United Nations Security Council

Directed By: Gabriel Wilson

TSMUN XXVII BACKGROUND GUIDE 2023

Topic I: Strengthening Global Cybersecurity

Topic II: Regulating Emerging Technologies and Weapons Proliferation

Dear Delegates,

Welcome to Tallahassee Southern Model United Nations. My name is Gabriel Wilson, and I am the Director of the Security Council for TSMUN 2024. Your Assistant Director is Nicole Ordonez. This is both our first year participating in MUN. We are both majoring in political science with aspirations to attend law school. We also are planning to transfer to FSU upon the completion of our tenure at TCC. Currently, we are members of the TCC Model United Nations team.

The topics under discussion for this year’s Security Council are:

1. Strengthening Global Cybersecurity
2. Regulating Emerging Technologies and Weapons Proliferation

The United Nations Security Council is one of the six main organizations of the UN. The Security Council is tasked with sustaining international peace and security. It is the only UN body with the authority to adopt binding resolutions as well as impose economic sanctions and military power. The Council is made up of fifteen Member States, which include five permanent members with the power of veto. The membership, functions, and governance of the Security Council make it a unique body of the UN.

I hope you find this background guide useful in your preparation for the conference. This background guide is meant to introduce delegates to the topic that will be discussed in committee and provide guidance as delegates begin their research. Delegates are strongly encouraged to research the positions, views, and opinions of their Member States as well as relevant regional and international frameworks, past resolutions, and organizations and initiatives.

Each delegation will submit a position paper for the committee. Delegates must turn in a hard copy of their papers before the start of the first committee session to their directors.. Papers may be emailed to “sg@tsmun.org” or a usb drive will be appropriate.. For a position paper guide and an example position paper, please visit http://www.tsmun.org/position-papers.html. Papers that are not in the correct format will not be eligible for awards. For conference information, resources for preparation, scholarships, and other useful information, visit http://www.tsmun.org/. If you have any questions leading up to the conference, feel free to contact me at sc@tsmun.org. I look forward to seeing you all in committee.

Sincerely,

Gabriel Wilson, Security Council Director

Nicole Ordonez, Security Council Assistant Director

Sc@tsmun.org

Committee Overview

Introduction

The United Nations Security Council's (UNSC) primary duty is to maintain peace and security, and to act when they're encroached upon.[1] When a concern arises, the UNSC initially encourages settlement upon peaceful means. Should the dispute lead to hostility the UNSC's new objective is to reach an amicable agreement between those involved. When these options aren't viable, the Council is authorized to use enforcement measures, such as: economic sanctions, blockades, severance of diplomatic relations; even collective military action.[2] Ultimately, the scope of response is meant to hold those responsible accountable for their actions and minimize the impact of those caught in the crosshairs.

Committee Mandate

The UN Charter called for the creation of six main organs for the function of the UN. Amongst them was the Security Council, in which the Charter gives primary responsibility of maintaining international peace and security. The Charter bestows the UNSC four purposes: maintain peace and security, develop friendly relations between nations, cooperate in solving international problems and promote respect for human rights; and be a hub for reconciling the actions of nations. It is the only organ that makes decisions Member States are obligated to follow.[3]

History

The Cold War paid a heavy toll on the effectiveness of the UNSC, to some making it a very ineffective institution. However, the Soviet Union's boycott of the UNSC meant the United States (US) was allowed to push through resolutions in support of South Korea during the Korean War. In the latter part of the 20th century, the Council saw its power grow when there was a surge of peacekeeping missions. Such missions included those conducted in the Balkans, Haiti, Somalia, and Liberia. Though, a notable failure of this newfound strength, that led to some questioning the Council's effectiveness, is the events that occurred in Rwanda and Bosnia. A poor judgement decision made to rollback troops in Rwanda, in part lead to the Rwandan genocide. Originally, the UNSC had 11 members with only 5 of those members being permanent ones. Those Member States are The Republic of China (Taiwan), France, the Soviet Union, the United Kingdom, and the United States, with six temporary members. These members are elected by the United Nations General Assembly (UNGA) every two years. In 1965, the UN

[1] "What is the Security Council? ." United Nations. United Nations.
[2] "What is the Security Council? ." "Maintaining Peace and Security ." United Nations. United Nations.
[3] "What is the Security Council? ." "Mandate ." United Nations. United Nations.

