CSMUN 2026

RESEARCH REPORT

COMITTEE:

UNITED NATIONS SECURITY COUNCIL

SUBJECT:

HOW CAN HYBRID WARFARE BE REGULATED AS THE PROLIFERATION OF TECHNOLOGICAL INNOVATIONS IS RESHAPING THE WORLD ORDER?

TABLE OF CONTENTS

INTRODUCTION

« PEACE AND SECURITY »

The **United Nations Security Council** (UNSC) is one of the six principal organs of the United Nations. It was established on January 17, 1946. The Security Council has taken permanent residence at the United Nations Headquarters in New York City. According to the Charter, the United Nations has four purposes: to **maintain international peace** and security; to **develop friendly relations** among nations; to **cooperate** in solving international problems and in promoting **respect** for **human rights**; and to be a centre for harmonising the actions of nations. To do so, the Council can set the framework of an agreement; dispatch a mission, an investigation and mediation; and ask the Secretary-General to seek a pacific settlement of a dispute. As the **main peacekeeping body** of the UN, its powers include establishing **peacekeeping operations**, imposing **international sanctions** or authorising **military action**. It was originally composed of eleven members: five permanent and six non-permanent. In 1965 the Council was expanded to include ten non-permanent members, bringing the total to fifteen. Every month, the presidency is held by a different country, the order depending on the alphabetical order of the different members. The country that leads the Security Council sets the agenda and guides meetings.

The **five permanent members** (P5), **China**, **France**, the **Russian Federation**, the **United Kingdom** and the **United States**, hold **veto power** (meaning they can block any resolution). The ten non-permanent members are elected by the General Assembly for two-year terms and have equal voting rights, though they do not possess veto power.

As of 2026, the current non-permanent members of the Security Council are:

- until the end of 2026: Greece, Denmark, Pakistan, Panama and Somalia
- until the end of 2027: Bahrain, Colombia, Democratic Republic of Congo, Latvia and Liberia

For a resolution to be adopted, it has to be voted by at least nine out of fifteen members, and not to be vetoed by any of the five permanent members.

DEFINING THE TOPIC

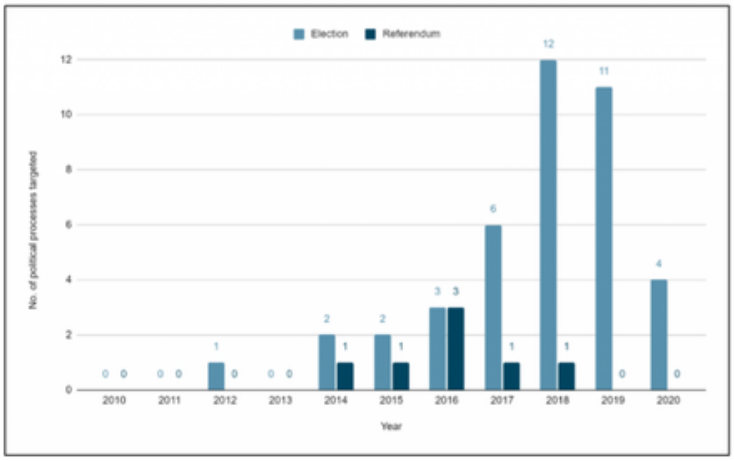
With the rapid and widespread development of **technological advancements**, in fields such as **artificial intelligence**, cyber capabilities or digital communication, hybrid warfare has emerged as one of the most **destabilising** yet complex **challenges to international peace** and security in the 21st century. Combining conventional military operations with **cyber attacks**, **disinformation** campaigns or economic coercion, hybrid warfare operates in the '**grey zone**' between peace and war, making its actions and their perpetrators **difficult to punish**. The proliferation of the technologies mentioned earlier have significantly amplified the **scale**, **speed** and **influence** of such operations, allowing both state and non-state actors to exert unprecedented precision, but also anonymity. Recent events going from the annexation of Crimea to interference in democratic processes demonstrate how hybrid tactics can **undermine sovereignty** and destabilize institutions while making conventional responses almost impossible.

