advocates* that Member States create legislation to implement stronger cyber security measures in banks to better ensure that digital transactions are being done safely and legally by implementing pattern recognition, fraud detection, and risk management artificial intelligence (AI) in transaction monitoring in order to detect accounts involved in fraud;

3. *Further recommends* the implementation of ITI policies regarding information sharing among Member States on the flow of illicit arms within the international community by:

    a. Increasing the scope of comprehensive and selective training, as described in the ITI;

    b. Increasing the quantity and verification of small arms marked by import marking, as indicated in the ITI;

    c. Implementing the transfer of information through comprehensive guidance documents that are shared with utmost transparency;

    d. Reconsidering the ITI with new technological developments in mind, like malware tracing and the rise in popularity of three-dimensional printing;

4. *Encourages* Member States to strengthen local laws to identify and trace, in a timely and reliable manner, illicit SALW;

5. *Recommends* the utilization of blockchain technology in the establishment of an international SALW tracking network to be maintained and managed by UNODA, thereby creating an easily verifiable and immutable record which should increase confidence in the system’s data and promote participation from Member States;

6. *Strongly suggests* that the United Nations Development Programme establishes a comprehensive database using information voluntarily provided by participating Member States to track and trace the movement of arms using digital technologies;

7. *Calls upon* all Member States to ratify the Firearms Protocol to create more transparent and effective tracing mechanisms geared towards the illicit manufacturing and trafficking of firearms between non-governmental actors at the international level;

8. *Urges* the expansion of the ITI in order to explore the implementation of best technological practices regarding weapons tracing by:

a. Researching blockchain technologies;

b. Exploring malware prevention;

c. Renewing the ideas explored in the 2005 ITI, to reflect the modern technological climate;

9. *Encourages* the expanded outreach of programs like the UNICC's Common Cyber Security Operation Center to include in its scope Member States with less developed cybersecurity foundations;

10. *Strongly recommends* Member States to ratify or continue their commitment to upholding the revisitation and renewal of the ATT and to maintain the spirit of ensuring the treaty's implementation and sustainable development as part of the holistic effort to place an emphasis on cybersecurity and specifically on the treaty's commitment to develop an export and import control system as well as the regulation of the transit of weapons;

11. *Suggests* Member States to work with United Nations bodies such as the UNICC to partner with NGOs to engage in discussions that emphasize the development of cyber security and intelligence infrastructure to track and prevent the illicit trade of arms;

12. *Suggests* UNODA to focus efforts on the primary objective of monitoring and mitigating the online presence associated with the illegal trade of firearms;

13. *Invites* Member States to a Global Cyber Conference with the support of UNODA and the ICT Development Fund to facilitate collaboration in order to develop cybersecurity technology to combat the illicit arms trade online and to address new technologies that exacerbate the issue by inviting government, industry, and academic experts to promote cutting-edge cybersecurity efforts and share best practices to combat online illicit arms trade;

14. *Recommends* Member State oversight on surplus and abandoned weapons that can enter the illicit arms trade;

15. *Recommends* to expand the ongoing negotiation of the Cybercrime Convention regarding its utilization and functionalities in order to:

    a. Address new and emerging ICT technology such as cryptocurrencies and AI in proactively addressing cybercrime threats;

    b. Include the implementation of educational programs and the open sharing of best practices between Member States;

    c. Create mentorship workshops led by Member States with advanced ICT infrastructure to better support Member States with limited technological capacity;

    d. Focus on education regarding best practices for the identification and prevention of cybercrime in the illicit trade of arms in smaller Member States;

16. *Encourages* the expansion of the Security Council's investigation program, which verifies Member States' estimated armaments, to include an estimated flow of illegal weapons through blockchain and ICTs;

17. *Advises* the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to develop and call for the implementation of comprehensive legislation to effectively regulate and counter the illicit activities on the dark web through:

    a. The establishment of clear legal definitions and provisions specifically addressing illicit activities on the dark web, including the illegal arms trade;

    b. The creation of cooperative mechanisms between governments, technology companies, and relevant stakeholders to ensure the swift adaptation of legislation to the evolving landscape of the dark web;

    c. The incorporation of robust measures to enhance the investigatory powers of law enforcement agencies, enabling them to effectively track, monitor, and prosecute individuals involved in illicit activities on the dark web;