Charter adopted an amendment that allowed the UNSC to take in 4 more members making it a 15-membership council, with 5 members being permanent and the other ten being elected by the UNGA every two years. In 1971 The Republic of China (Taiwan) was replaced by The People's Republic of China and in 1991 when the Soviet Union fell, it was replaced by its succeeding state, the Russian Federation

In the 21st century, the perceived effectiveness of the Council began to wane when the first peacekeeping mission failed. In 2003, militias in the Sudanese region of Darfur began terror campaigns, and the UNSC voted to send a peacekeeping mission to the region. However, the Sudanese government rejected it. A compromise was reached that included UN peacekeeping forces and African Union (AU) peacekeeping forces. The Council voted to formulate the Joint Investigative Mechanism to investigate the usage of chemical weapons by President Assad in the Syrian Civil War.

Governance, Structure, & Membership

The UNSC can do much more than just making decisions to maintain peace and security. In the case the UNSC needs to make a decision all Council members need their representatives present. In accordance with its power to hold parties responsible, it is allowed to form tribunals to try such parties. Unlike decisions made by the GA, those made by the UNSC are binding. Should its decisions not be followed the UNSC is allowed to take measures to ensure the enforcement of its decisions. It also is allowed to make recommendations to the GA on appointing a new Secretary-General of the UN (SG) and inducting new Member States.

The UNSC is composed of 15 Member States, five of these members are permanent. The Council members that hold those seats are China, France, Russia, United Kingdom (UK), and the US. All five of them are allowed to veto resolutions. All decisions require nine votes to pass, except procedural ones which require a simple majority. Should a member vote “no” or there’s a veto, then the resolution isn’t passed. Members may abstain should they want to. The UNSC also constantly changes its working methods to reflect the demands made by the political and economic environment of the day. The UNSC conducts itself into four types of meetings. These include open debate, debate, briefings, and adoption. The differences between the debates is open debate is on issues concerning everyone, debate is about a particular issue in a country. Briefings are conducted to update Council members on the current status of a conflict. Adoption is the procedure the Council undertakes to take action on a draft resolution. There are private meetings as well. The UNSC is chaired by a President that rotates each month among Council members alphabetically. Should the President wish to recuse themselves then the next Member State on the list assumes the position. The President may introduce thematic issues onto the Council’s programme of work with consent of Council members. The powers of the President are: presiding over meetings of the Council, briefing non-Council members, holding bilateral meetings between parties, representing the Security Council and delivering messages on its behalf, and being the face of the Council at press meetings.

Conclusion

The UNSC is one of the most important institutions of the UN. Its importance in the day-to-day operations of the world can not be dwarfed by anything. Its resolutions have had profound effects on the events they were intended to influence, effects we still feel today even. The UNSC is really the highest deliberative body on our planet and without it we wouldn't have the ability to make decisions that need haste. That being said, it is also important to note that the UNSC is also a cog in the machine that we call world peace. If it wasn't for the actions of the other organs of the UN, such as the GA, the world we live in would be very different. This also includes the Member States of the UN agreeing to participate in the biggest experiment imaginable, an experiment that includes the entire world and all of the people in it.

Topic I: Strengthening Global Cybersecurity

Introduction

As technology has developed we have increasingly become more interconnected with one another. More often than not we are seeing aspects of commerce, communication, government, and enterprise utilize these technological developments. At the same time there has been a growing concern for the security and privacy of these connections. In order to help alleviate these concerns, the UN has adopted necessary policies through the United Nations System Chief Executive Board (CEB) and two high-level committees. These committees being the High-level Committee on Management (HLCM) and High-level Committee on Programmes (HLCP). These bodies have worked to advance cybersecurity of our international systems as well as curtail the frequency and severity of cybercrime. In recognition that the UN's own systems can fall victim to cyberattacks, the CEB and HLCP have backed UN-wide frameworks to establish development of cybersecurity.