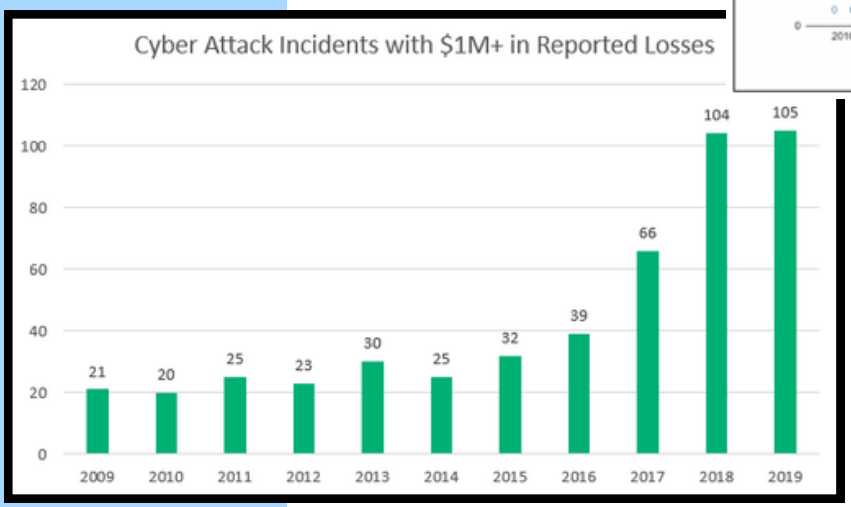
At the same time, existing legal frameworks are **ill-equipped** to face these modern and ever-changing threats. The central challenge of hybrid warfare lies in the **difficulty of attribution**. Without the ability to clearly **identify perpetrators**, legal responsibility cannot be established, retaliation becomes risky, and traditional deterrence mechanisms are weakened. This issue underpins

most of the **legal and political challenges** discussed in this report. It is urgent for the international community, and in particular the United Nations Security Council, to develop **coherent and enforceable mechanisms** to regulate hybrid warfare while preserving global peace and stability as well as the rule of law and human rights.

While the Security Council is responsible for maintaining international peace and security, its ability to address hybrid warfare is limited by political divisions among permanent members. The use of the veto by major powers can block collective action, particularly when hybrid operations are attributed to those same powers or their allies. This structural limitation reduces the Council's effectiveness in responding to ambiguous and contested threats such as cyberattacks or disinformation campaigns.

Figure 1: Cases of cyber-enabled foreign interference, by year and type of political process





KEY DEFINITIONS

- **Hybrid warfare:** a strategy that combines conventional and unconventional methods, including military operations, cyber warfare, disinformation campaigns, and economic pressure to achieve political or strategic objectives while avoiding direct, full-scale war

- **Grey zone conflict**: activities that occur between peace and war, where actions are aggressive and coercive but remain below the threshold that would trigger a traditional military response or formal declaration of war

- **Cyber warfare**: the use of digital attacks against computer systems, networks, or infrastructure to disrupt, damage, or gain strategic advantage over another state or actor

- **Disinformation**: the deliberate spread of false or misleading information with the intent to deceive, manipulate, or influence public perception and political outcomes

- **Artificial Intelligence (AI) in Warfare**: the use of machine learning and automated systems in military or strategic contexts, including surveillance, decision-making, cyber operations, and disinformation campaigns

- **Proxy Warfare**: a form of conflict where states indirectly fight each other by supporting third-party actors, such as militias or armed groups, rather than engaging in direct confrontation

- **Attribution (in Cyber Context):** the process of identifying the actor responsible for a cyberattack or hybrid operation, which is often difficult due to anonymity and deception techniques

- **Plausible Deniability:** the ability of a state or actor to deny responsibility for an action due to lack of clear evidence linking them to it

- **Sovereignty**: the principle that a state has authority and control over its territory and internal affairs, extended to include its digital infrastructure and cyberspace

