Disarmament and International Security Committee (DISEC) Background Guide

Cleveland Council on WORLD AFFAIRS

CWRUMUN

Disarmament and International Security Committee (DISEC) Background Guide

Written by: *Dhruv Raman, Case Western Reserve University*

Written December 2024

The Disarmament and International Security Committee (DISEC), officially the First Committee of the United Nations General Assembly, addresses the critical issues of global peace and stability, with a focus on disarmament and threats to international security.[1] Established in 1945 with the rest of the UN General Assembly, DISEC has played an important role in shaping international law guiding emerging fields of conflict.[2] Though DISEC resolutions are non-binding, they often lay the groundwork for future treaties and agreements that shape global security policy.

Topic I: Addressing State-Sponsored Cyber Warfare

Statement of the Issue:

State-sponsored cyber warfare refers to the use of cyber operations by governments or their proxies, generally hacking collectives, to achieve strategic objectives that often advance their nation's global standings but undermine international peace. These activities are diverse, ranging from espionage and intellectual property theft to highly destructive attacks on critical infrastructure like power grids, oil and gas pipelines, defense facilities, and financial institutions. Recently, state-sponsored actors have also used cyber operations to spread misinformation and manipulate public opinion via disinformation campaigns.[3]

The clandestine nature of cyberwarfare complicates potential international responses. Unlike conventional military action, cyberattacks are, by nature, extremely difficult to attribute

[1] United Nations "Disarmament and International Security (First Committee)"
[2] Kurtas, "Research Guides: UN Documentation: General Assembly: Main Committees."
[3] FBI, "RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS."

to a nation state or organization. This allows states to convincingly deny involvement, which they generally do either by erasing digital fingerprints or by subcontracting to intermediaries to conduct operations on their behalf.[4] This ambiguity challenges the concept of international accountability and complicates enforcement actions. Meanwhile, the relative novelty of cyberwarfare, and by extension, the lack of international regulation governing state behavior in cyber spaces, has led to cyber operations being treated as a legitimate extension of state sovereignty.

There are numerous ethical issues associated with cyberwarfare. Cyberattacks often target civilian infrastructure like hospitals, power grids, and banks, in addition to traditional military targets. The exploitation of these systems can have an immense financial and social cost on the targeted population.

History:

The roots of state-sponsored cyber warfare can be traced back to the early 2000s, when governments around the world realized how valuable cyberspace was as a strategic domain. When it was established, the internet served as a tool of communication and information sharing. However, by the late 1990s and early 2000s, the internet and other digital tools began to be incorporated into critical infrastructure, both in the defense and civilian sectors, revealing significant vulnerabilities that could be exploited by malicious actors. Governments quickly realized that cyberspace offered a new battlefield, one where strategic operations could be conducted covertly, economically, and with plausible deniability. These characteristics made cyber warfare an attractive tool for advancing strategic objectives without the traditional risks that come with conventional military conflict.

One of the first significant demonstrations of state-sponsored cyber warfare occurred in Estonia in 2007. A dispute between Estonia and Russia over the relocation of a Soviet-era war memorial escalated into a series of distributed denial-of-service (DDoS) attacks that crippled

[4] NATO, “Cyberwar - does it exist?”

Estonian government websites, banks, media outlets, and other critical services.[5] Though never officially attributed to Russia, the scale and coordination of the attacks suggested state involvement or support. This event highlighted that even technologically advanced nations have cyber vulnerabilities and underscored the diverse utility of cyber operations.

In 2010, the word "cyberweapon" became widely used after Iran's nuclear program was attacked by a sophisticated worm. This worm, dubbed "Stuxnet," sabotaged centrifuges at the Natanz nuclear plant (setting Iran's nuclear ambitions back by years), and was the largest and most complex piece of malware developed to that day. It exploited numerous flaws in commercial software systems, the scale of which had never been accomplished before. Because of this, cybersecurity experts widely believed that this was the work of state actors, most likely the United States and Israel, although neither nation has ever publicly taken responsibility.[6] Stuxnet opened the floodgates of full-fledged cyber warfare as the international community realized that cyber operations had evolved beyond basic espionage into a domain capable of strategic military strikes.