There is a need for internal cooperation between UN agencies/entities to ensure the security of UN systems. The CEB endorsed a plan for coordination in 2014, a plan reviewed, approved, and submitted to the CEB by the HLCM and HLCP. In this plan agencies agree to cooperate with one another to cope with cyberthreats and recognize that such threats can slow the progress of UN development efforts. The Digital and Technology Network (DTN) agreed to form the Information Security Special Interest Group (UNISSIG) that is dedicated to promoting inter-agency cooperation. The UNISSIG is the principal mechanism in this manner with its primary objective being securing information within member organizations. This is done through the assessment of UN systems and their exposure to internal and external threats.

Current Situation

With the onset of the COVID-19 pandemic the world saw an exponential amount of people connected to the internet. In the United States (US) alone there were 800,944 complaints of cybercrimes with a net loss amount of $10.3 billion in 2022, according to the FBI. Though there was a decrease of 5% in the number of complaints, there was also a 49% increase in the dollar losses experienced. Of the crimes committed, phishing schemes were the most reported with 300,497 complaints with a total of $52 million in losses. In regard to financial losses, with a total of $3.3 billion in losses, investment schemes take the cake. The largest demographic to report cybercrime were those between the ages of 30 and 39, but the greatest dollar loss was experienced by those in the 60+ range. Interestingly enough, cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in losses with those between 30 and 49 being the most targeted.

The US, however, wasn't the only nation afflicted with an onslaught of cybercrimes. Another nation heavily attacked was India. According to Statista, there were 27,374 arrests nationwide in India for those committing cyber crimes in 2023. The most common crime committed was multipurpose malware, or software designed to harm multiple facets of a target's software. 52,000 crimes were committed in 2023 with a total accumulation of $2.18 million in damages. Another country that has been a hotspot for cybercrimes was Russia. In 2021, Russia accounted for a quarter of all unsolicited spam emails sent to persons, in one day alone that year more than 7 billion spam emails were sent from Russia according to Statista. Though, also in 2021, 18% of personal computers faced at least one malware attack and one-tenth of all computers in Russia were attacked by phishing schemes on a yearly basis.

Other nations, such as those in Latin America, have faced some serious damages from cybercrimes as well. In 2019, Ecuador and Paraguay saw the most cyberattacks than any country in the region with 70% of their IT managers reporting malware infections. Brazil, Colombia, and Mexico account for 9 out of 10 attacks registered in Latin America combined, according to Statista. 65% of cyberattacks reported in 2020 in Brazil were ransomware attacks, it's the same case for Colombia and Mexico but at 44% of crimes reported. That being said the Brazilian, Colombian, and Mexican governments have taken some steps to prevent these crimes being committed. Colombia has the highest percentage of companies with cybersecurity politics and all three nations have their IT teams spend exorbitant amounts of time on security. However, the three spend at least a third of their time responding to cyberattacks.

Actions Taken by the UN

The UN has taken many steps in the effort to curtail the effect of cyberattacks and to bolster the development of cybersecurity. One of the first actions taken to curb cyberattacks was Resolution 55/63, adopted in January 2001. In this resolution, the UN recognizes the need to combat the criminal misuse of information technologies. That the development of free flow technologies and telecommunications can promote economic and social development, education, and democratic governance. However, it also recognizes that there is a concern in these advancements that may create new opportunities for criminal misuse and activity. The resolution also gives credit to the Council of Europe, Group of Eight (at the time), and the Organization of American States and their subsidiary bodies for putting effort into the prevention of criminal misuse of information technologies. It also notes that Member States should update their laws to prevent criminal misuse of these new technologies as well as ensuring cooperation between Member States and their law enforcement agencies in the prosecution of those that commit cyber crimes. That Member States legal systems should also be updated to ensure the safety and protection of data that may be breached.

Another resolution enacted by the UN is Resolution 57/239 that was passed in January 2003. This resolution calls for the creation of a global culture of cybersecurity. In its call for the creation of a global culture, the UN, in this resolution, recalls previous resolutions such as Res. 55/63. It also notes the growing dependence on information technologies and that with increased usage of these technologies there must be an increase in cybersecurity provided, that effective cybersecurity isn't guaranteed by governments or law enforcement, but also through prevention and societal support. That it is pertinent that all parties that use this technology, whether it be governments, organizations, or private owners or users, must be aptly informed of necessary cybersecurity measures to prevent and combat criminal misuse. It acknowledges that gaps in the access to and use of these technologies by Member States can greatly impair the effectiveness of international cooperation in combating criminal activity.

The aforementioned resolution also notates the elements needed to create a global culture of cybersecurity. The resolution labels those that utilize information technologies as "participants." This includes governments, businesses, other organizations, and individuals. It highlights that participants should be aware of the need for security, that they are responsible for the security of their systems, and that they should respond in a timely manner to prevent, detect security incidents. It also stressed that participants should act in a manner that is ethical and should routinely conduct risk assessments to their systems. That they must design and implement, as well as manage the security used in their systems. Participants should also assess the security of their systems as well. Ultimately though, security should be implemented in a manner that is in accordance with democratic principles.

Resolution 58/199 passed by the UN General Assembly (UNGA) in March 2010 was adopted to create a global culture of cybersecurity and to protect critical information infrastructures. This resolution recognizes the newfound reliance of information technologies in business sectors such as the generation, transmission, and distribution of energy, or banking and financial services, to name a few. It acknowledges that for the effective protection of systems there is a required communication and cooperation nationally and internationally amongst all parties that are involved. The resolution highlights the elements needed to protect the critical information infrastructures of those it concerns. Such elements include having emergency warning systems to alert one of cyber threats. Raise awareness to help those involved in their understanding of these infrastructures and the role each plays. Examine the infrastructures and identify any dependencies to help enhance their protection. Promote partnership, both public and private, to share and analyze these systems to prevent, investigate and respond to damage or attacks on such infrastructures. Carry out the training and exercises necessary to enhance the response capabilities as well as have adequate substantive and procedural laws and trained personnel to enable Member States the ability to investigate and prosecute attacks on critical information.

Regional and International Framework

The Association of Southeast Asian Nations (ASEAN) has developed a regional framework for its Member States to use since 2016. The framework though must be adequate to the risks posed by the acceleration in digitalization, escalating cybercrime, and the growing geopolitical tensions. It also must be adequate to implement UN recommended norms that ASEAN has expressed it intends to do. Cyberthreats have increased in Southeast Asia in quantity and sophistication in the past 10 years. This is driven by a number of factors such as the COVID-19 pandemic, the adoption of advanced technologies, and the growing status of Southeast Asia being the target of cyber espionage attacks due to its geopolitical significance. There is a high level of cooperation among members of computer emergency response teams (CERTs) and has moved to formalize existing CERT cooperation. In the past five years there has been an open dialogue among partners, international organizations, and the private sector to establish an enhancement of regional cybersecurity and to strengthen the trust between Member States. Notably, Singapore and Malaysia have played critical roles in leading initiatives and mechanisms in the financial and defense sectors. For example, the Central Bank of Malaysia has led members to establish the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP). The platform aims to allow banks to share cyber threat intelligence and develop collaborative mitigating actions. The Monetary Authority of Singapore has collaborated with the Financial Services Information Sharing and Analysis Center (an outside, third party organization with a goal to increase cybersecurity) to establish the Asia Pacific Regional Intelligence and Analysis Center. The Center has the goal to offer support to regional finance institutions in areas including the threat to intelligence, mitigation of such threats, and technical-skills development to combat possible threats. It already has participation from Malaysia, Singapore, and Thailand.

The Economic Community of West African States (ECOWAS) has passed legislation that suggests to Member States to adopt and update at least every five years a national cybersecurity and cybercrime policy and strategy. Policies and strategies should include monitoring and evaluation mechanisms to enhance them. It also tells Member States to establish a national cybersecurity authority that should have all the necessary powers to overlook all critical information intelligence sectors. ECOWAS asks its members to establish a system that alerts of any incidents and to increase response capabilities as well as implenting a risk management approach, both on the strategic level and within private and public bodies. Member States should ensure the necessary support to its cybersecurity team that their assessments and recommendations would be considered by decision makers and that this team would be a developed, qualified human workforce trained in different aspects of cybersecurity. There would be a prioritization of cybersecurity for critical infrastructure and essential services. That Member States would adopt necessary penal, procedural provisions, and proportional sanctions for the criminal offenses that have or would affect the information and data system. Member States are asked to ensure national cooperation and promote regional and international cooperation. That Member States will collaborate to establish a regional assistance plan for the implementation of a regional strategy, that said strategy would include a monitoring system and coordination center. It also asks Member States to ensure the proper funding necessary to include cybersecurity in its systems.

The Nordic Council has announced its desire to establish a coordinated, joint cybersecurity strategy that has been accelerated due to the Russian Invasion of Ukraine. Since the conflict started there has been an increase in the number of cyber attacks experienced by Nordic industries and military. Such attacks include those against the Swedish and Danish Defense departments. The Nordic Council established the Nordic Defense Cooperation (NORDEFCO) and charged it with cross border Nordic cybersecurity collaborative solutions. NORDEFCO has expressed that in the long term its military influenced strategy has the goal of enhancing intelligence sharing between Member States. Individual members have increased the funding in their military budgets to enhance cybersecurity efforts, such as Sweden's $130 million budget and Finland's $80 million. Iceland has launched a national cybersecurity development strategy that includes joint exercises with its Nordic partners to test defensive and offensive cyberthreat solutions that began in 2022 and will continue until 2037.

Conclusion

Ultimately, it is no secret that we are seeing our world, our civilization growing more and more interconnected. Whether it's through our governments making agreements, or through more accessible internet connections, it can not be ignored. With that being said it is also our job, as the population of our world, to ensure the safety, protection, and security of our most valuable data. We are seeing more often than not the use of the very systems we rely on against us. We see our information technologies used to harm us during times of war and we use it to harm others in time of war. All of us, no matter our position, must recognize the importance of cybersecurity to protect the world's most vulnerable. We have seen the increased quantity of cybercrimes across the globe due to the increased accessibility as a response to the COVID-19 pandemic. The UN itself has taken actions towards making these technologies and our critical information infrastructure safer to use and access. Other international organizations have began the negotiations and opened the conversations needed to create inclusive systems to protect one another. It is up to you, the delegates of the United Nations, to continue these conversations when times get tough and to find common ground to pass resolutions to ensure the safety of not just everyone today, but of everyone tomorrow!

Topic II: Regulating Emerging Technologies and Weapons Proliferation

Introduction

In recent years, the rise of computing power and larger datasets have led to the trend of countries like China, Australia, The United States and The Russian Federation acquiring *advanced weapons systems* (AWS) such as MAHEM The Magneto Hydrodynamic Explosive Munition and hypersonic glide vehicles. These systems are equipped with emerging technologies such as artificial intelligence/machine learning or robotics, which significantly enhance the potency of *advanced conventional weapons* (ACW) systems. These advancements have enabled machines to execute tasks that were previously exclusive to humans. However, concerns have surfaced regarding the use of deadly autonomous weapons, and it has become necessary to create a platform where these issues can be deliberated and resolved.

It is worth noting that the production of hardware equipment, materials, and components for various systems can be carried out either locally or through importation. The recent wave of technological breakthroughs in Artificial Intelligence (AI), drones, or genetic engineering (CRISPR/Cas) has captured the attention of the global community. These advancements have led to a renewed interest in the ability of humanity to secure its own survival through the development of commonly agreed rules and regulations that govern the use of these technologies. This is especially important as the potential for misuse of these technologies can have disastrous consequences for humanity and the planet as a whole, cyber attacks can manipulate information and compromise decision-making, leading to the launch of nuclear weapons and interfering with their operation. The increased use of advanced machine learning in defense systems can accelerate warfare, leaving decision makers with little time to consider the consequences of launching nuclear weapons. Therefore, proper regulations must be put in place to ensure that these technologies are used for the greater good of humanity.

Current Situation

China has developed advanced weapon systems using American chip technology. In a secretive military facility in southwest China, there is a supercomputer simulating the heat and drag on hypersonic vehicles speeding through the atmosphere, capable of launching missiles aimed at a U.S. aircraft carrier or Taiwan, according to former U.S. officials and Western analysts. The creation of weapons like the hypersonic glide vehicle DF-17 poses a real and immediate danger to global security. What is more concerning is how they manufactured it. The computer is powered by tiny chips designed by a firm located in China called Phytium Technology, using American software and built in the world's most advanced chip factory in Taiwan. This puts a spotlight on the need for more stringent regulations and monitoring of technology transfer to countries with known military ambitions.

The *Defense Strategi*c update of 2020 leaves no room for doubt, Australia is ready to shape strategic developments. Recently, the Australian Navy released an update on its strategy to protect the environment and take military action when required. The report emphasizes the importance of maritime capabilities, such as robotics, autonomous systems, and artificial intelligence (RAS-AI). The Navy has established a RAS-AI Directorate with the mandate to develop a strategic roadmap that will guide the development and use of RAS-AI until 2040. The report provides concrete evidence to inform the Navy's RAS-AI Strategy. The RAS-AI has set its sights high - it aims to make AI increasingly pervasive and RAS capabilities increasingly numerous in the future operational environment. Moreover, it seeks to normalize human-machine teaming to create an unbeatable combination.

Actions Taken by the UN

The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW) is an important instrument of international humanitarian law (IHL) and arms control. It was negotiated under United Nations auspices in 1979-1980, and has five Protocols. These include *Protocol I* on Non-Detectable Fragments, *Protocol II* on Prohibitions or Restrictions on the Use of Mines, Booby-Traps, and Other Devices, *Protocol III* on Prohibitions or Restrictions on the Use of Incendiary Weapons, *Protocol IV* on Blinding Laser Weapons, and *Protocol V* on Explosive Remnants of War. The Convention has a modular design that allows new instruments to be added to the framework treaty as humanitarian concerns around weapons systems evolve and new systems emerge.

The CCW effectively facilitated discussions about lethal autonomous weapons systems and provided a flexible platform for states with varying views. All countries with established or emerging capabilities in AI systems are High Contracting Parties to the Convention, including the Russian Federation, the United Kingdom, and the United States. The forum's status as an instrument of International Humanitarian Law (IHL) made it attractive to all those concerned about the potential undermining of IHL principles by autonomous combat systems.

Financial instability is causing uncertainty around some 2017 meetings due to arrears from High Contracting Parties. Industry and technology developers are hesitant to discuss lethal autonomy for fear of being stigmatized. Traditional arms control communities view weapons in material terms, and Hollywood depictions of Ironman and Terminator add to the issue. Nonetheless, the CCW is the best platform to discuss emerging technologies related to lethal autonomous weapons systems (LAWS).

Numerous organizations, such as the Red Cross, UNIDIR, think tanks and NGOs, have played a crucial role in advancing the conversation around autonomous weapons systems. They have held expert meetings on technical, military, legal, and humanitarian aspects of this issue. The CCW in

Geneva hosted an Informal Meeting of Experts, where the complex issue was discussed covering several aspects including humanitarian, ethical, military, legal, and techno-commercial elements. The CCW rules allowed a broad range of stakeholders, including civil society, to participate in the discussions. The GGE was formed in Dec 2016 to discuss "autonomous weapons systems". The International Committee of the Red Cross and UNIDIR participated in expert meetings to examine the technical, military, legal, and humanitarian aspects of these systems. UNIDIR created a primer, and think tanks and NGOs, including Amnesty International and the Stockholm International Peace Research Institute, also contributed.