- **International Humanitarian Law:** a set of rules that regulate conduct during armed conflict, aiming to protect civilians and limit the means and methods of warfare

- **Cyber Deterrence:** Strategies aimed at preventing cyberattacks by threatening retaliation or by strengthening defenses to make attacks less effective

- **Non-State Actors:** Groups or individuals that operate independently of governments, including terrorist organizations, private military groups, corporations, and hacktivist networks

- **Autonomous Weapons Systems:** Weapons that can select and engage targets without direct human intervention, often powered by AI

- **Economic Coercion:** The use of economic tools (sanctions, trade restrictions, resource control) to influence the behavior of another state without direct military force

CAUSES

→The main reason for the rapid development of hybrid warfare in the past decade is the **acceleration of technological development**. Advances in **artificial intelligence**, digital communication or **cyber capabilities** have given powerful tools to state and non-state actors to influence and destabilise adversaries. **Cyberattacks** can target key infrastructures remotely, while social media platforms allow **disinformation** to be spread rapidly on a worldwide scale, with new technologies such as **deepfakes** of automated bots further increasing the sophistication and range of these actions. Most importantly, many of these technologies are **low-cost** and **widely accessible,** therefore enabling a broader range of actors to engage in hybrid tactics.

→Another key factor in the recent proliferation of hybrid warfare is the growing role of **non-state actors** on the international scene. Technological accessibility and globalisation have allowed groups such as **militias**, private **military companies**, **hacker groups** or **cybercriminal** organisations to acquire capabilities that used to be limited to states. These actors can operate **across borders**, sometimes with informal support from governments, making attribution extremely difficult and expanding the range of potential threats far beyond conventional military forces.

→Furthermore, due to nuclear deterrence, economic interdependence and a risk of worldwide escalation, direct large-scale military conflicts have become increasingly risky, and states try to avoid them at all cost. As a result, states look

for **alternative means** of pursuing their strategic objectives without triggering open war. Hybrid warfare offers that opportunity by allowing actors to operate in the "**grey zone**" below the threshold of what would usually trigger armed conflict. By maintaining **ambiguity** and leveraging **plausible deniability**, states can weaken adversaries while avoiding formal retaliation under international frameworks such as those of the United Nations.

→Finally, hybrid warfare is also driven by the **structural limitations** of international law and enforcement mechanisms. In many cases, it is extremely difficult to identify the origin of cyberattacks or disinformation campaigns with certainty. This **lack of clear attribution** makes effective retaliation and accountability very difficult and unlikely. At the same time, existing legal frameworks are not fully adapted to address non-kinetic forms of aggression, creating a regulatory gap that actors can exploit. As a result, hybrid tactics offer a relatively low-risk, high-impact strategy in the current international system.

CASE STUDIES & PREVIOUS EXAMPLES

Annexation of Crimea - 2014

In early 2014, following political instability in Ukraine, armed personnel without insignia seized key infrastructure in Crimea, including airports, government buildings, and communication centers. These forces, later acknowledged to be Russian, operated alongside local militias and pro-Russian groups. At the same time, Russian media and online platforms disseminated narratives portraying the Ukrainian government as illegitimate, while cyber operations disrupted Ukrainian communications and military coordination.
The use of **unmarked troops** and **unofficial narratives** allowed Russia to maintain **plausible deniability** in the early stage of the

operation. The **absence of clear insignia** and the reliance on **local proxies** created **ambiguity**, delaying a unified international response and the application of international law in the early stages.