In subsequent years, state-sponsored cyber operations became more frequent and diverse. By the mid 2010s, cyberattacks targeting civilian infrastructure became more prominent. The 2015 and 2016 cyberattacks on Ukraine's power grid, attributed to Russian state-sponsored groups, caused widespread blackouts, demonstrating the ability of cyber operations to disrupt essential services and spread fear among civilian populations. Similarly, the NotPetya malware attack in 2017, initially aimed at Ukraine, spread globally, affecting companies and institutions in multiple countries.[7] The collateral damage of such operations revealed how interconnected systems could amplify the impact of cyber warfare far beyond the intended target.

Election interference has also become a hallmark of state-sponsored cyber activities, with the 2016 U.S. presidential election serving as a prominent example. Russian actors engaged in hacking, data leaks, and disinformation campaigns to influence public opinion and undermine

---

[5] NATO
[6] Nakashima, "Stuxnet was work of U.S. and Israeli experts, officials say"
[7] Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes"

trust in democratic institutions[8], demonstrating how cyber operations are increasingly used to achieve political objectives.

Most recently, cyberweapons have been used to perpetrate kinetic action. In September 2024, Israeli intelligence agencies transmitted messages to pagers belonging to members of the paramilitary group Hezbollah in Lebanon and Syria, causing them to simultaneously explode.[9] This was the first major use of a cyberweapon (installed in the pagers) to take physical action against an adversary, possibly heralding a new era of cyber warfare.

In response to these growing threats, efforts to address state-sponsored cyber warfare have developed, but progress has been slow. The 2001 Budapest Convention on Cybercrime remains the only binding international treaty on cyber issues, but it primarily addresses criminal activities and lacks provisions for state-sponsored actions.[10] The United Nations has convened groups such as the Group of Governmental Experts (GGE)[11] and the Open-Ended Working Group (OEWG)[12] to discuss responsible state behavior in cyberspace. These efforts have produced some consensus, such as the affirmation that international law applies to cyberspace, but international disagreements have stalled real progress.

Meanwhile, regional initiatives like the European Union's General Data Protection Regulation (GDPR)[13] are localized efforts to establish governance over cyberspace. However, the absence of universal agreement on cyberspace and the lack of enforcement capabilities leave a significant gap in governance, creating an unregulated gray area for bad actors.

Analysis:

[8] FBI
[9] Murphy, Tidy "What we know about the Hezbollah device explosions"
[10] Council of Europe, "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols"
[11] GGE, "Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security"
[12] OEWG, "Final Substantive Report"
[13] European Parliament, "General Data Protection Regulation"

State-sponsored cyber warfare operates within a complex intersection of technological, political, and ethical concerns, each of which presents significant challenges to the international community. Unlike conventional forms of warfare, cyber operations are ambiguous, allowing states to deny responsibility or to act through proxies. This “plausible deniability” erodes trust between nations and complicates efforts to hold states accountable under existing international law.

One of the most pressing challenges is the lack of universally accepted guidelines governing state behavior in cyberspace. While frameworks like the UN GGE have proposed voluntary norms, such as refraining from targeting critical infrastructure, these lack binding authority and enforcement mechanisms. Nations often prioritize their strategic and national security interests, further delaying the establishment of a cohesive regulatory framework, and undermining the potential for collective action to regulate cyber warfare.

The nature of digital infrastructure increases the risks posed by cyber operations. Cyberattacks targeting one nation often have unintended cascading effects on others, as seen in the global impact of malware like NotPetya and to a lesser extent, Stuxnet. In both cases, the malware spread beyond the targeted nation and affected other members of the international community. This amplifies the consequences of cyber warfare, turning localized attacks into global crises that can also have negative effects on the nation that deployed them.

In addition to technical and strategic challenges, cyber warfare raises significant ethical concerns. Civilian infrastructure, including hospitals, banks, and power grids, is frequently targeted by cyberattacks, causing widespread disruption and suffering. The line between military and civilian targets becomes blurred in cyberspace, and the lack of clear distinctions undermines the protections afforded to civilians under international humanitarian law. The lack of regulation around cyber warfare prevents accountability in international arenas when civilians are harmed by these operations.

The rise of cyber warfare also highlights disparities in national cybersecurity capabilities. Wealthier nations, like China, Russia, Israel, and the United States, often have advanced

defenses and response mechanisms, while other nations remain highly vulnerable due to limited resources and expertise. One notable example was the 2016 Bangladesh Bank cyber heist, when the North Korean backed Lazarus Group and its affiliates attempted to steal around 1 billion USD from the central bank of Bangladesh.[14] The hackers were able to perpetrate this attack due to weak cybersecurity infrastructure in Bangladesh, including extremely outdated systems. $81 million was stolen[15], dealing a serious blow to the central bank. Such an incident only highlights the inequality, which exacerbates global security risks.

The private sector plays an increasingly prominent role in cyberspace. Technology companies like Google, Microsoft, Huawei, and Samsung often own and operate the critical infrastructure targeted by cyberattacks and are frequently called upon to assist with defense and recovery efforts. Their involvement complicates the traditional state-centric approach to security and raises questions about the balance of responsibility between public and private entities.

Conclusion:

State sponsored cyber warfare has become a hallmark of 21st century military strategy, and there are no indications it will fade anytime soon. For that reason, guidelines that allow the world to hold states responsible for their actions in cyberspace are incredibly important. DISEC and other UN bodies are vital to regulate cyber attacks against civilian infrastructure in peacetime, determining whether cyber operations are subject to international warfare law, and providing guidelines for what retaliatory measures are acceptable against cyber attacks.

However, the path toward establishing these guidelines is riddled with hardships. Disagreements among major powers about the scope and enforceability of international regulations, combined with the difficulties of attributing cyber attacks to a specific state, make consensus difficult to achieve. The lack of a universally binding framework has left states operating in a legal gray area, where cyber warfare is often viewed as a legitimate extension of statecraft.

[14] CISA, “FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks”
[15] CISA

To address these gaps in regulation, DISEC must encourage collaboration among UN member states to balance national sovereignty with collective security in cyberspace. This includes creating agreements on the protection of civilian infrastructure, developing mechanisms for transparent attribution, and promoting accountability for violations of established norms. Furthermore, the committee must consider the unique challenges faced by developing nations, which often lack the resources to defend against sophisticated cyber threats, and discuss integrating these efforts to increase these resources into its resolutions.

Delegates must approach this issue with a focus on pragmatism and inclusivity, recognizing the diverse interests of all actors involved. Crafting solutions that are enforceable, equitable, and adaptable to the rapidly evolving nature of cyber technologies will be essential to maintaining international peace and security in the digital age. The actions taken in this committee could lay the groundwork for a safer and more cooperative cyberspace for years to come.

Questions to Consider:

1. How can nations be held accountable for actions done in cyberspace?

2. What kind of civilian infrastructure in your country is vulnerable to cyberattacks?

3. How does your nation engage, either openly or discretely, in cyberwarfare?

References:

United Nations. “Disarmament and International Security (First Committee)”
United Nations, n.d.
https://www.un.org/en/ga/first/.

Kurtas, Susan. “Research Guides: UN Documentation: General Assembly: Main Committees.”
UN General Assembly Documentation, n.d.
https://research.un.org/en/docs/ga/committees.

North Atlantic Treaty Organization. “Cyberwar - does it exist?”
NATO Review, n.d.
https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.

Federal Bureau of Investigation. “RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS.”
FBI, n.d.
https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

Nakashima, Ellen. “Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes.”
Washington Post, 13 January 2018
https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Nakashima, Ellen. “Stuxnet was work of U.S. and Israeli experts, officials say.”
Washington Post, 8 September 2015
https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Murphy, Matt, and Joe Tidy. “What we know about the Hezbollah device explosions.”

BBC, 20 September 2024
https://www.bbc.com/news/articles/cz04m913m49o.

Council of Europe. “The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols.”
Council of Europe, n.d.
https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Group of Governmental Experts. “Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.”
United Nations, December 2019
https://front.un-arm.org/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

Open-ended working group on developments in the field of information and telecommunications in the context of international security. “Final Substantive Report.”
United Nations, 10 March 2021
https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

European Parliament. “General Data Protection Regulation.”
European Union, 27 April 2016
https://gdpr-info.eu/.

Cybersecurity and Infrastructure Security Agency. “FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks.”
CISA, 24 October 2020
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-239a.

Topic II: Regulating the Use of Lethal Autonomous Weapons Systems (LAWS)

Statement of the Issue:

Lethal Autonomous Weapons Systems (LAWS), often referred to as "killer robots," represent a transformative and controversial development in modern warfare. These systems, powered by artificial intelligence, can independently identify, select, and engage targets without direct human intervention. While proponents highlight the potential of LAWS to enhance military efficiency, reduce human casualties among soldiers, and limit collateral damage through precision targeting, their use raises significant ethical, legal, and security concerns.

One of the primary issues surrounding LAWS is the delegation of life-and-death decisions to machines. The lack of human judgment in critical moments of military engagement raises moral questions about accountability. The potential for algorithmic errors or biases in decision-making increases the risk of civilian casualties and violations of international humanitarian law. These risks are particularly alarming in environments where distinguishing between combatants and civilians is inherently complex, especially urban settings.

The lack of an international framework regulating the development and use of LAWS exacerbates these challenges. Current international humanitarian law, while applicable to some extent, was not designed to address the unique nature of autonomous systems. This gap in regulations allows states to develop and deploy LAWS with little to no oversight, creating the potential for a new arms race. Additionally, the proliferation of LAWS increases the likelihood of their misuse by non-state actors or states with a track record for little accountability, further destabilizing global security.

Additionally, the accessibility of these systems to non-state actors or terrorist organizations heightens global instability, particularly in regions already vulnerable to conflict and exploitation. Without clear guidelines, the unchecked development and deployment of LAWS risk eroding existing norms of warfare, undermining human rights, and lowering the threshold for armed conflict. To preserve global security, DISEC must play a central role in

facilitating the dialogue surrounding this issue and ensuring that the deployment of LAWS aligns with the shared values and long-term stability of humanity.

History:

The evolution of Lethal Autonomous Weapons Systems (LAWS) is deeply intertwined with advancements in robotics and artificial intelligence. While fully autonomous systems capable of making independent life-and-death decisions have yet to be widely deployed, many existing or experimental systems demonstrate the trajectory toward their development. These systems range from missile defense technologies to advanced drones, providing both opportunities and challenges for modern warfare.

One of the earliest examples of automated defense systems is the Phalanx Close-In Weapon System (CIWS)[16], used by the United States and several other militaries. Developed in the 1980s, the Phalanx is capable of autonomously detecting, tracking, and engaging incoming missiles or aircraft within its operational range.[17] Although human operators retain oversight, the system's automated features serve as a precursor to fully autonomous weapons.[18]

A more recent development is the deployment of autonomous drones in conflict zones. Recently, the Russo-Ukrainian war has demonstrated the versatility of drones.[19] The Russo-Ukrainian conflict has underscored the trajectory of modern warfare toward increased reliance on autonomous and semi-autonomous systems.[20] These technologies, capable of performing tasks ranging from reconnaissance to direct engagement, are changing the dynamics of conflict by reducing human risk while amplifying precision and operational flexibility.[21] However, the growing complexity of these systems raises critical ethical, legal, and security concerns, particularly as they evolve toward greater autonomy and decreased human oversight.

---

[16] Raytheon, "Phalanx Weapon System"
[17] Raytheon
[18] Raytheon
[19] Reuters, "How drone combat in Ukraine is changing warfare"
[20] Reuters
[21] Returers

The international community, recognizing these challenges, has engaged in discussions on regulating LAWS, primarily under the framework of the United Nations Convention on Certain Conventional Weapons (CCW).[22] Beginning in 2013, the CCW established a Group of Governmental Experts (GGE) to explore the implications of LAWS and to evaluate whether new international regulations are needed.[23] The GGE has emphasized key principles, such as ensuring that autonomous weapons comply with international humanitarian law, including the principles of distinction, proportionality, and military necessity.[24]

While there is widespread agreement on the need for human accountability in the use of force, member states remain divided on how to achieve this. Some nations advocate for a preemptive ban on LAWS, arguing that their deployment would undermine human dignity and violate the moral principles governing armed conflict. Conversely, others, such as the United States, Russia, and China, contend that existing international humanitarian law is sufficient to regulate these systems and that further restrictions could stifle technological innovation and military modernization.

Despite these divisions, there has been progress in identifying common ground. Discussions within the CCW have stressed the importance of maintaining human control over critical functions, particularly those involving the use of lethal force.[25] Furthermore, calls for increased transparency and information-sharing on LAWS development have gained traction, as have proposals for confidence-building measures to reduce the risks of unintended escalation.

The lack of binding agreements remains a significant obstacle, as current UN discussions have yet to produce a comprehensive framework for the regulation of LAWS. Without a clear international consensus, the proliferation and potential misuse of these systems pose a growing threat to global stability.

---

[22] UNODA, “Convention on Certain Conventional Weapons”
[23] GGE, “Convention on Certain Conventional Weapons - Group of Governmental Experts on Lethal Autonomous Weapons Systems”
[24] GGE
[25] UNODA

Analysis:

The advent of Lethal Autonomous Weapons Systems (LAWS) raises a host of challenges, particularly in terms of legal, ethical, and security considerations. While technological advancements in artificial intelligence (AI) and robotics offer military advantages, such as increased efficiency and reduced risk to human soldiers, these systems also introduce significant risks that must be carefully managed. The primary concerns revolve around accountability, ethical implications, the potential for misuse, and the lack of regulation and oversight.

Accountability is the most important issue surrounding LAWS. Traditional ideas of warfare rely on human decision-makers who can be held accountable for their actions in conflict, particularly when violations of international law occur. In the case of autonomous systems, the question arises as to who should be held responsible if a LAWS commits a war crime, such as targeting civilians or engaging in unlawful attacks. If an AI system makes a bad decision or malfunctions, determining accountability becomes challenging. This lack of clarity could potentially erode the credibility of existing international regulations.

Security implications also play a central role in the debate over LAWS. As these systems become more advanced and more widely available, there is a growing concern about their potential proliferation, particularly to non-state actors or rogue states. The ability to deploy autonomous weapons increases the risk of destabilization, as these systems could be used in conflicts that might otherwise have been avoided or de-escalated. Moreover, the ease with which autonomous weapons can be deployed—without the need for human soldiers—could lower the threshold for initiating warfare. This “risk of lowering the threshold for war” could result in more frequent or more widespread conflicts, with countries feeling emboldened to engage in military actions without fear of significant casualties or repercussions.

The lack of a comprehensive international regulatory framework is a significant gap in the current state of LAWS development. Although there have been discussions within the United

Nations, particularly under the Convention on Certain Conventional Weapons (CCW)[26], the divide between states on how to regulate LAWS remains profound. This disagreement hinders the creation of a universal, legally binding framework to govern the development and deployment of these systems.

As such, the role of DISEC in addressing the regulation of LAWS is critical. Delegates must consider comprehensive solutions that integrate military necessity with ethical considerations, creating frameworks that ensure these technologies are used responsibly, are subject to adequate oversight, and comply with international law. At the same time, proposals must account for the rapidly evolving nature of this technology, ensuring that future regulation is adaptable and forward-thinking, rather than reactive.

Conclusion:

The development and potential deployment of Lethal Autonomous Weapons Systems (LAWS) represent one of the most profound challenges to international security, ethics, and law in the modern era. While these technologies promise significant military advantages, such as enhanced precision and reduced human casualties on the battlefield, they also pose serious risks. The possibility of these systems being deployed in a way that undermines international humanitarian law, increases global instability, and lowers the threshold for warfare makes it extremely important for the international community to act quickly.

In the coming years, the decisions made within DISEC and other international bodies will have lasting implications for how autonomous systems are integrated into global military strategy. The committee must ensure that any future regulation of LAWS is grounded in international humanitarian law, incorporates sufficient oversight, and considers the ethical ramifications of giving life-and-death decisions to machines. Only by addressing these challenges can the international community safeguard the principles of humanity and prevent the destabilization of global security.

[26] UNODA

Questions to Consider:

1. Who is responsible for war crimes committed by LAWS?

2. Is your country developing LAWS? How have precursor technologies been incorporated into your country's military doctrine?

3. How could the use of LAWS impact warfare for your country?

References:

United Nations Office for Disarmament Affairs. “The Convention on Certain Conventional Weapons.”
United Nations, n.d.
https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/.

United Nations General Assembly. “Resolution 78/241. Lethal autonomous weapons systems.”
United Nations, 22 December 2023
https://documents.un.org/doc/undoc/gen/n23/431/11/pdf/n2343111.pdf.

United Nations General Assembly First Committee. “General and complete disarmament. Report of the First Committee.”
United Nations, 10 November 2023
https://documents.un.org/doc/undoc/gen/n23/347/86/pdf/n2334786.pdf?OpenElement.

Raytheon. “Phalanx Weapon System”
RTX Corporation, n.d.
https://www.rtx.com/raytheon/what-we-do/sea/phalanx-close-in-weapon-system.

Reuters. “How drone combat in Ukraine is changing warfare.”
Reuters, 26 March 2024
https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

Group of Governmental Experts. “Convention on Certain Conventional Weapons - Group of Governmental Experts on Lethal Autonomous Weapons Systems.”
United Nations, n.d.
https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024.