KING'S ACADEMY MODEL UNITED NATIONS 2026

The Security Council

PRESIDENT RESEARCH PACKET

President: Ali Lahham

Combating the Use of Cyber Mercenaries in International Conflicts

President's Letter:

Dear Delegates of The Security Council,

It is my utmost pleasure to welcome you to KAMUN'26 .In the Security Council, delegates will face the unique challenge of debating under pressure while adapting to rapidly shifting situations. What makes the SC so special is its AD-HOC debate style, which encourages quick thinking, open exchange, and a dynamic atmosphere that mirrors real-world diplomacy.

I am Ali Lahham, an eleventh grader at King's Academy, and I am honored to serve as this year's President of the Security Council. My passion for MUN was inspired by my aunt, who co-founded the Amman Model United Nations (AMMUN), Jordan's first ever conference and only THIMUN affiliated conference. Her example showed me the power of youth in shaping dialogue, and it has motivated me to grow as a delegate and now as a chair.

The Security Council has always stood out to me because of its intensity and unpredictability. Unlike other committees, where debate is often structured and steady, SC forces delegates to think on their feet, adapt to new crises, and make decisions that can change the course of discussion within minutes. It is where diplomacy meets strategy, and it gathers some of the sharpest minds in MUN, making every session both a challenge and a thrill.

This year, we will be addressing two urgent topics: *"Preventing the Militarization of the Red Sea and Bab El-Mandeb Strait"* and *"Combating the Use of Cyber Mercenaries in International Conflicts."* Both issues highlight how modern conflicts threaten global peace on both physical and digital fronts, and I look forward to seeing how you approach these challenges.

As you prepare for this committee, I leave you with a quote that captures the essence of leadership in difficult times: *"Success is not final, failure is not fatal: it is the courage to continue that counts."* – **Winston Churchill.** I cannot wait to see the solutions you will create when faced with catastrophe.

Best regards,

Ali Lahham

President of The Security Council

Introduction:

Cyber mercenaries have very fast emerged to become one of the most troubling phenomena of contemporary geopolitics because they possess the capability to disrupt states, interfere with economies, and sway conflicts that span

borders. Unlike regular soldiers or private military companies, cyber mercenaries exist in the cyber sphere and are often commissioned by nations, companies, or non-state actors to execute offensive cyber actions. These vary from stealing classified information and knocking out key infrastructure to the creation and dissemination of disinformation amidst political instability. Their actions ignore conventional land borders and hence cyber mercenaries are a multinational threat that directly violates the concepts of sovereignty, security, and international law. The ease of access to advanced cyber tools and the obscurity of the cybersphere has rendered the deployment of these actors an increasingly appealing but perilous weapon in international conflicts.

The principal risk in this region arises from the blurred boundary between the responsibility of the state and the non-state, because governments may surreptitiously hire cyber mercenaries to conduct attacks and deny direct involvement. Such a dynamic propels cyber warfare and produces an environment of suspicion across the world. Cyber mercenaries have been implicated in attacks against power grids and financial centers and against electoral systems and threaten not only the national security of nations but the world economy at large. A number of states have been found guilty of using these actors in order to achieve a form of technological or political ascendancy while other states are unable to defend against them because they lack cyber resilience. In most instances the attackers remain unknown or untraceable and the states are able to eschew accountability under the rules of international law. Competition between great world powers—the United States and China and the Russian Federation—along with the ascent of private groups of hackers for hire has created cyberspace into a disputed domain of power and competition that quickly crosses the threshold into the material world.

Emerging advances in technology and global tensions have increased the necessity of forestalling the normalization of cyber mercenary activity. Ransomware attacks, disinformation operations, and cyber penetrations of government and military networks have risen sharply in the past decade. The increased use of automation and artificial intelligence in cyber operations has enabled the attacks to be executed more quickly, more complexly, and increasingly untraceably, and the danger of unintended escalation between states has increased accordingly. Allegations of mercenary organizations marketing "cyber-attack packages" through the dark web further illuminate the commercialization of cyber warfare. The greater adoption of great powers, not only in defensive cyber postures but in offensive contracting itself, is the harbinger of a situation in which cyberspace becomes the battleground of a protracted proxy conflict unless a global framework is put in place quickly to monitor, control, and punish cyber mercenary activity before it plunges world security into the kind of irreversible instability that would make it impossible to contain the

consequences of cyber war.

Definition of Key Terms:

Cyber mercenaries:
Independent hackers or private groups hired by states, corporations, or non state actors that create offensive cyber operations such as espionage, sabotage, or disinformation campaigns.