Russian interference in the 2016 US elections

During the 2016 U.S. presidential election, **cyber actors** often considered to be linked to Russia **infiltrated** political party servers, notably those of the Democratic National Committee (DNC), and leaked sensitive emails through platforms such as WikiLeaks. At the same time, **coordinated disinformation** campaigns were conducted on social media platforms like Facebook and Twitter, where fake accounts and automated bots spread polarizing and misleading content targeting specific demographic groups. According to the U.S. Intelligence Community (IC), the operation (code named "Project Lakhta") was ordered directly by Russian president Vladimir Putin and aimed to sabotage Hillary Clinton's presidential campaign while boosting Donald Trump's and increasing **political and social discord** in the United States.
The operations were conducted through **intermediary groups** and online personas, **masking direct state involvement**. While U.S. intelligence agencies later attributed the actions to Russian actors, the process required extensive investigation and was not immediately verifiable. This delay **limited rapid retaliation** and created political controversy domestically and

internationally and made it almost impossible to sanction the perpetrators.

Stuxnet cyberattack

Discovered in 2010, Stuxnet was a highly sophisticated computer worm designed to target Iran's Natanz nuclear facility. It **infiltrated** industrial control systems and caused centrifuges to spin at irregular speeds, leading to physical damage while reporting normal operations to operators. The attack significantly delayed Iran's nuclear program without the need for **conventional military strikes**. Although neither the United States nor Israel has openly admitted responsibility, multiple independent news organizations claim Stuxnet to be a **cyberweapon** built jointly by the two countries in a collaborative effort known as Operation Olympic Games.
No state officially claimed responsibility for the attack. Although widely attributed to the United States and Israel by cybersecurity experts and media investigations, the absence of formal acknowledgment created **legal ambiguity**. This lack of clear attribution prevented Iran from responding through conventional military or legal channels.

These examples collectively illustrate that one of the greatest challenges in addressing hybrid warfare is the **difficulty of attribution**. In each case, the use of proxy actors or cyber tools created uncertainty around responsibility, **delaying international responses** and limiting the possibility of accountability. This ambiguity not only complicates legal and military reactions but also **weakens deterrence**, as actors can operate with a reduced risk of consequences.

ETHICAL AND LEGAL CHALLENGES

→Hybrid warfare often targets **civilian infrastructure** and **populations**, particularly through cyberattacks and disinformation campaigns. This challenges the principles of **International Humanitarian Law** (IHL), which are based on the distinction between combatants and civilians. For instance, cyberattacks on **hospitals** or **energy systems** directly affect civilians and disinformation campaigns **manipulate public opinion** rather than military targets. As a result, it becomes difficult to apply traditional protections, raising concerns about the relevance of existing legal safeguards in modern conflicts.

→Efforts to counter disinformation in the context of hybrid warfare raise complex **ethical** and **legal dilemmas**, particularly regarding the protection of **freedom of expression**. While limiting the spread of false or manipulative information may be necessary to protect democratic institutions and public order, such measures risk enabling **censorship** or political control over information. A central challenge lies in determining who has the authority to define what constitutes “disinformation,” as governments may be tempted to label dissenting or critical voices as harmful. Additionally, the increasing role of **private technology companies** in moderating online content raises concerns about **accountability**, **transparency**, and the concentration of power over public discourse.

RELEVANCE OF EXISTING FRAMEWORKS

1. **Limitations of the UN Legal Framework**

The primary legal framework regulating the use of force between states is the **United Nations Charter**. In particular:
- **Article 2(4)** prohibits the **use of force** against the territorial integrity or political independence of any state
- **Article 51** recognizes the right of **self-defense** in the event of an "**armed attack**"

However, these mechanisms were designed in the context of **conventional military conflict** and do not clearly apply to hybrid warfare. A key issue is the **lack of clarity** regarding whether cyber operations or disinformation campaigns constitute a "use of force" under Article 2(4), or rise to the level of an "armed attack" under Article 51.
For example, while a cyberattack causing physical destruction, such as damage to infrastructure, may be interpreted as an armed attack, other actions such as data theft, election interference, or large-scale disinformation remain in a legal grey zone. This **uncertainty** limits the ability of states to invoke self-defense or seek collective action.

2. **Absence of clear thresholds for the use of force**

Another major challenge is the absence of a **clearly defined threshold** at which hybrid actions qualify as **acts of war**. International law does not specify when a cyberattack or coordinated hybrid campaign becomes severe enough to justify a military response.

This creates a **dilemma** for states as responding too strongly risks escalation but responding too weakly may encourage further attacks
The lack of agreed thresholds contributes to **legal uncertainty** and increases the risk of miscalculation in crisis situations.

3. **Limits of previous efforts**

Several international initiatives have attempted to address aspects of hybrid warfare, particularly in the cyber domain. Within the United Nations system, the **United Nations Group of Governmental Experts** has developed **voluntary norms** of responsible state behavior, such as the principle that critical infrastructure should not be targeted during peacetime.
In addition, the **Tallinn Manual** represents a significant **doctrinal effort** to interpret how existing international law applies to cyber operations, addressing issues such as sovereignty, state responsibility, and the use of force.
However, these frameworks face **important limitations** since they are largely **non-binding**, lack enforcement mechanisms and reflect limited consensus among states, particularly major powers.
As a result, while they contribute to norm-building and legal clarification, they do not provide a comprehensive or enforceable system for regulating hybrid warfare.

BLOC POSITIONS

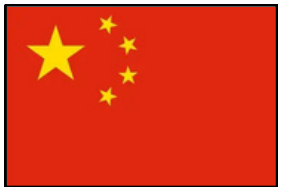




Western Bloc - United Kingdom, France, United States of America, Denmark, Greece, Latvia

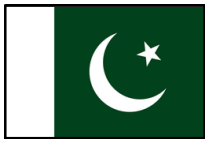
These states advocate for a proactive and regulatory approach to hybrid warfare. These states view hybrid threats, particularly cyberattacks and disinformation campaigns, as major risks to democratic institutions and international stability. They support the development of clear international norms, stronger attribution mechanisms, and, where necessary, sanctions against actors responsible for hybrid aggression. Many of these countries also emphasize the importance of collective defence, particularly within frameworks such as NATO. At the same time, they seek to balance regulation with the protection of fundamental rights, including freedom of expression, which can create internal tensions when addressing disinformation. Countries of this bloc are likely to push for binding international frameworks.

- **EU Members**: focus on regulating tech companies/platforms and disinformation
- **Latvia:** hardline stance on hybrid threats (due to proximity with Russia)




Russia and China

Russia and China adopt a markedly different approach, emphasizing the primacy of state sovereignty and non-interference, particularly in the digital domain. These states are generally cautious about the development of binding international regulations that could restrict their strategic flexibility or be used to justify external intervention. Instead, they argue that each country should have the right to regulate its own digital environment according to its political and social context. While rejecting accusations of hybrid warfare they tend to favor non-binding agreements and oppose enforcement mechanisms such as sanctions based on contested attribution.




Strategic Emerging Powers and Power Balancers - Pakistan, Colombia, Panama, Bahrain

This group of emerging and mid-sized powers tend to adopt more flexible and pragmatic positions on hybrid warfare. These states recognize the growing risks associated with cyber threats and disinformation but remain cautious about applying strict international regulations that could limit their sovereignty or strategic autonomy and mainly emphasise on the importance of capacity-building, technical cooperation, and information-sharing.

- Pakistan: strong focus on cyber sovereignty and regional security
- Colombia: emphasis on internal stability and combating non-state actors
- Bahrain: aligned with Western security frameworks but cautious on regulation

Vulnerable and Developing States - Democratic Republic of Congo, Somalia, Liberia

These states approach the issue of hybrid warfare from the perspective of vulnerability and limited capacity. These countries may lack the technological infrastructure and institutional resources necessary to effectively defend against cyberattacks, disinformation campaigns, or interference by external actors. As a result, they are particularly concerned about the destabilizing impact of hybrid tactics on fragile political systems and ongoing conflicts. This bloc generally advocates for stronger international cooperation, capacity-building initiatives, and clear protections against external interference. Rather than focusing primarily on deterrence or enforcement, they emphasize the need for support from the international community, including technical assistance and funding, to strengthen resilience against hybrid threats.

