Topic A: Addressing the Threat of State-Sponsored Cyberwarfare

Introduction

State-sponsored cyberwarfare has emerged as an urgent international security challenge that undermines the integrity of critical infrastructure, democratic institutions, and public trust. Unlike traditional kinetic conflict, cyber operations can target power grids, electoral systems, and financial networks with little visibility or immediate physical damage, making them difficult to deter and attribute. Recent high-level discussions at the United Nations Security Council have highlighted how malicious cyberactivity, including ransomware attacks and digital intrusions into public institutions, can erode the foundations of peace and stability, disrupt essential services, and fuel geopolitical tensions if left unaddressed.[1]

The existing international framework for responsible behaviour in cyberspace reflects early but significant progress in establishing norms aimed at preventing cyber conflict. The United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have developed a set of voluntary norms that encourage states to respect international law in cyberspace, protect critical infrastructure, and cooperate to prevent malicious activities. These norms, while non-binding, provide a shared basis for reducing risks to international peace and security and form the core of ongoing multilateral dialogue.[2][3] Nevertheless, gaps remain in implementation and accountability, and many states continue to prioritize national security interests over collective commitments, highlighting the need for stronger, more operationalized frameworks that can address the evolving threat landscape.[4]

Addressing state-sponsored cyberwarfare is essential to achieving Sustainable Development Goal 16, which calls for the promotion of peaceful and inclusive societies and the strengthening of effective, accountable institutions.[5] Without robust international norms and mechanisms to deter and respond to cyberattacks on critical systems, states and citizens remain vulnerable to disruptions that can undermine governance, economic stability, and democratic processes. Building consensus on international cyber norms, enhancing cooperation on attribution and

---

[1] United Nations. (2024). *Secretary-General's remarks to the Security Council's High-Level Debate on Addressing Evolving Threats in Cyberspace*. https://www.un.org/sg/en/content/secretary-generals-remarks-the-security-councils-high-level-debate-addressing-evolving-threats-in-cyberspace

[2] United Nations Office for Disarmament Affairs. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report*. United Nations.

[3] United Nations Office for Disarmament Affairs. (2021). *Report of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*. United Nations

[4] ICT4Peace Foundation. (2019). *A Call to Governments: Critical Infrastructure and Offensive Cyber Operations*. https://ict4peace.org/activities/a-call-to-governments-critical-infrastructure-and-offensive-cyber-operations/

[5] United Nations Department of Economic and Social Affairs. (n.d.). *Sustainable Development Goal 16*. https://sdgs.un.org/goals/goal16

response, and integrating cyber considerations into broader peace and security efforts will be crucial steps for the international community to ensure that cyberspace contributes to peace, justice, and strong institutions rather than conflict and mistrust.

Current Situation

State-sponsored and state-enabled cyberattacks are increasingly undermining national security, civic trust, and essential services around the world. Developed nations with advanced digital infrastructures are frequent targets; cyber intrusions into government networks, financial systems, and critical infrastructure can disrupt services and demand costly remediation. For example, Ukraine has faced persistent cyber operations linked to Russian actors targeting power grids, telecommunications, and government agencies, illustrating how sophisticated attacks can hamper a nation's capacity to govern and deliver services.[6] At the same time, even high-income economies like Canada have reported high-profile intrusions into parliamentary systems, signaling that no state is fully immune.[7] Developing robust defenses, incident response mechanisms, and legislative frameworks remains a priority for all states seeking to secure stability and uphold the rule of law.

Developing countries are often more severely impacted by cyber operations due to limited cybersecurity capacity, inadequate incident response infrastructure, and weaker institutional frameworks. A striking example is Costa Rica, where a series of ransomware attacks in 2022 forced the government to declare a national state of emergency after cybercriminal groups targeted more than two dozen public institutions, including the Ministry of Finance, social security systems, and customs databases.[8] These attacks disrupted tax filing, customs operations, healthcare administrative systems, and government digital services for weeks, resulting in significant economic losses and forcing many processes onto manual systems while recovery efforts continued. The incident highlighted how developing nations with nascent cybersecurity ecosystems can suffer profound operational, economic, and social consequences when essential digital systems are targeted.