18. *Welcomes* Member States to consider adding the integration of a program like the PoA on cybersecurity and ICTs in Member States' governments with a focus on:

    a. The robust protection of vital societal functions;

    b. The improvement and prioritization of skills and management;

    c. The strengthening of the cooperation between the public and private sectors;

    d. Active participation in the international fight against cyber threats;

    e. The facilitation of communication for the dual track discussions occurring between the GGE and the Open-ended Working Group on security of and in the use of information and communications technologies;

19. *Encourages* the United Nations Educational, Scientific, and Cultural Organization to develop educational programs focused on the proper use of cybersecurity, which can be utilized in developed and developing Member States alike;

20. *Suggests* Member States to be open to anticipating and potentially supporting the finalization of the current draft of the Cybercrime Convention, in order to share resources and security information between governmental agencies about potential cybercrime threats related to the illicit trade of arms;

21. *Encourages* Member States to volunteer in financially supporting the implementation of educational programs and capacity-building efforts related to the intersection of ICTs, cybersecurity, and arms trade;

22. *Strongly recommends* the UNODC to compile and disseminate pertinent guidelines, such as case studies on the spread of illicit weapons and instruction materials on best practices regarding cybersecurity, to assist Member States in their capacity-building efforts;

23. *Encourages* the expansion and acknowledgment of regional and interregional programs to include the illicit trade of arms as one of their focal points to better emphasize threats related to cybersecurity, promote best-practice sharing, and to help Member States lacking critical infrastructure against the proliferation of arms.

Code: GA1/1/6
Committee: General Assembly First Committee
Topic: The Role of Information and Communication Technologies, and Cybersecurity in the Illicit Trade of Arms

---

The General Assembly First Committee,

Taking into account that Member States have suffered attacks without being able to identify the actor,

Fully alarmed that 27% of all civilian deaths in armed conflict are the result of small arms and light weapons (SALW) with developing Member States being disproportionately affected by the trafficking of arms as it correlates to injurious socioeconomic conditions,

Concerned that the Secretary-General reported that the widespread availability of SALWs was a factor in 250 conflicts and more than 50,000 deaths a year,

Alarmed by the estimated 1 billion illicit SALWs that are in international circulation,

Considering a lack of implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components, and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime within General Assembly resolution A/RES/55/255 (2001) on the "Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime",

Aware that Member States have not updated their implementation status of the Programme of Action (PoA) for 2022, thus highlighting the lack of transparent tracking data available for illicit SALWs,

Deeply concerned by the lack of a strong international system of accountability and transparency concerning tracing arms,

Believing that enhancing education in cybersecurity and blockchain technologies benefits technological advancements in the least-developed countries (LDCs),

Recognizing Sustainable Development Goal (SDG) 17.9 ("enhance international support for implementing effective and targeted capacity building in developing countries to support national plans to implement all SDGs, including through North-South, South-South, and triangular cooperation") and the need for international and inter-organizational partnerships that aid in addressing the illicit trade of SALWs to non-state actors especially in regards to Information and Communication Technologies (ICT) and cybersecurity,

Further recognizing the importance of technological development in achieving SDG 3 (Good Health and Well-being), SDG 5 (Gender Equality), SDG 16 (Peace, Justice, and Strong Institutions), and SDG 17 (Partnerships for the Goals),

Further considering the insufficiency of effective cyber security infrastructure among developing nations due to economic and financial limitations**,**

Taking into account the lack of educational programs and funding for cybersecurity in developing nations,

Recognizing the important relevance of the *Addis Ababa Action Agenda* (AAAA) of 2015,

Emphasizing the necessity of engaging and working with private technology industries for neutral, cooperative development and action,

Advocating working through the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and enforcing a more actionable framework against terrorism based upon the United Nations Charter as urged by Security Council Resolution 2354 (2017) on “Countering violent extremism and terrorist narratives,”

Emphasizing a need for more developed cybersecurity legislation on the African continent as e-commerce is forecasted to expand to 520 million people by 2025 as stated by the International Trade Administration,

Deeply disturbed by the lack of technological assistance development and usage in combating the illicit trade of arms,