WHAT SHOULD YOUR RESOLUTIONS BE ABOUT?

Hybrid warfare represents a complex and evolving challenge that cannot be addressed through a single legal instrument or military strategy. Its multidimensional nature (combining cyber attacks, disinformation, the role of non-state actors, economic coercion...) as well as the lack of clear existing legal frameworks to face this issue makes the development of binding global rules difficult. Effective resolutions should aim not only to strengthen international cooperation, but also to clarify legal frameworks, improve collective resilience, and establish practical mechanisms for accountability. Effective resolutions should aim not only to strengthen international cooperation, but also to clarify legal frameworks, improve collective resilience, and establish practical mechanisms for accountability. Delegates are encouraged to propose solutions that are realistic, adaptable, and sensitive to geopolitical divisions within the international system, particularly within the United Nations Security Council context.

Here are some questions to guide your research and help build your stance on the topic:

- How can hybrid warfare be clearly defined within an international legal framework?
- At what point should a cyberattack or hybrid action be considered an act of war?
- Should there be an international body responsible for cyberattack attribution?
- How can attribution be made more reliable, transparent, and widely accepted?
- Should hybrid attacks trigger collective defence mechanisms such as those under NATO?
- How can states regulate disinformation without violating freedom of expression?
- What responsibilities should private technology companies have in preventing hybrid threats?
- How can international cooperation be improved in cybersecurity and intelligence-sharing?
- How can developing states be supported in building resilience against hybrid threats?
- What sanctions or consequences should apply to confirmed hybrid warfare activities?
- How can international law be updated to reflect non-traditional forms of conflict?
- Should there be limits on state use of proxy actors in hybrid warfare?
- How can trust between states be rebuilt in an environment of persistent informational conflict?

BIBLIOGRAPHY

SOURCES

- Stowell, Joshua. “What Is Hybrid Warfare?” Global Security Review, Aug. 2018, globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

- “Hybrid Threats.” Defence-Industry-Space.ec.europa.eu, defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

- Shevchenko, Vitaly. ““Little Green Men” or “Russian Invaders”?” BBC News, 11 Mar. 2014, www.bbc.com/news/world-europe-26532154

- Danyk, Yuriy, et al. “Hybrid War: High-Tech, Information and Cyber Conflicts.” Connections: The Quarterly Journal, vol. 16, no. 2, 2017, connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts

- ASD Team. “Fact Sheet: What We Know about Russia’s Interference Operations | German Marshall Fund of the United States.” Www.gmfus.org, 2019, www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations

- Trellix. “What Is Stuxnet? | Trellix.” Www.trellix.com, 2024, www.trellix.com/security-awareness/ransomware/what-is-stuxnet/

- Robertson, Anthony. “What Is Grey Zone Confrontation and Why Is It Important? | the Cove.” The Cove, 2022, cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important

- Beckett, Conrad. “Getting to Grips with Grey Zone Conflict – Cyber & Specialist Operations Command.” Blog.gov.uk, 26 Apr. 2021, cyberandspecialistoperationscommand.blog.gov.uk/2021/04/26/getting-to-grips-with-grey-zone-conflict/

SOURCES TO GO FURTHER

- https://www.unesco.org/gem-report/en/articles/new-unesco-report-warns-social-media-affects-girls-well-being-learning-and-career-choices : UNESCO report on social media's impact on girl's mental health

- https://www.who.int/europe/publications/i/item/WHO-EURO-2025-12187-51959-79685 : WHO policy brief on adressing the digital determinants of youth mental helath and well-being

- https://www.who.int/europe/news/item/23-05-2025-online-lives--offline-consequences : WHO article "Online lives, offline consequences"

- https://www.theguardian.com/lifeandstyle/2026/feb/16/dr-rangan-chatterjee-interview-screen-time-mental-health-banning-social-media-18-podcaster : The Guardian article (interview) on screen time and mental health

- Mini-Series on Netflix, "Adolescence"