Cyber warfare:
The usage of digital attacks by a country or its proxies to disrupt the activities of another state, often targeting critical infrastructure, government networks, or military systems.

Attribution:
The act of identifying who or what is responsible for a cyberattack.

Critical infostructure:
Systems and assets that are crucial to the functioning of a society and economy, such as energy grids, financial networks, communication systems, transportation, and healthcare. Cyber mercenaries often target these to cause maximum disruption.

Ransomware:

Malicious form of cyber malware that freezes or encrypts a victim's information until a ransom is received. Ransomware attacks are frequently conducted by cyber mercenaries in an attempt to amass riches or unseat governments.

Disinformation campaign:

The deliberate spread of false or misleading information online, often during conflicts or elections, to influence public opinion, create division, or undermine trust in institutions.

Proxy warfare:

When states or powerful actors employ cyber mercenaries or hacker groups to carry out attacks on their behalf, avoiding direct confrontation while still achieving political or strategic goals.

Major Parties Involved:

Russia:

Russia has been accused many times of supporting cyber mercenary organizations like APT28 (Fancy Bear) and Sandworm. These players have conducted election interference, misinformation campaigns, and destructive cyberattacks like the Ukraine power grid attacks of 2015–2016. Cyber mercenaries are frequently used by Moscow in order to keep a deniability that is plausible while overseas strategic objectives are pursued.

The People’s Republic of China (PRC):

China has been associated with the APT10 (Stone Panda) and APT41 teams, among others that are described as private contractors who work on behalf of the state. These are experts in intellectual property theft and cyber spying against governments, companies, and NGOs. By using contractors for operations that are outsourced, China is able to achieve economic and strategic objectives but making it more challenging to attribute the actions taken.

Iran:

Iran has counted on cyber-for-hire units like Charming Kitten and APT33 to conduct cyber campaigns. These frequently involve attacks against foreign governments, critical infrastructure, and foreign dissents. The deployment of cyber mercenaries lets Iran exert influence in the region and internationally with limited conventional military force.

North Korea:

North Korea has resorted to cyber mercenary activity as a weapon of statecraft and a source of income under sanctions pressures. The Lazarus Group is suspected of big-ticket attacks such as the Sony Pictures hack (2014) and the WannaCry ransomware epidemic (2017). These activities have been aimed at banks and cryptocurrency exchanges globally and have earned the regime a great deal of money.

israel:

Israel is the headquarters of NSO Group that developed the Pegasus spyware marketed to world governments. Though the nation itself is a cyber power house with Unit 8200 (its best cyber unit), private companies from the nation have been found to be involved in providing the tools that are then misused against journalists, activists, and political opposition figures. Such concerns lead to questions about state control of private offensive cyber companies.

United States Of America (USA):

The US has broad offensive cyber operations under the US Cyber Command and the intelligence communities led by the NSA. While it has not ostensibly used cyber mercenaries like some of its rivals do, Washington has contracted private firms and individuals for cyber operations and has been linked to exploits like Stuxnet that has struck the Iranian nuclear program. The US is also a driver of defining the world cyber norms and of opposition to mercenary acts through sanctions and prosecutions.

Timeline:

2007:

Following Estonia's move to relocate a Soviet war memorial, it came under giant cyberattacks that paralyzed banks, government sites, and media outlets. The attacks

were largely attributed to Russian hackers, and they reflected the ability of states to utilize cyber mercenaries or patriotic hackers in instruments of coercion. It was among the first big events to uncover the destructive capability of cyberspace in interstate conflicts.

2010:

The Stuxnet worm, reportedly jointly created by the United States and Israel, attacked the Natanz nuclear installation in Iran and destroyed its uranium centrifuges. While not a "mercenary" organization per se itself, it proved the concept of using state-associated or contractor-related cyberattack operations to disrupt vital infrastructure could be applied. That date stands as the start of cyber instruments being publicly acknowledged as instruments of warfare.

2013–2015:

Organizations such as APT33 and Charming Kitten conducted cyberattacks against Middle Eastern petroleum firms and American banks. These campaigns, frequently run by Iranian-state contractors, displayed the ability of cyber mercenaries to reconcile criminal hacking with geopolitical aims.

2016:

The cyber gang APT28 (Fancy Bear), associated with the GRU of Russia, was suspected of breaking into Democratic Party emails and circulating disinformation on the internet. Though not directly recognized by Moscow, most experts found them to function as cyber mercenaries at the behest of the state. In this case, it became evident that cyber mercenaries could be utilized in order to disrupt democratic processes globally.

2017:

The global ransomware outbreak, attributed to North Korea’s Lazarus Group, affected over 150 countries, crippling hospitals, banks, and companies. The attack demonstrated how cyber mercenary-style groups could use digital tools for both profit and geopolitical disruption.