Regional and International Frameworks

The U.S Department of States strategically created the *Bureau of Arms Control, Verification, and Compliance (AVC)*: AVC forms strategies and goals of the U.S. government on arms control aimed at achieving two broad objectives. Firstly, it involves assisting the United States and other nations in negotiating arms control and disarmament treaties. Secondly, it involves building strong relationships with other nations to facilitate the implementation of such treaties. And *Bureau of International Security and Nonproliferation (ISN):* ISN aims to prevent the spread and roll back the proliferation of Weapons of Mass Destruction (WMDs), delivery systems, and advanced conventional weapons capabilities. It tracks, develops, and implements effective responses to proliferation threats and shapes the international security environment to prevent their recurrence.

The North Atlantic Treaty Organization (NATO) created the *Alliance Policy Framework on Proliferation of Weapons of Mass Destruction:* The UN Security Council declared that the spread of weapons of mass destruction (WMD) was a threat to international peace and security. NATO recognized this issue and directed its members to develop a policy framework to prevent the proliferation of WMD and ballistic missiles. NATO aims to prevent the spread of weapons of mass destruction (WMD) through diplomatic means. The Allies will evaluate the risk of WMD proliferation, hold regular consultations on WMD proliferation threats, and explore ways to strengthen international arms control and non-proliferation norms. They will also support efforts to increase participation in international non-proliferation forums and activities, share information on dismantling nuclear weapons in the former Soviet Union, and consider relevant initiatives to support non-proliferation objectives. The Allies will consult with NACC and PfP Partners to foster a mutual understanding and approach to the WMD proliferation issue, considering efforts in this field in other forums.

Conclusion

Arms control has been an effective tool to regulate certain types of weapons, but the system is now facing major violations, suspensions, and withdrawals. The rapid pace of technological change is disrupting the regimes in three key ways.

Advanced nations and those who aspire to be are pushing the rate of development of new innovations. New technologies are emerging too quickly for the working group members, who are usually a combination of technologists and diplomats, to keep control lists up to date with emerging threats. Moreover, existing weapons, platforms, and systems' underlying technologies, from their schematics to the software that runs them, are being digitized, and newer technologies are emerging in digital formats that circumvent existing regulation. Finally, accelerated innovation and digitization are contributing to the digital diffusion of technologies that augment the risk of proliferation and enable states to maintain latent military capabilities. Existing arms control regimes are failing to adapt to these technological shifts. To strengthen the existing nonproliferation architecture from the bottom up, states must muster the political will to address the challenges and meet the moment.

References

The Role of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. December 2018, Nos. 3 & 4 Vol. LV, "New Technologies: Where To?
https://www.un.org/en/un-chronicle/role-united-nations-addressing-emerging-technologies-area-lethal-autonomous-weapons
Carnegie Endowment for International Peace “Can We Still Regulate Emerging Technologies?” May 09, 2019, Valdai Club.
https://carnegieendowment.org/2019/05/09/can-we-still-regulate-emerging-technologies-pub-79125
U.S Department Of State: Arms and Nonproliferation. Apr 4, 2023.
https://www.state.gov/policy-issues/arms-control-and-nonproliferation/
LawFare: “How Emerging Technology is Breaking Arms Control?” April 24, 2022.
https://www.lawfaremedia.org/article/how-emerging-technology-breaking-arms-control
North Atlantic Treaty Organization: “Alliance Policy Framework on Proliferation of Weapons of Mass Destruction” November 2008.
https://www.nato.int/cps/en/natohq/official_texts_24450.

ECOWAS regional cybersecurity and cybercrime strategy - OCWAR-C. (n.d.).
https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf

FBI. (2023, March 22). Internet crime complaint center releases 2022 statistics. FBI.
https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

Iiss. (n.d.). ASEAN cyber-security cooperation: Towards a regional emergency-response framework. IISS.

https://www.iiss.org/en/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/

Information security special interest group. CEB. (n.d.). https://unsceb.org/topics/cybersecurity

O’Dwyer, G. (2023, March 27). Nordic Council seeks deeper regional cybersecurity cooperation. Defense News. https://www.defensenews.com/global/europe/2023/01/17/nordic-states-to-develop-common-cybersecurity-strategy/

The Statistics Portal. Statista. (n.d.). https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#insights

Un resolutions. ITU. (n.d.). https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx