**Abstract**

This background paper will summarize the need for effective regulation of cyber mercenaries and private entities operating in cyberspace. It will explore the evolving nature of cyber threats and the rising influence of private entities in conducting cyber activities for various purposes, including economic espionage, information warfare, and critical infrastructure attacks. Emphasizing the urgency of addressing this issue, the paper will delve into the advantages and disadvantages of cyber activities by mercenaries and private entities, their history as well as possible solutions.

**Introduction**

The United Nations Disarmament and International Security Committee (DISEC) was created as the first of the Main Committees in the General Assembly when the charter of the United Nations was signed in 1945. the purpose of DISEC is to establish ‘general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments

DISEC faces several modern-day challenges in addressing global security issues. Some of these challenges include the rapid development and deployment of emerging technologies, such as artificial intelligence, autonomous weapons systems, and missile technologies, the proliferation of nuclear weapons and concerns about non-state actors acquiring nuclear capabilities. In order to overcome these challenges, DISEC hopes to strengthen global security, adapt to emerging threats and advance disarmament diplomacy

**Glossary**

**Cyber Mercenary:** companies dedicated to developing, selling, and supporting offensive cyber capabilities which enable their clients to access the networks, computers, phones, or internet connected devices in ways that violate human rights and undermine democratic principles**.**

**Private Entity:** corporation, individual, nonprofit organization, company, or any other organized group that is not government-affiliated.

**Cyberspace:** an electronic system that allows computer users around the world to communicate with each other or to access information for any purpose

**Infrastructure:** the basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise

**espionage:** the practice of spying or of using spies, typically by governments to obtain political and military information

**Diplomacy:** the profession, activity, or skill of managing international relations, typically by a country's representatives abroad

**Proliferation:** rapid increase in the number or amount of something

**Current situation**

The realm of cyberspace is increasingly recognized as a domain marked by conflict and strategic competition among nations. Nevertheless, the creation and maintenance of offensive and intrusive cyber capabilities are expensive, time-consuming, and reliant on specialized skills that many countries lack or find hard to sustain. As a consequence, a new phenomenon has arisen in the form of cyber mercenaries, encompassing private entities willing to develop and supply these capabilities to nations and corporations in exchange for compensation. While the utilization of cyber mercenaries may be tempting for countries seeking to employ such tactics, the unregulated proliferation of this market poses a significant risk of destabilizing the broader online environment over the long term.

**Advantages of cyber mercenaries and private entities in cyberspace:**

| **Innovation:**  |
| --- |

Private sector actors are driven by market competition and innovation. This can

lead to the development of cutting-edge cybersecurity solutions and strategies that may outpace those developed by traditional government entities.

| **Cost-Efficiency:**  |
| --- |

Hiring cyber mercenaries or outsourcing cybersecurity services to private

entities can be cost-effective for nations that may not have the resources to build and maintain a dedicated cybersecurity infrastructure.

**Disadvantages:**

| **Potential for Misuse:**  |
| --- |

Cyber mercenaries may be hired for malicious purposes, such as

conducting cyber espionage or launching attacks on critical infrastructure. This raises ethical and legal concerns regarding the potential misuse of cyber capabilities.

| **Risk of Escalation:**  |
| --- |

Engaging private entities in cyber operations may increase the risk of

escalation in international conflicts. The use of cyber mercenaries by one nation could prompt a response from another, leading to a potentially dangerous escalation in cyberspace.

| **Lack of International Regulation:**  |
| --- |

The absence of comprehensive international regulations

governing the actions of cyber mercenaries creates challenges in holding them accountable for their activities. This can contribute to the uncontrolled proliferation of cyber capabilities.

**Groups affected by the issue**

| **International Relations and Diplomacy:**  |
| --- |

The activities of cyber mercenaries can strain

diplomatic relations between countries. Instances of cyber espionage or attacks carried out by private entities may lead to diplomatic tensions, raising questions about state responsibility and accountability.

| **Global Internet Users:**  |
| --- |

The broader population of internet users may be indirectly affected as

the unregulated expansion of cyber mercenaries could contribute to a less secure online environment. This may lead to increased risks of cyberattacks, data breaches, and compromised personal information.

| **Private Entities:**  |
| --- |

Companies operating in cyberspace may be directly affected by the activities

of cyber mercenaries. They face the risk of being targeted for cyber espionage, intellectual property theft, or other malicious activities that could harm their operations and competitiveness.

**UN involvement**

The United Nations has been actively engaged in establishing cyber norms to promote stability and security in the digital realm. These norms, found in various documents such as the 2015 Group of Governmental Experts (GGE) report, emphasize the importance of responsible state behavior in cyberspace. Key principles include refraining from cyber activities that could harm critical infrastructure or weaken the general functioning of states, respecting the sovereignty of other nations in the digital domain, and preventing the use of information and communication technologies for malicious purposes.

**Agreements/treaties currently in place:**

**Convention on Cybercrime (2001):** this is the first international agreement aimed at reducing computer-related crime by harmonizing national laws, improving investigative techniques, and increasing international cooperation.

**Brief history:**

| Cyber mercenaries, private entities offering cyber capabilities for hire, gradually emerged in the late 20th century as skilled individuals provided hacking and cyber espionage services. Their professionalization occurred in the mid-2000s, expanding to include cybersecurity firms and individual hackers. By the 2010s, the use of cyber mercenaries gained prominence, with reports of nation-states and corporations leveraging private entities for cyber operations. In the present day, the private sector continues to play a significant role in providing cyber capabilities, highlighting the evolving landscape of cyber threats and the need for ongoing regulation and oversight. |
| --- |

**Possible solutions to the issue:**

∙ Develop and implement international agreements and conventions specifically addressing the activities of cyber mercenaries and private entities in cyberspace.

∙ Invest in the development of technologies that enhance cybersecurity resilience and the detection of malicious activities.

| ∙ Invest in educational programs and training initiatives to build a skilled workforce capable of addressing cybersecurity challenges and promote awareness among businesses, governments, and individuals regarding the risks associated with cyber mercenaries and the importance of cybersecurity measures. |
| --- |

**Bibliography**

Microsoft Word - Cyber mercenary principles\_Tech Accord\_3272023 FINAL.docx (cybertechaccord.org)

Mercenary-Related Activities in Cyberspace | CyberPeace Institute

UN experts alarmed by growing use of mercenaries in cyberspace | OHCHR AccessNow.pdf (ohchr.org)

The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf (unoda.org)