In recognition of these cross-border risks, the United Nations has played a central role in developing norms and cooperative mechanisms to mitigate malicious cyber activity and support member states' resilience. Negotiations within the Open-Ended Working Group (OEWG) on ICT security and related UN processes have led to a set of voluntary norms encouraging states to protect critical infrastructure, respect international law in cyberspace, and enhance transparency

[6] United Nations. (2024). *Digital breakthroughs must serve betterment of people, planet, speakers tell Security Council during day-long debate on evolving cyberspace threats*. UN Press. https://press.un.org/en/2024/sc15738.doc.htm
[7] United Nations Digital Watch Observatory. (2025). *UN OEWG and GGE processes on ICT security*. https://wp.dig.watch/processes/un-gge
[8] World Bank. (2025). *Enhancing cyber resilience in developing countries*. https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

and confidence-building measures.[9] The UN also supports capacity-building initiatives, such as workshops on protecting critical infrastructure in nations like Mongolia, which bring technical expertise and collaborative frameworks to help states improve detection, response, and governance in the face of cyber threats.[10] UN-affiliated alliances like the International Multilateral Partnership Against Cyber Threats (IMPACT) further unite governments, academia, and private sectors to strengthen global cyber defense capabilities.[11]

Non-governmental organizations complement these efforts by advocating inclusive norms, documenting harms, and promoting human-centric approaches to cybersecurity. Groups such as the CyberPeace Institute engage with multilateral forums to quantify impacts on civilian systems and promote accountability and resilience.[12] Similarly, digital-rights NGOs emphasize protection of fundamental rights, data privacy, and equitable access to cybersecurity resources.[13] Despite advancing frameworks and cooperative programs, significant challenges remain: many UN norms are non-binding, capacity disparities persist between states, and enforcement mechanisms are limited. Strengthening multilateral cooperation, expanding technical assistance, and supporting legal and institutional capacity in vulnerable states will be critical to mitigating cyber threats and advancing the goals of SDG 16, particularly by fostering peaceful, just, and inclusive institutions resilient to the evolving landscape of digital conflict.

Conclusion

In today's interconnected world, cybersecurity is a key component of national and international security. Cyberattacks can disrupt essential services, undermine public trust, and threaten state legitimacy, making resilience a top priority for all Member States. Addressing these threats requires not only technological defenses but also robust legal frameworks, institutional capacity, and international cooperation.

The international community plays a vital role in providing guidance, capacity-building, and shared standards through UN initiatives, multilateral partnerships, and public-private collaboration. Voluntary norms, such as those from the OEWG, offer valuable guidance, but states must actively engage in cooperation to strengthen enforcement, transparency, and accountability in cyberspace.

---

[9] United Nations Office for Disarmament Affairs. (2022). *UN norms of responsible state behaviour in cyberspace*. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[10] United Nations Office of Counter-Terrorism. (2021). *Protecting national critical infrastructure from terrorists' cyber-attacks in Mongolia*. https://www.un.org/counterterrorism/fr/node/19016

[11] International Multilateral Partnership Against Cyber Threats (IMPACT). (n.d.). *IMPACT Global Headquarters*. https://impact-alliance.org/

[12] CyberPeace Institute. (2025). *Advancing cyber framework norms*. https://cyberpeaceinstitute.org/news/eighth-statement-oewg/

[13] ICT4Peace Foundation. (2023). *Cybersecurity and human rights in international norms*. https://ict4peace.org/cybersecurity-human-rights-international-norms/

Policy recommendations include enhancing multilateral cyber defense frameworks, providing technical support to vulnerable states, securing critical infrastructure, and investing in cybersecurity education and public awareness. By taking these steps, Member States can reduce risks, protect citizens, and ensure that digital infrastructure contributes to sustainable development, stability, and resilient governance.

Questions to Address

1. What practical measures can the UN and member states take to strengthen the enforcement of international cyber norms and protect critical infrastructure globally?
2. How can developing countries build cybersecurity capacity and resilience without compromising sovereignty or increasing dependence on foreign technologies?
3. In what ways can states, NGOs, and international organizations collaborate to ensure cyber defense strategies protect civilians, uphold human rights, and maintain trust in democratic institutions?

Topic B: The Proliferation and Regulation of Lethal Autonomous Weapons Systems(LAWS)

Introduction

The rapid development of Lethal Autonomous Weapons Systems (LAWS), AI-driven technologies capable of selecting and engaging targets without meaningful human intervention, poses profound challenges to international peace, security, and the ethical conduct of warfare. Unlike traditional weaponry, LAWS could make life-and-death decisions autonomously, risking violations of international humanitarian law and eroding human accountability on the battlefield. These concerns have been underscored in ongoing United Nations discussions, where the Secretary-General has described machines that can take human lives without human control as "politically unacceptable" and "morally repugnant," calling for a legally binding prohibition or regulation to prevent delegation of lethal force to machines.[14] In the absence of clear norms, unchecked proliferation of LAWS could undermine both the legal frameworks that govern armed conflict and the foundations of human dignity, threatening the realization of Sustainable Development Goal 16, which seeks to foster peaceful, just, and inclusive societies.

Multilateral efforts to address LAWS are centered within the United Nations Convention on Certain Conventional Weapons (CCW), a framework historically used to regulate or ban weapons considered excessively injurious or indiscriminate. While the CCW has facilitated

[14] United Nations. (2025, May 14). *'Politically unacceptable, morally repugnant': UN chief calls for global ban on 'killer robots'*. United Nations Office at Geneva. https://www.ungeneva.org/en/news-media/news/2025/05/106320/politically-unacceptable-morally-repugnant-un-chief-calls-global-ban

technical dialogue on the risks and regulatory options regarding autonomous weapons, no consensus has been reached on binding controls, in part due to divergent state interests and the complexity of defining autonomy in weapon systems.[15] [16] The CCW's Group of Governmental Experts on emerging technologies in the LAWS area continues to explore normative and operational elements for potential regulation, yet progress has been slow and voluntary norms remain the primary output.[17] This impasse has highlighted gaps between humanitarian principles, such as distinction and proportionality, and the realities of AI-driven systems that may not reliably adhere to those norms without robust human oversight.

Civil society and human rights organizations have been at the forefront of advocacy for stronger international action, arguing that autonomous weapons systems lacking meaningful human control pose unacceptable humanitarian and ethical risks. The Campaign to Stop Killer Robots, a coalition of NGOs including Human Rights Watch, the International Committee for Robot Arms Control, and Amnesty International, calls for a new treaty to prohibit fully autonomous weapons and ensure compliance with international humanitarian law.[18] [19] Their advocacy was echoed at a 2025 UN General Assembly meeting attended by nearly 100 countries, where many states expressed alarm at the prospect of machines making autonomous lethal decisions and urged negotiations toward a legally binding instrument.[20] As technological advances accelerate and LAWS become more feasible and affordable, establishing clear international norms, whether through prohibition or a strict code of conduct with guaranteed human control, will be essential to uphold accountability, protect civilians, and reinforce the rule of law in the conduct of armed conflict.

Current Situation

The proliferation of Lethal Autonomous Weapons Systems (LAWS) is already influencing how states conduct and prepare for modern conflict, with tangible effects on both national security and ethical norms and has increasingly raised international concern regarding civilian protection and legal accountability. In active conflict zones, semi-autonomous and autonomous systems

---

[15] United Nations Office for Disarmament Affairs. (n.d.). *Lethal Autonomous Weapon Systems (LAWS)*. UNODA. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/

[16] United Nations Digital Watch Observatory. (2025). *Convention on Certain Conventional Weapons – Group of Governmental Experts on LAWS*. https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024

[17] Arms Control Association. (2024, June). *Strong support at conference for 'killer robot' regulation*. https://www.armscontrol.org/act/2024-06/news/strong-support-conference-killer-robot-regulation

[18] Human Rights Watch. (2025, May 21). *UN starts talks on treaty to ban 'killer robots'*. https://www.hrw.org/news/2025/05/21/un-start-talks-treaty-ban-killer-robots

[19] Human Rights Watch. (2019, March 27). *Statement on options for future work by the Campaign to Stop Killer Robots*. https://www.hrw.org/news/2019/03/27/statement-options-future-work-campaign-stop-killer-robots-ccw

[20] Human Rights Watch. (2025, May 21). *UN start talks on treaty ban killer robots* (summarized—includes report on UN General Assembly meeting). https://www.hrw.org/news/2025/05/21/un-start-talks-treaty-ban-killer-robots

have been deployed with increasing frequency. For example, Russia has utilized large numbers of Veter "kamikaze" drones in Ukraine, capable of independently searching for and engaging targets, raising concerns about escalation and civilian harm in an environment where clear international oversight is lacking.[21] These deployments also demonstrate the erosion of traditional command responsibility in warfare. Ukraine, meanwhile, has relied on semi-autonomous drones for defensive operations, illustrating how even states under attack are integrating AI-enabled weapons into their military strategies.[22] These real-world deployments demonstrate that autonomous weapon technologies are not theoretical; they are shaping battlefield dynamics and complicating traditional concepts of command responsibility, civilian protection, and accountability under international law.

The United Nations has taken multiple steps to address these emerging risks, though progress remains challenging. In 2025, the UN Secretary-General publicly described LAWS as "politically unacceptable" and "morally repugnant," calling for a global ban on systems that can take human life without direct human control and advocating for a legally binding treaty to regulate or prohibit their use.[23] A UN General Assembly resolution in late 2024, supported by more than 120 Member States, mandates negotiations toward such a treaty, with debates focusing on ensuring "meaningful human control" over weapon systems and preventing accountability gaps where no clear human agent can be held responsible for violations of humanitarian or human rights law.[24] These multilateral efforts are centered on the Convention on Certain Conventional Weapons (CCW), where states continue to discuss the legal, ethical, and operational frameworks needed to regulate autonomous weapons, though no binding agreement has yet been achieved.

Non-governmental organizations play a critical role in shaping international discourse on LAWS and advocating for stronger action. The Campaign to Stop Killer Robots, coordinated by NGOs including Human Rights Watch and Amnesty International, brings together civil society voices from more than 70 countries to push for a treaty banning fully autonomous weapon systems and to ensure that human rights, humanitarian principles, and ethical norms are integrated into any regulatory framework.[25] These NGOs also provide technical, legal, and policy guidance to states during CCW discussions. NGOs highlight the risks of delegating life-and-death decisions to

---

[21] Global Education News. (2025). *Regulating autonomous weapons: UN efforts and global challenges in 2025*. https:/x/globaleducationnews.org/regulating-autonomous-weapons-un-efforts-and-global-challenges-in-2025/

[22] Global Education News. (2025). *Regulating autonomous weapons*.

[23] United Nations Office at Geneva. (2025, May 14). *'Politically unacceptable, morally repugnant': UN chief calls for global ban on 'killer robots'*. https://www.ungeneva.org/en/news-media/news/2025/05/106320/politically-unacceptable-morally-repugnant-un-chief-calls-global-ban

[24] Human Rights Watch. (2025, May 21). *UN starts talks on treaty to ban 'killer robots'*. https://www.hrw.org/news/2025/05/21/un-start-talks-treaty-ban-killer-robots

[25] Human Rights Watch. (2025). *UN treaty talks on killer robots*.

machines and provide technical, legal, and civil society perspectives in UN forums and public debates, urging states to prioritize civilian protection and accountability.[26] Despite these efforts, gaps in consensus—especially among major military powers that resist binding restrictions—mean that continued advocacy, diplomatic engagement, and cooperative norm-building will be necessary to address the rapidly evolving threat landscape and support the objectives of Sustainable Development Goal 16 on peace, justice, and strong institutions. Member States must also integrate these discussions into national defense policies and AI governance frameworks.

Conclusion

The rise of LAWS represents a significant shift in modern warfare, raising ethical, legal, and strategic challenges. Autonomous drones in Ukraine demonstrate how these technologies enhance military capabilities while complicating accountability, civilian protection, and compliance with international humanitarian law.

UN-led initiatives under the Convention on Certain Conventional Weapons (CCW) and advocacy by NGOs such as the Campaign to Stop Killer Robots have established norms emphasizing "meaningful human control" and ethical oversight. Yet, disagreement among major military powers and the lack of binding treaties leave governance gaps and persistent risks.

Moving forward, the international community should pursue legally binding frameworks that ensure human oversight, establish liability standards, and promote transparency in autonomous weapons development. Complementary capacity-building efforts for developing states and multilateral dialogue can help mitigate risks, uphold humanitarian principles, and support responsible technological advancement in armed conflict.

Questions to Address

1. How can the international community establish legally binding frameworks or enforceable norms to ensure meaningful human control over LAWS, while balancing national security interests?
2. How can states ensure that the deployment of LAWS complies with international humanitarian law, minimizes civilian harm, and maintains accountability, especially in active conflict zones where attribution and oversight are difficult?
3. What policies and mechanisms can states adopt to regulate the development, testing, and transfer of LAWS to ensure transparency, ethical compliance, and global stability?

[26] Human Rights Watch. (2020). *Stopping Killer Robots: Country Positions on banning fully autonomous weapons and retaining human control*. https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

4. How can civil society, NGOs, and international advocacy campaigns contribute to shaping ethical norms, public awareness, and regulatory frameworks for LAWS?