Disarmament and International Security Committee

Measures to Prevent the Rising Threat of Hybrid Warfare in Contemporary Armed Conflicts in Southeast Asia

-Committee Guide-

Ela Ünlü
-Chairperson-
Gracia Dimitrova
-Chairperson-
Hannah Steiner
-Chairperson-

TABLE OF CONTENTS

I. INTRODUCTION

a. Introduction to the Committee:

The First Committee of the United Nations General Assembly is known as the Disarmament and International Security Committee (DISEC). It addresses problems associated with international peace, global security, disarmament, and threats to international stability. DISEC offers a forum for Member States to deliberate on and devise solutions for challenges like nuclear proliferation, terrorism, cyber warfare, arms trafficking, and emerging military technologies.

DISEC lacks the power to impose sanctions or authorize military action, in contrast to the United Nations Security Council. The committee concentrates on debate, collaboration, and submitting resolutions that promote peaceful conflict resolution and international cooperation instead. DISEC includes representatives from all UN Member States, with each country having a single vote.

The committee's goal is to foster international security via diplomacy and multilateral discussions. It is recommended that delegates engage in negotiations, forge alliances, and develop pragmatic resolutions that tackle global security issues while upholding international law and national sovereignty.

Founded in 1945, DISEC is one of the six principal committees of the United Nations General Assembly. It has since been significant in talks about arms control accords, diminishing worldwide tensions, and bolstering mutual security. During General Assembly sessions, the committee convenes once a year at the UN Headquarters in New York City.

During Model United Nations (MUN) conferences, DISEC prompts delegates to engage in critical thinking regarding contemporary international security challenges and to work together toward balanced and feasible solutions. While striving for agreement and upholding diplomatic behavior.

b. Introduction to the Topic:

Topic 1: Measures to Prevent the Rising Threat of Hybrid Warfare in Contemporary Armed Conflicts in Southeast Asia

Hybrid warfare is a serious issue. It is when countries use a mix of non-military ways like cyberattacks and fake news to cause trouble without directly fighting. Southeast Asia is in a spot. There are tensions between countries, arguments over land and people rely a lot on technology.

This makes the region an easy target for warfare.

We need to talk about this because hybrid warfare is happening more and more. Our laws and security systems are not ready to deal with it. We will discuss ways to work together make our ways to make our digital security system safer and keep the region stable.

II. FACTS AND CURRENT SITUATION

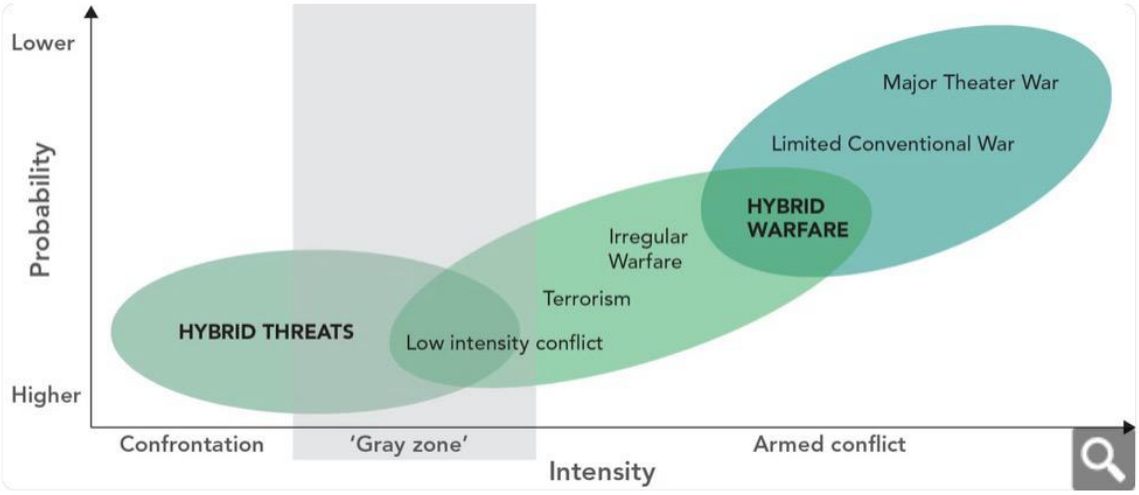

FIGURE 1. Hybrid Threats and Hybrid Warfare Shown on a Continuum of Conflict. SOURCE:After Linton Wells, "Cognitive Emotional Conflict," PRISM 7, no. 2 (2018): 6 (who refers to "hybrid warfare" as "hybrid threats"); and Hoffman, "Examining Complex Forms of Conflict" (who refers to "hybrid threats" as "measures short of war").

https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979787/countering-hybrid-warfare-so-what-for-the-joint-force/

a. Facts

- Hybrid warfare is a mix of non-military tactics. This includes cyberattacks and spreading false information. It also includes using pressure and working with proxy groups.
- Southeast Asia is an important place because it has major trade routes and there is a lot of competition between countries.
- Many countries in Southeast Asia are becoming increasingly dependent on digital infrastructure, such as communication networks, government databases, and energy systems. This makes them more vulnerable to cyber threats.
- There are also disputes over territory in the South China Sea. This is causing a lot of tension in the region.

b. Current Situation

- There are cyberattacks and misinformation campaigns happening in Southeast Asia now.
- The rivalry between the United States and China is intensifying → . This is increasing tensions in Southeast Asia.
- Some countries are spending money on cybersecurity and working together to defend the region.
- Hybrid warfare is not clearly defined in international law. This means that there are no rules, about what is and is not allowed.

III. Relevant Cases / Major Parties Involved

The South China Sea is a deal for China and some Southeast Asian countries. They have conflicting claims over islands, fishing rights, and natural resources.

The Philippines have had some problems with people hacking into their computers and spreading information about the conflicts in the region.

Vietnam and Malaysia are also having a hard time because of the security issues in the region.

The Association of Southeast Asian Nations is trying to help these countries work together and be more stable.

IV. Past International Actions

The Association of Southeast Asian Nations has been working together to make the region safer from cyberattacks.

The United Nations talked about how countries should behave in cyberspace.

Many countries have made their cybersecurity stronger and have improved their digital defense systems.

International organizations are still trying to figure out how to deal with conflicts and hybrid warfare.

V. Current Challenges

We still do not have a definition of what hybrid warfare is. It is hard to find out who is behind cyberattacks and prove it. Countries often disagree on how to deal with threats. New technology is coming out fast and it is hard to make rules to regulate it.

VI. Definition of Key Terms

Hybrid Warfare is when a country uses a combination of non-military tactics to destabilize another country.

A Cyberattack is when someone tries to hurt or get into systems without permission.

Disinformation is misleading information that is spread on purpose to influence what people think.

Proxy groups are non-state actors that receive support, such as funding, weapons, or training, from a state that seeks to influence a conflict without becoming directly involved. For example, Hezbollah has often been described as an Iranian proxy group.

VII. Guiding Questions for Delegates

- How can we make law better at dealing with hybrid warfare?
- What role should regional organizations like the Association of Southeast Asian Nations play in helping countries work together on cybersecurity?
- How can countries protect themselves from cyberattacks and disinformation?
- Should there be rules about hybrid warfare tactics?

VIII. Useful links:

- United Nations Office for Disarmament Affairs
- ASEAN Official Website
- Cyber ASEAN Framework
- EU Cyber Direct – Cyber Diplomacy in Southeast Asia
- ISEAS Yusof Ishak Institute – Cyber Attacks in Southeast Asia
- East Asia Forum – Hybrid Warfare's Assault on ASEAN Regionalism
- CSIS Asia Maritime Transparency Initiative

IX. Sources:

- United Nations Reports on Cybersecurity and International Security
- ASEAN Cybersecurity Cooperation Strategy
- ISEAS Yusof Ishak Institute Research
- East Asia Forum Security Analysis
- Academic Journals on Hybrid Warfare and Cybersecurity