Noting that with the identification of Member State vulnerabilities that are possible targets for illicit arms trade by malicious actors in cyberspace, Member States can better mitigate future cyber risks,

Deeply disturbed by the constant adaptation of illicit arms to the advances of the interconnected technologies and interweb implications,

Fully aware of the main streams of illicit trade of arms, which are the places where these can be purchased, such as the black market or the dark web,

Aware of the use of a large percentage of communications between illicit arms traders occurs on social media platforms,

Illuminating the advancements in technology, such as 3-D printing of firearms, and the critical need for cyber security measures to combat the misuse of these new technologies,

Recognizing that manufacturing weapons without restrictions or proper tracking makes it possible for unauthorized groups and individuals to obtain them,

Further recognizes the challenges of physically policing Member State borders,

Noting the lack of common language and information sharing around combating the illicit arms trade,

Firmly convinced that a lack of engagement with civil society actors in spreading public awareness about ICT perpetuates illegal trafficking and arms markets,

Stressing the consequences that the illicit trafficking of arms has on Member States' civilian populations affecting SDG 3,

Recognizing that the further use and development of new ICTs such as Artificial Intelligence (AI) and Internet of Things (IoT) devices, can effectively address illicit trade of SALWs,

Deeply alarmed by the illicit trade of arms affecting Member States in the area of border security,

Guided by the passing of the *United Nations Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition* (Firearms Protocol), which provides Member States with a guideline on how to criminalize the illicit manufacturing and distribution of firearms, their parts, components, and ammunition,

Noting with deep concern vulnerable nations and their internal issues to regulate SALWs due to lack of ICT regulation,

Alarmed with how the illicit use of three-dimensional printed guns can be used by terrorist organizations to create and distribute small arms without government oversight,

Bearing in mind the finding of a 2013 report from the European Commission that between 224 million USD to 424 million USD is generated from the illegal arms trade per year globally,

Fully aware of the growing adoption by criminal groups of communication technologies that obstruct the detection of weapon trafficking,

Deeply concerned that the illegal weapons market currently amounts to 20% of the volume of legally traded weapons,

Recognizing the lack of a framework for the task force to draw upon triumphant United Nations models like the Counter-Terrorism Implementation Task Force (CTITF),

Acknowledging the effectiveness of the illicit arms records and tracing management system (iARMS) database in addressing the illicit arms trade and supporting countries in promoting and implementing SDG target 16.4 (“by 2030 significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime”),

Acknowledging SDG target 8.7 (“take immediate and effective measures to eradicate forced labour, end modern slavery and human trafficking and secure the prohibition and elimination of the worst forms of child labour, including recruitment and use of child soldiers, and by 2025 end child labour in all its forms”), which describes the necessity to urgently eradicate forced labor including the use of child soldiers,

Understanding that excess military spending to fight militants leads to a reduction in funds for social and economic development, the increase of child soldiers, and fragmentation locally within communities,

Reaffirming its respect for each individual’s right to live a peaceful life,

Recognizing that women and other genders experience more armed violence than men generally do,

Acknowledging The Onion Router (TOR) program and its effects in granting anonymity to traders on the dark web, where the majority of illicit trade online occurs,

Acknowledging the pivotal function of collective intelligence in tackling threats that cross national boundaries,

Recognizing that manufacturing weapons without restrictions or proper tracking makes it possible for unauthorized groups and individuals to obtain them and hinders the ability of member states to regulate illicit activity,

Taking into account the Secretary-General report 2021/839 (2021) on “Small arms and light weapons” highlighting the alarming statistics on the negative impact of the illicit arms trade, including its contribution to conflicts, human suffering, and threats to sustainable development,

Highlighting the potential for all Member States to play a significant role in shaping global initiatives and regulations related to arms control and arms trade, considering the diverse experiences and challenges each nation brings to the table,

1. *Implores* Member States to regularly update and utilize the International Tracing Instrument (ITI) to further continue and facilitate global cooperation and transparency in the eradication of illicit weapons;