2019

The year Investigations discovered that the NSO Group's Pegasus software has been used by many governments to hack into the communications of diplomats, activists, and journalists. The case also highlighted private companies acting as

cyber mercenaries inasmuch as they sell cyber-surveillance systems to governments and non-state actors.

2020:

A wide-scale cyber spying operation that has been linked to Russian state-sponsored hackers breached U.S. government and business networks using tainted software updates. The level of attack sophistication showed the ability of the state-sponsored cyber aggressors to work akin to mercenary armies waging stealth long-term penetration.

2021:

Hackers linked to China's APT Hafnium exploited Microsoft Exchange vulnerabilities, affecting tens of thousands of organizations worldwide. The attack reflected how cyber mercenary groups can cause collateral damage globally while serving geopolitical goals.

2022:

At the onset of the Ukraine-Russian conflict, Ukrainian banks, media channels, and government networks became the subject of cyberattacks (such as wiper malware that comprised the HermeticWiper type). Nation-state groups and cyber mercenaries were suspected of being the architects of the highly synchronized attacks.

2023–2024:

cyber mercenary groups from the Middle East, Eastern Europe, and India offering "cyber-attack services" through the dark web. These included tailored phishing, disinformation-for-hire, and ransomware. Cyber mercenaries' commodification escalated the threat of cyber conflicts growing more frequent and unmanageable.

Implications:

The rise of cyber mercenaries has been gaining worldwide attention because of the power it has to transform present conflicts. Major world powers such as the United States, Russia, and China are highly alarmed that the uncontrolled deployment of cyber mercenaries would let both state and non-state actors exert excessive influence in world politics. The economic consequences are perhaps the most important of them all because cyber attacks against financial establishments, supply chains, and power grids could precipitate long-term turbulence in the world markets, raise expenses for business enterprises, and derail the world economy.

Furthermore, the proliferation of cyber mercenaries is a grave threat to the safety and security of civilians. Attacks against hospitals, water plants, and transportation networks have already proven the very tangible human toll of cyber weaponized activity. The world is alarmed that escalation of cyber mercenaries may lead to blackouts, disruption of critical services, and the creation of humanitarian crises in countries that cannot protect themselves from mass-scale cyber war.

In addition, the increasing commercialization of spyware and hacking tools escalates global concerns. If private enterprises or freelance hackers continue to market offensive cyber capacities on the open or dark internet, immediate escalation is a strong likelihood as governments and companies or radical groups vie for control of the tools. Such a situation would shift the balance of power in the world, create new rivalries, and redefine alignments. Competition for control of cyber instruments has the likelihood of intense digital posturing akin to classic arms races observed in the Cold War era. Security and military tensions continue to be central because history has proven that cyberattacks frequently precede or happen in tandem with conflict in the physical world. The Russian deployment of cyber actions in its Ukraine invasion and the global ransomware campaigns of North Korea confirm that cyber arms could unseat states and economies. Any repetition or escalation of the attacks has the ability to immobilise governments, disable industries and escalate into larger confrontations.

Finally, the most dreaded situation is the increased involvement of more world powers, both Western countries and regional players, using cyber mercenaries to attain strategic objectives. If the situation becomes a continuation of the present situation, cyberspace may turn into a busy battlefield where the rival hacker communities and hired mercenaries wage proxy wars in the name of the hiring nation. Such instability would not only threaten global security but also raise chances of unintended escalation between the opposing nations. Such a situation makes it

necessary for the world to come together in terms of cooperation, regulation, and accountability in order to avert cyberspace from slipping into long-lasting conflict waged by cyber mercenaries.

Proposed Solutions:

1. Developing Strong International and Regional Cybersecurity Partnerships;

b. Evolving the Multilateral Cybersecurity Framework,

i. The establishment of a UN Cyber Security Council of leading countries (U.S., China, Russia, EU, Israel, Iran, N Korea) with observer status to regional organizations (NATO, ASEAN, African Union),

ii. That the Council acts in line with the United Nations Charter principles and the Tallinn Manual in order to hold itself and other actors accountable and to avert state exploitation of cyber mercenaries,

b. Stopping and Tracing Cyber Mercenary Attacks,

i. Sending a UN mandate-bound international cyber attribution mission to monitor and investigate the use of cyber mercenaries in international conflicts,

1. Intelligence sharing between nations and private cybersecurity firms in a quest to identify suspicious cyber activity,

2. Mutual monitoring of darknet markets with the aim of preventing the trade in offensive cyber instruments and services,

ii. Requiring all member states to publicly disclose contracts with private cyber companies developing offensive technologies to avoid secret employment of mercenaries,

c. Developing Cyber Resilience and Protection of Civilians i. Establishing a UN-operated fund to finance susceptible nations in gaining better cyber protection through the inclusion of Computer Emergency Response Teams (CERTs). ii. Coordinating protection and technical assistance measures to prevent civilians, media professionals, and critical infrastructure from cyberattacks by mercenaries,

“Food for Thought”:

.