2. *Recommends* the creation of the Reducing Digital Arms Trade Program as a joint effort with cooperating nations and the United Nations Office for Disarmament Affairs (UNODA):

    a. To publish reports highlighting the role of ICTs and cybersecurity in the illicit trade of arms;

    b. To guide policy-making and actions by Member States and stakeholders;

    c. That is implemented by UNODA's Conventional Arms Branch;

    d. That is funded by UN Trust Facility Supporting Cooperation on Arms Reduction Nations Office for Disarmament Affairs;

3. *Encourages* Member States to ratify the Firearms Protocol as an international framework to ensure global tracking of illicit arms supporting SDG 17;

4. *Further encourages* Member States to negotiate a voluntary agreement prohibiting the exportation of SALWs to Designated Conflict Zones, with provisions for sanctions to be enforced against Member States that do not comply with the agreement;

5. *Suggests* the integration of the International Criminal Police Organization (INTERPOL) into the United Nations, in line with General Assembly resolutions 71/19, 73/11, 75/10, and 77/20, and the creation of an INTERPOL task force focused on the links between cybercrime and arms trafficking, to support Member States in the implementation of:

    a. The Firearms Protocol;

    b. The PoA SALW;

    c. The ITI;

    d. The ATT;

6. *Invites* the expansion of the scope of the World Information Society in the works of an international conference for nations to engage in discussion on security concerns pertaining to illicit arms trade;

7. *Further requests* efforts towards the development of new and existing educational frameworks for cybersecurity in developing nations through:

    a. Collaborating with the United Nations Information Security Special Interest Group to ensure inter-agency cooperation and sharing of cyber-security information;

    b. Establishing a framework focusing on education of cyber-safety in developing nations;

8. *Suggests* the creation and transference of new technologies during the annual conferences to address the illicit arms trade, reminiscent of the AAAA of 2015;

9. *Advises* Member States to work within the PoA SALW to coordinate their management and control interventions to strengthen national mechanisms for small arms management and control;

10. *Recommends* the implementation of the Illicit Arms Records and Tracing Management System (iARMS) database by the Member States through their respective police services, customs agencies, border protection agencies, and regulatory authorities to accurately track and deter the illicit trade of arms;

11. *Recommends* the formation of a task force to address the issue of the trade of illegal arms by supporting the formation of an international task force that:

    a. Establishes and administers of a specialized group, whose sole task is to oversee and eradicate platforms that aid in the illicit distribution or trading of weaponry;

    b. Acknowledges the pivotal function of collective intelligence in tackling threats that cross national boundaries;

    c. Formulates the framework for the task force by drawing upon triumphant UN models like the CTITF, customizing its structure to confront the unique challenges presented in combating illegal weaponry;

    d. Uses the CTITF's framework, focus on efficient mechanisms for disseminating information among member nations, intelligence bodies, and global institutions;

12. *Strongly encourages* the offering of educational opportunities that therefore can give enough preparation to government's representatives on cryptocurrencies and blockchain, mostly by implementing blockchain analysis tools that:

    a. Provide education systems of all supporting Member States, integrating the said topics to produce individuals that show competency in adapting to the 21st century;

    b. Promote the expansion of opportunities for individuals, especially the youth through programs that hold the objective of future advancement;

13. *Recommends* the increment of educational opportunities in cybersecurity and blockchain technology to train and prepare Member States representatives to lead in creating an adequate number of instructors;

14. *Suggests* the Security Council create and implement a cyber-security peacekeeping branch with Member States;

15. *Recommends* the creation of an International Organization for Standardization standard for the serialization of small arms to address the overlapping of serial numbers for different models of firearms, and the creation of an International Firearms Database for small arms using INTERPOL's iARMS as a framework, with a formal commitment by Member States to abide by the standard to be considered;

16. *Recommends* the development of modern systems employing reallocation and adapting the necessary infrastructure to utilize and maintain these systems within LDCs, which:

    a. Offer the concentration of the development of said infrastructure in countries with high rates of conflict or rate of arms deals;

b. Calls for the implementation of programs in developed Member States to support digital assets in Member States in need;

17. *Strongly recommends* the establishment of blockchain technology, which allows the surveillance of activities such as the use of cryptocurrencies as a means of tracing arms to combat illicit activities cultivated by private companies to allow for international cooperation and data sharing regardless of a nation's developed status;

18. *Invites* partnerships with NGOs and Member States that have existing and extensive ICT infrastructure that will assist in installation and education on ICT technology to ensure continuous safety of civilians in all Member States, supporting SDG 11 (Sustainable Cities and Communities) in making cities and human settlements safe, resilient, and sustainable, which:

    a. Recommends the strengthening of the legal frameworks to prosecute individuals and entities involved in illicit arms trading through ICT networks;

    b. Looks to the Member States to individually determine punishments for illicit arms traffickers based on where the violation occurred;

    c. Includes ICT technology for protective surveillance of universities, schools, hospitals, and other public sectors around Africa, supporting the SDG 5, ensuring safety, especially for women/children that are a part of the vulnerable population preventing situations such as the Chibok schoolgirls kidnapping;

19. *Encourages* developed countries to consider investing in LDCs for the construction of infrastructures necessary for preventing the illicit trade of arms;

20. *Strategizes* for African Member States to work alongside organizations such as The Infrastructure Consortium for Africa and more developed Member States to develop ICT infrastructure within least developed African communities;

21. *Further encourages* members to contribute to the improvement of digital forensic tools and policing software to further combat the ongoing trade online;

22. *Invites* Member States to consider the use of drones in monitoring sensitive areas that are directly and indirectly impacted by the illicit trade of arms within borders of Member States, and the support of other Member States to such technology to be accessible;

23. *Encourages* Member States to use search algorithms to track down and eliminate documents, files, and downloads of three-dimensional firearms and other small arms that are not traceable, by:

    a. Monitoring the type of three-dimensional firearms by using search and artificial algorithms;

    b. Using search and AI algorithms to track down and eliminate documents, files, and downloads of three-dimensional firearms and other small arms that are not traceable;

24. *Advises* Member States to cooperate and work together to distribute knowledge of techniques, technology, strategies, or other methods to assist Member States in regulating three-dimensional printed firearms and their ammunition;

25. *Directs attention to* new ICT technologies with possible applications in monitoring the distribution, transportation, and tracing of all arms and their components such as:

    a. AI analysis in the detection of anomalies in arms transactions;

    b. IoT devices and sensors for tracking movement and usage of SALWs and their components;

26. *Recommends* Member States to consult with manufacturers about incorporating AI into the firmware of 3D printers to detect and prevent the printing of firearms;

27. *Proposes* Member States establish and implement virtual manning strategies utilizing geo-surveillance options for the effective monitoring of land and sea borders;

28. *Encourages* all Member States to engage private technology industries in their efforts to develop ICTs and address illicit arms trade for the purposes of:

    a. Learning about new endeavors and advances in ICTs available to state and non-state actors;

    b. Developing a neutral environment for standardized discourse between Member States about the development and utilization of ICTs;

29. *Encourages* cooperation between Member States and civil society organizations to play a vital role in spreading public awareness about the illicit trade of SALWs to:

    a. Establish non-state bases to monitor illicit trade of SALWs at local levels;

    b. Educate civilians about the threats of illegal arms trafficking;

30. *Invites* further support of the Tech Against Terrorism (TAT), a public-private partnership with the UN Security Council as the TAT, which:

    a. Funds smaller companies to combat terrorism and further the development of cyber technology to hinder terrorist success;

    b. Addresses the illicit trade of arms by addressing challenges related to AI usage and terrorism;

31. *Supports* the creation of the Transnational Conference Against Arms Trafficking that will meet annually to give a platform for the public and private sectors to come together and discuss best practices and progress on the mitigation of arms trafficking by:

    a. Achieving SDGs 3, SDG 5, SDG 16, and SDG 17 (partnerships for the goals) by creating partnerships between Member States and NGOs such as Amnesty International;

    b. Requesting implementation by the UNODA;

    c. Increasing transparency and cooperation regarding Member States' arms transferring methods and progress on the mitigation of the illicit trade of SALW through reports from each Member State during the conference;

32. *Affirms* the continuation of research on the ever-changing aspects of technology to better address the illicit arms trade which will be addressed through:

    a. The World Economic Forum, where Member States and non-member states attend and are updated on ICT-related issues, and relevant information regarding the success of the program;

    b. The multilateral communication between Member States;

33. *Recommends* increasing buyback programs and volunteer dismantlement, reminiscent of campaigns utilized internationally, exemplified in various World Bank initiatives;

34. *Calls upon* Member States to increase parameters of security cooperation regarding illicit arms trade through ICTs with the goal of:

    a. Addressing cross-border security cooperation to address the global reach of the illicit arms trade through ICTs and cross-border black markets;

    b. Suggesting international standard for explicitly defining SALWs and larger weapons of destruction within the illicit market;

35. *Requests* the United Nations Office on Drugs and Crime and other relevant international organizations to provide guidance and support to Member States to enforce regulations to combat the illicit arms trade facilitated by ICTs to:

    a. Publish reports highlighting the role of ICTs and cybersecurity in the illicit trade of arms;

    b. Guide policy-making and actions by Member States and stakeholders;

36. *Reiterates* the importance of Member States following the guidelines set by the Firearms Protocol and implementing their strategies for regulating the illicit production and distribution of three-dimensional firearms and their ammunition;

37. *Emphasizes* collaboration among Member States and the United Nations Cyber Security Council in information regarding the tracking of individuals who use TOR to gain access to the dark web and partake in the illicit trade of arms;

38. *Strongly urges* Member States to address the issue of the trade of illegal arms by supporting the formation of an international task force by:

    a. The establishment and administration of a specialized group, whose sole task is to maximize and enhance coordination and coherence of efforts to combat the issue of ICTs and their role in cybersecurity;

    b. Ensuring that the UN system is accommodating the needs of Member States, provides them with the necessary policy support and spreads in-depth knowledge with regard to ICTs, and wherever necessary, addresses the paramount issue regarding cybersecurity;

    c. Replicating the CTITF's focus on efficient mechanisms for disseminating information among member nations, intelligence bodies, and global institutions;

39. *Endorses* the United Nations Cyber Security Council to encourage and support social media companies to bolster their security and use AI to identify profiles of illicit arms traders and share information with law enforcement of Member States on the network of illicit arms trade;

40. *Recommends* the standards of acknowledgment be adopted universally and pushed to modify international law to incorporate attribution standards and encourages all United Nations partners to adopt this practice to better prepare for future attacks;

41. *Calls upon* Member States to seize and destroy illicit weapons, unmarked weapons, and weapons seized following an armed conflict;

42. *Encourages* Member States to utilize the United Nations Register of Conventional Arms (UNROCA) to maintain a system of accountability and transparency by:

    a. Keeping records and submitting reports of weapons that are seized and destroyed to UNROCA;

    b. Establishing national databases with yearly records of all weapons dealings and voluntarily submitting these reports to UNROCA;

43. *Proposes* to expand the PoA SALW framework through international cooperation with local police and military on cybersecurity and understanding the online black market;

44. *Promotes* communication with cybersecurity experts who are knowledgeable on the dark web and internet monitoring to:

    a. Inspect platforms on the dark web that favor the transaction, transportation, communication, planning, and recruitment that small groups of terrorists may adopt and utilize;

    b. Investigate a way to monitor the financial flow in the dark web;

    c. Incorporate the result of those investigations into the database for further research and AI learning for a more effective way of tracking;

45. *Encourages* Member States to develop national laws to keep track of weapon manufacturers and hold the private sector accountable to the tracking requirements as outlined in ITI and PoA, to:

    a. Develop national databases in accordance with ITI that track which companies manufacture weapons;

    b. Require companies to keep track of the number of weapons they produce and report that to the national government;

    c. Have a security body review and approve weapons transactions and the likeliness of them alluding to illicit operations;

    d. Utilize the definitions and tracking frameworks outlined in ITI for developing specific tracking methods;

    e. Create a third-party group to extensively manage the collection of data analysis to keep track of how conventional weaponry is being transferred among all Member States;

46. *Recommends* the Member States that depend economically on the manufacturing and exportation of weapons, have a 15-year goal to lessen the specific creation of certain weapons by 5% and those Member States without current weapon manufacturers should consider never creating those for civilian use;

47. *Stresses* that Member States gain knowledge of the danger that arises with the use of child soldiers and suggests the additional support of the United Nations Office of Counter-Terrorism.