- Should cyber mercenaries be regarded in the same footing with the traditional mercenaries in the international law of war or are they different?
- How does the global community hold the states accountable for the deployment of cyber mercenaries when attribution of the attacks is often questionable?
- Would the establishment of a UN Cybersecurity Council help limit the sending of cyber mercenaries or just introduce another level of bureaucracy?
- To what degree do cyber mercenaries endanger civilians more compared to state-sponsored cyber activity?
- In what way could increased commercialization of hacking tools in the dark web shift the power dynamic between big and small nations?
- Will sanctions and external pressures actually deter the government from using cyber mercenaries or do they push the activity further into the underground?
- Would creating a UN-led Red Sea Maritime Security Mission reduce tensions, or would it simply add another layer of foreign involvement?
- Is the Red Sea conflict primarily about regional rivalries (Saudi Arabia vs. Iran, UAE vs. Turkey), or has it become part of a larger global power struggle (U.S. vs. China)?

Citations:

Timur, F. B. "Cyber Mercenaries: The Failures of Current Responses." *ORF Online*, Observer Research Foundation, orfonline.org, Accessed 30 Aug. 2025. Razorthorn SecurityORF Online+1

"Cyber Mercenaries: A New Threat to National Security." *UNG Journals – ISSR*, issr.ungjournals.org, Accessed 30 Aug. 2025. International Social Science Review

"The Rise of Cyber-Mercenaries." *HS Centre*, 15 May 2021, hscentre.org, Accessed 30 Aug. 2025. International Social Science Review+6HS Centre+6ORF Online+6

"The New Age of Digital Warfare: What is a Cyber Mercenary?" *Entropiq Cybersecurity*, 18 Mar. 2025, entropiq.com, Accessed 30 Aug. 2025. entropiq.com

"Cyber Mercenaries: The State, Hackers, and Power." *Carnegie Endowment for International Peace*, 18 Jan. 2018, carnegieendowment.org, Accessed 30 Aug. 2025. ORF Online+3Carnegie Endowment+3Razorthorn Security+3

"Cyber Mercenaries: A Call to Action for the Quad." *ORF Online*, 20 Sept. 2023, orfonline.org, Accessed 30 Aug. 2025. ORF Online+1

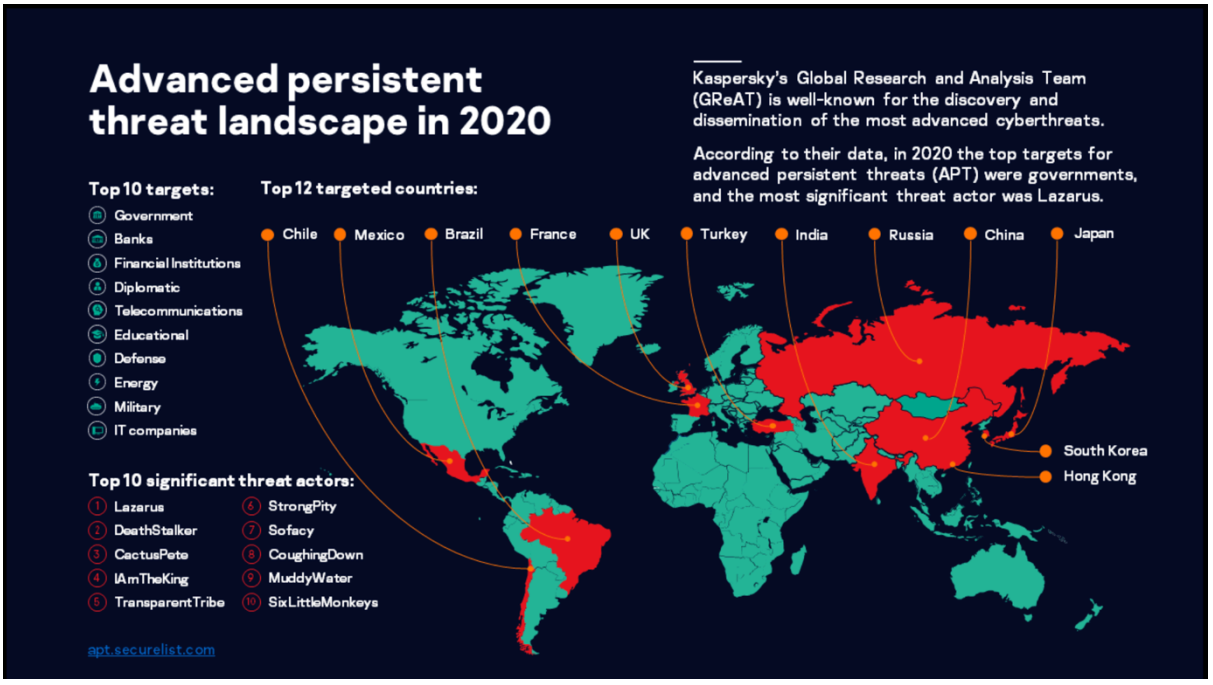
"Tallinn Manual." *Wikipedia*, Wikimedia Foundation, en.wikipedia.org, Accessed 30 Aug. 2025.

Appendix:

Appendix A

"Global Distribution of State-Sponsored Cyber Threat Groups."
Carnegie Endowment for International Peace, *Cyber Mercenaries: The State, Hackers, and Power*, 2018.

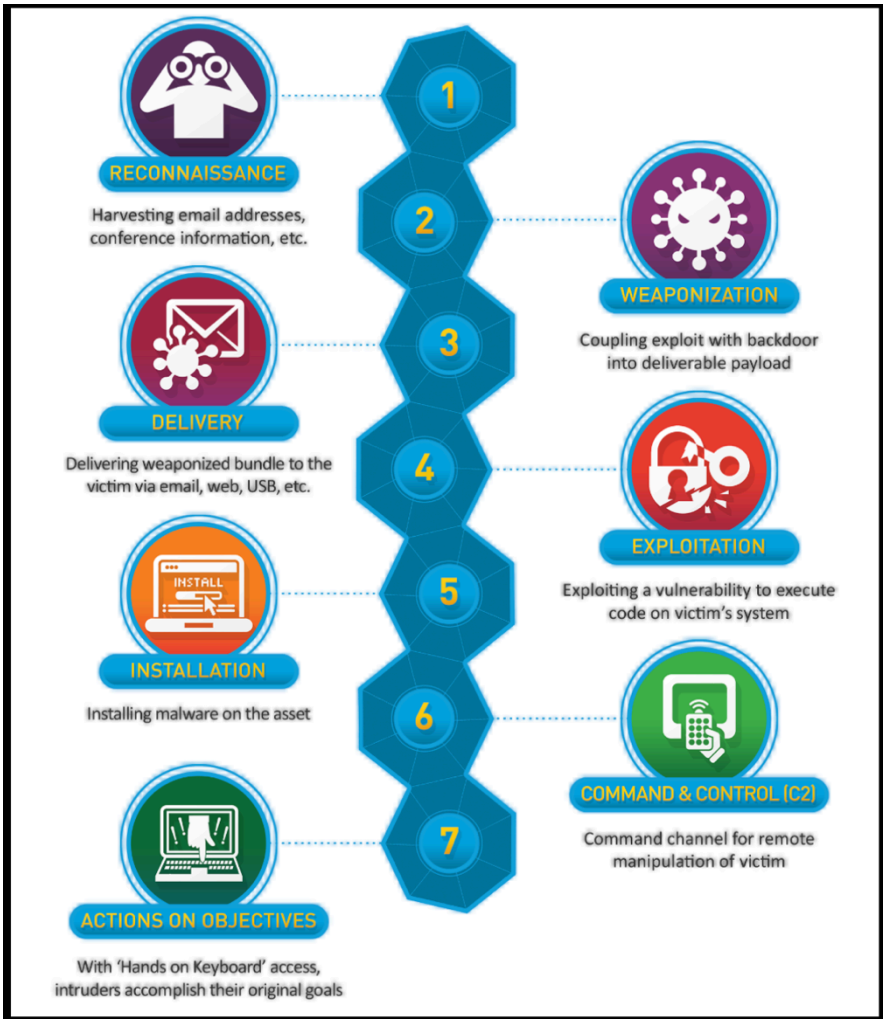
Exhibits the global locations and operational reach of major cyber mercenary organizations, including APT28, APT10, APT33, Lazarus Group, and other actors involved in offensive cyber operations.



Appendix B

“Cyberattack Pathways Targeting Critical Infrastructure.”
Entropiq Cybersecurity, “The New Age of Digital Warfare,” 2025.

Exhibits how cyber mercenaries carry out intrusions against government networks, banks, power grids, and communication systems using tools such as ransomware, phishing, zero-day exploits, and malware.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals