RENMUN XI

REJUVINATION



March 14th & 15th, 2026

Chair Report #1
Disarmament and International Security Committee

Addressing the security risks of Grey Zones

Vanessa Chan

Chair Introduction

Dear DISEC delegates,

Greetings! We are Vanessa and Wilfred, G10 / Y11 students from Diocesan Girls' School and the French International School, respectively, and we are delighted to be chairing DISEC for this iteration of RENMUN!

The United Nations Disarmament and International Security Committee (DISEC) was established in 1945 to address topics such as the regulation of armaments, terrorism, and arms trafficking. According to the UN Charter, the role of DISEC is to help set 'general principles of cooperation in the maintenance of international peace and security', and can make topic recommendations for the UNSC to discuss. Despite not having the ability to authorise legally binding resolutions like the UNSC, this feature should allow for more diversified and nuanced debate among delegates, granting more freedom to debate.

As DISEC is an intermediate council, we expect delegates to have at least a basic understanding of council procedure, and also to not only reference the chair report but also conduct their own additional research on the topic. Position papers are **not** mandatory, though we will read them should you choose to submit them. Additionally, you will be expected to give **one 60-second opening speech** for each topic (two mandatory speeches in total). Lastly, and most importantly, we expect delegates to remain diplomatic throughout the entire conference and seek cooperation whenever possible.

Should you have any questions, feel free to reach out to either of us by whatever means possible. Good luck, and we look forward to seeing you in March!

Cheers,
Vanessa Chan (s221010@student.dgs.edu.hk)
Wilfred Kwan (wi2fr2@gmail.com)

Topic Introduction

Grey zone security risks are an omnipresent threat to international security, involving the use of all kinds of power in order to increase a country's sphere of influence or indirectly attack adversaries. Grey zone activities can involve the use of economic pressure, third-party actors, or informational warfare to act as threats, characterised by their legal ambiguity. Currently, grey zone activities are able to thrive due to the binary security international standard, direct clashes against liberalist values, and plausible deniability. Delegates will have to reevaluate international security frameworks, as well as national security standards and approaches in order to counter grey zone security risks effectively.

Key Terms

Term	Definition
Grey zones	Activities by a state that are harmful to another state that are sometimes considered to be acts of war, but are not legally considered acts of war.
White zones	Peaceful, transparent actions that adhere to existing international standards. Refers to activities that occur legally in the realm of peacetime.
Black zones	Outright acts of war that are considered active, open and conventional warfare. Refers to activities that occur legally in the realm of wartime.
Soft power	The use of a country's cultural and economic influence to persuade other countries to do something, rather than the use of military power.
Proxy war	Military conflict fought between groups or smaller countries that each represent the interests of other larger powers, and may have help and support from these.

Background Information

Defining Grey Zones

Grey zones are often referred to as hybrid threats or indirect threats that do not fit into a neat definition of 'direct military action' or are legally ambiguous. These actions are below the threshold of war (i.e. they cannot be considered a formal military response), but are also aggressive in nature. These include the usage of cyberattacks, information manipulation, or even economic strategy, as long as it takes the form of non-violent pressure. One way to phrase it is to use civilian instruments to achieve military goals. To put it in clear terms, grey zones can be defined by these aspects:

1. Unconventional means

This includes the aspect of not using typical military aggression and direct application of military force, but rather a variety of other methods to apply pressure. This includes propaganda, sabotage, cyberattacks, proxy forces, and insurrections. These means are seen as useful, as while they can provoke some retaliation from the adversary and risk war, they are chosen specifically to avoid escalation. A fundamental aspect of grey zones is to skirt the line between peace and war.

2. Ambiguous ways

Grey zone activities also blur the lines between war and peace through methods that are specifically calculated in order to avoid attribution. Examples of this include the use of proxy groups, technologies that are able to mask the identity and motivations of the perpetrator, and generally means that are able to cover up the tracks by dispersing blame, such as through disinformation. Grey zone activities are made to generate confusion and internal divides in the adversary in order to complicate their response, allowing the perpetrator to have political space to amplify and realise their objectives.

3. Limited ends

Grey zone activities do not directly target and attack the core interests of the adversary, but instead pose as a gradual process to degrade and erode the credibility or position of the adversary. This involves attacking peripheral interests that are unseen, foundational pillars that may make up the adversary's strategy.

Additionally, grey zone challenges are also seen as perspective-dependent, and each party in a single conflict may depict the situation and correspondingly react differently. For example, in the Russo-Ukrainian war, the United States depicts a contest to take place in the white zone, employing tactics such as economic sanctions and diplomatic pressure. For Russia and Ukraine, however, the attack and defence strategies lie directly in the black zone of war, and direct military aggression is required. While there is usually a clear-cut response for war and peace, there is also

a vast range of conflict types between these poles that may be more difficult to respond to.

The description of grey zones and grey zone activities here may seem to be incredibly vague and abstract, so delegates are encouraged to reference the examples in later sections and consolidate that information with the general understanding of grey zones given here.

Origin of Grey Zones

The term 'grey-zone' was coined by the United States Special Operations Command, described as 'competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality'. In fact, grey zone activities have been conducted since ancient civilisation, and have only become increasingly developed and strategic with the improvement of technology and infrastructure. There are some landmark and more modern cases of grey zones that exemplify how it functions and its danger to international peace.

The Cold War (1947-1991)

The Cold War is perhaps the most distinct example of grey zone tactics – during this period, the US and the USSR were not directly at war, but employed various methods to weaken the other. The root cause of this war was the deep-seated ideological differences in capitalistic democracy and authoritarian communism, both of which aimed to exert a larger global influence than the other, especially with disagreements in the aftermath of WWII.

1. Information warfare

Both sides utilised extensive intelligence-gathering measures, including the Soviet 'active measures', which were sophisticated and covert operations aimed at influencing Western societies to advance Soviet foreign policy objectives. The USSR used the deployment of agents of influence and undercover operatives to infiltrate and manipulate key sectors of Western society. The overarching goal of these covert measures was to destabilise political structures and further Soviet interests abroad. This approach was described as 'political warfare', with manipulative and deceptive techniques in the 'active measures'.

A case example of this is Operation Denver, which was an active measure disinformation campaign by the KGB to plant the idea that the United States had invented HIV/AIDS as a part of a biological weapons research project. The operation involved funding radio programs, courting journalists, and distributing scientific studies to create this lie. The ultimate goal of this operation was to undermine the US's credibility, foster anti-Americanism and diplomatically isolate the US abroad. This was quite successful in undermining the US's global position and even forcing an official denial from the US government.

On the US side, the CIA initially funded Radio Free Europe / Radio Liberty, a media organisation that broadcast Western news culture to various countries, an attempt to communicate with their adversary's citizens. Furthermore, the US developed organisations that published all forms of media aimed to sway public opinion and promote anti-communist values. From music, visual arts, to films, the US integrated the idea of 'American freedom', countering Soviet accusations of racism, portraying a nation that was culturally diverse and harmonious.

This kind of ideological and cultural attack, based on disinformation, spreading propaganda, and altering the political and social beliefs of the adversary, is only one kind of grey zone method. Delegates will have to keep in mind this kind of more passive attack, and how this plays in with the rising spread of social media and internet usage in general, allowing the effect of information warfare to become amplified on a new global scale.

2. Proxy warfare

Proxy warfare is a key pillar of the tactics that the US and USSR employed against each other, with an estimated almost 60 proxy conflicts that involved the two parties, including the Korean War and the Vietnam War. This was conducted by the countries that provide military, economic, and humanitarian aid to opposing sides in a conflict. They served as the microcosms of the ideological and geopolitical struggle between the two, including their attempts to increase their political sphere of influence over the world. The US believed in the domino theory, which claimed that if one nation fell to communism, this would lead to a cascade of communist takeovers in the region. Thus, this funnelled the significant military effort in order to prevent countries from succumbing to communist ideologies through Soviet-backed forces gaining control. However, historians also point out economic hegemony as a factor for the US's incredibly aggressive foreign policy, aiming to gain economic leverage, especially in Southeast Asia.

A common model involved in proxy conflicts is the objective to revise and alter the current government controlling regions, changing the power structure to favour their political and economic interests. While one power uses military action to maintain the current status quo, the other power targets vulnerable areas of strategic interests. Referred to as the 'revisionist' power, they use activities such as promoting political instability or uprisings or small, sub-conflict actions to gain land or strategic positions.

An example of this is the Korean War, which was a strategic extension of the ideological clash between communism and democracy. In a nutshell, the conflict stemmed from the polarisation of Korean leadership, with both sides viewing each other as illegitimate and wanting to unify Korea. The South formed its own

anti-communist, while in the North emerged a leadership that came from a formed communist guerrilla. The US identified this as a threat of global communism and sent ground troops labelled as 'police action', though never formally declaring war on North Korea. The USSR had already been heavily involved in North Korea after WWII, though it tried to hide direct Soviet intervention in the conflict, providing both military and economic aid. This kind of covert political guidance and support is a key feature of proxy warfare in grey zone activities.

3. Economic Coercion

Aside from waging different types of warfare, the distribution of resources and usage of soft power were also critical in the Cold War. The Marshall Plan, also known as the European Recovery Program, was a US post-WWII initiative created by the fear of communist expansion and deterioration of European economies in the aftermath of the war. The plan was effective due to its conditional nature – it demanded European cooperation and specific commitments, helping to expand the US's sphere of influence and strengthening US integration on a global scale, as well as aligning the region with American political objectives. The US capitalised on its economic abundance to address the European crisis, but in such a way that would reinforce the country's importance and interests in the new economic structure.

In fact, the USSR was invited to participate in this economic program, which was presented as a European collaboration. Naturally, however, the terms that were written into the plan went completely against Soviet interests and ideologies, emphasising transparency in national economics and moving into multilateral trade. The inevitable denunciation of the plan by the USSR shifted the blame for Europe's economic division to the Soviets and also ensured that the plan would be focused on the Western bloc. Not only was this an attempt to improve the post-war economic situation by the US, but it also proved to be a strategic move to weaken the USSR's place on the global stage. Additionally, the US also established the Coordinating Committee for Multilateral Export Controls (COCOM), aimed to coordinate controls on exports from Western Bloc countries to the Soviet Union. This was only part of the economic strategies employed, including sanctions, trade restrictions and embargoes as tactics to strain the opposing side. Economic power can inflict significant consequences on the well-being of a nation, and this kind of economic competition and isolation could be as effective in harming countries in a conflict.

Aside from the cases stated here, there are still numerous other instances where the grey zone tactics are used by countries in order to exert political or economic influence, or counter the interests of adversary nations. Delegates can reference the 'Additional Events' section for reference to more specialised cases of grey zone activities. Such events not explicitly mentioned in the chair report include marine intimidation, social media interference, and the use of paramilitary forces. Delegates are encouraged to conduct their own research to gain a better understanding of

their country's interactions with grey zone activities, using this information to create solutions and strategies that befit their stance and specialities.

Potential Clashes

Binarism

In the current international security structure, countries generally treat wartime and peacetime as black and white zones. During peacetime, countries focus on civil liberties and establishing diplomacy; during wartime, miltiary authorisation is triggered, and international / national laws come into effect, dictating the path that international relations occur. This is a rigid binary system that countries expect each other to abide by, and also capitalise on in order to carry out grey zone activities, which are unable to fit neatly into either black or white zones. Researchers have pointed out that despite its obvious flaws, current legislation (both national and international) is essentially built on this foundation, leading countries to be unable to respond to grey zone, ambiguous actions effectively. While in the distant past, conflicts were fought between states according to recognised conventions and definitive outcomes, this is a severely outdated approach to 21st century international politics. In order to tackle non-traditional forms of warfare, organised crime, and the rise of cyber warfare, the current international security structure needs to be heavily revised to adapt to the changing needs that grey zone activities bring.

Currently, the International Humanitarian Law defines war conflict or wartime involving International Armed Conflict (IAC), which is direct armed conflict between two or more states, when there is a resort to armed force between states. This definition largely dictates many other international security laws and the rights / protections that those affected by these conflicts have. However, there is no specification of the protections necessary for those affected by grey zone activities, despite their still being economically, militarily, and socially harmful to those involved. Delegates can consider reevaluating the existing legal framework surrounding conflicts and how the integration of grey zone security risks could help to improve international security.

Furthermore, current governments are often built on a branch structure, separating economic, military, and political factions. However, a key aspect of grey zone activities is the use of multilateral strategies to prove effective (e.g. see Russian Annexation of Crimea). This means that there needs to be a better cohesive relationship between all of these branches that are able to address hybrid attacks that may tackle various areas of a country. Delegates can consider creating an international standard for a central government hub or entity that is able to combine the various forces of a country as a means to tackle multi-faceted grey zone security threats.

Liberalism

The liberal world order is based on sovereign states, international law and free global trade – all key aspects that grey zone area activities attack, utilising proxy warfare and non-state actors, bypassing international standards of formal war, and manipulating economic leverage for national interests. The freedom of speech and press is an especially pertinent clash, as countries often use the spreading of disinformation and even forging new reports in order to sway public opinion and create confusion. However, the regulation method of censorship and content moderation goes against the liberalist policy of free speech. Similarly, developing protectionism and autarky in order to avoid being affected by global economic sanctions or international trade conditions poses a risky path that leads to the threat of geopolitical isolation and the deterioration of international relations. Thus, there is a risk that mitigating grey zone activities threatens the core interests of many powers, which is to uphold democracy and maintain liberalism, especially in Western powers.

Thus, some argue that the solution should not be to close off the channels of attack that grey activities employ, but instead to make them more resilient to succumbing to pressure by adversaries. Countries should set up stronger education and media literacy among the public in order to weaken the effectiveness of disinformation on shaping public opinion, while also strengthening national policy to account for the unique risks that grey zone activities bring, creating more efficient legal systems that can quickly address impending grey zone threats. This perspective focuses on bolstering the social and cultural aspects of the issue. In terms of the economic threat, creating regional blocs and actually pushing forward global trade and relations to diversify reliance could help to alleviate the issue of one nation holding too much economic leverage.

Legality

The issue of the legality of grey zone activities corresponds to the clash in the binary nature of the international security system. Another international standard for warfare is the UN Charter: under Article 2(4), which prohibits the threat or use of force in international relations, and Article 51, which protects the right of countries to act in self-defence 'if an armed attack occurs against a Member of the United Nations'. While these articles do outline the legal authority in terms of armed attacks, they do not account for non-military actions such as economic coercion and cyber warfare. Thus, there is still heated debate over whether these non-military actions can be considered as formal attacks on a country, signalling a national response. If such attacks are unable to meet this internationally-agreed threshold, then the affected nation does not have a legal right to retaliate while its economy or society is damaged.

Additionally, the idea of national sovereignty becomes vague when it comes to political and diplomatic influence, and when that crosses into illegal foreign interference. There is no international standard which is able to define when foreign influence, either through economic or political support in national politics, eventually becomes a violation of sovereignty by funding a political movement or insurgency. Nations exerting their political soft power currently remain safely within legal regulations, though this has massive political consequences for affected nations. Delegates can consider creating an international standard that evaluates the degree of foreign interference and the point at which that infringes on the national sovereignty of countries.

Plausible Deniability

The use of intermediate middlemen actors in order to facilitate grey zone actions means that while there are typically obvious connections to nations that have pushed for these actions, there is little ability to be able to prove it to a standard and hold such countries responsible for their actions. In order for countries to be able to retaliate and take action against perpetrators, they first need to be able to identify them. However, grey zones greatly muddle this knowledge, not only by using non-state and private actors, but even civilians and pinpoint the blame on them as independent parties, or use them as a barrier towards responsibility. This creates a sort of 'burden of proof' that the affected nation needs to be able to sustain, which is often impossible given the limited time to respond, despite the fact that this is required in order to retaliate on a safe international basis, or these countries risk being seen as aggressors on the global stage, weakening their international position.

This effect has only worsened with the progression of digital technologies and their integration into grey zone activities. Through using methods such as VPNs or falsifying code, perpetrators are able to cover their digital footprints, making it incredibly hard for the affected country to identify them and conduct formal retaliation (e.g. see Stuxnet). By the time that intelligence agencies are actually able to track down the source of the actions and decide on a response plan, the damage has already been done, and retaliation holds less political value. This points to a mismatch between the speed at which these attacks can be conducted and the speed at which verification and retaliation occur.

Furthermore, the political cost of acknowledging the perpetrator can also play into grey zone dynamics. If a country admits that they have officially been attacked by another powerful nation, then it is under a political obligation to respond to this attack. This poses the risk of escalation in conflict that the country may not be able to support militarily or economically – thus, national leaders may respond to such grey zone actions by utilising the plausible deniability to ignore the issue and neglect taking action. However, this also means that this will only incentivise the perpetrator to push even further due to the lacklustre response by the affected nations,

eventually leading to vicious cycles that worsen the degree and impact of grey zone actions, until they have already unconsciously entrenched into national sovereignty and integrity.

Key Stakeholders

Stakeholder	Involvement with the Issue
United States	The United States has played a key role in both perpetrating and countering grey zone activities, and is the originator and architect of the concept of grey zones. While the US often depicts itself as a country that suffers from grey zone activities and works to counter these actions, the nation also has a track record of grey zone activities itself. In fact, some may consider the coining of the term 'grey zone' itself rooted in political interests, where the US uses it to describe offensive actions by other powers, but refrains from describing similar actions taken by the government. This coincides with the issue of political manipulation and plausible deniability through legal loopholes, where adversaries are framed as disrupting rules and order, while the country itself is simply responding to these challenges and safeguarding international order. The US also stands as an important stakeholder due to the implementation of a new defence strategy under the recent governance, signalling a turn in international security. New security strategies mention integrated defence and deterrence, campaigning across all spectrums of conflict. This means that there is a larger effort to coordinate inter-branch activities and recognise the official risks of grey zone activities.
Russia	Russia currently operates under a security strategy that aims to change the current international order. In a post-Cold War landscape, Russia rejects the economic and political sphere of influence that the US has built up in the Western bloc. Thus, many argue that the ultimate Russian goal is to expand the country's international influence, creating an international order where the most powerful nations hold regional spheres of influence. This can be seen in the example of Ukraine, where Russia believes that as the regional power, it should dictate the trajectory and interests of Ukraine, while the US and other Western powers support the independent sovereignty that

	Ukraine has, separate from Russia. Russia depends heavily upon grey zone tactics in order to achieve its national objectives, which is to carry out competition and coercion towards adversaries as mentioned above. This not only includes the aforementioned illegal annexation of Crimea, but also involvement during the Syrian Civil War (with disinformation campaigns and cyber interference, thus discrediting Western powers), sabotage attacks on European infrastructure, among many other events.
China	China has been reported to be eager to safeguard maritime entitlement, utilising a combination of the coast guard, naval forces, and militia. Scholars contend that such operations often implement non-military tactics that progressively escalate conflict risks without crossing the threshold of warfare. Being a major opposing force against the US and disputing over issues such as the trade war, the usage of grey zone tactics in the clash between the Eastern and Western blocs will prove to be pivotal towards mitigating international security. China also holds considerable economic power on the global stage and utilises this leverage in order to protect national interests.
Iran	Aside from the Axis of Resistance, Iran has employed various other grey zone tactics, including maritime and airborne military exercises as well as proxy warfare in order to better exert political influence in the region. Iran is mostly important for its intervention and support towards non-state actors to counter Western influence, especially the US, without direct confrontation. While the US attempted to mitigate such Iranian actions through the maximum pressure campaign (intensified economic sanctions), this only served to further harm Iranian civilians, while the state retaliated with more severe military operations. While Iran is considered a mid-size power, its strategic employment of militias and non-state actors has allowed it to expand its political influence significantly in the region, proving that through the manipulation of grey zone tactics,

	even mid-size powers such as Iran can still pose valid threats against superpowers such as the US.

Possible Solutions

International standard framework

As mentioned above, a major weakness when trying to counter grey zone activities is the legal ambiguity. Thus, delegates can consider reforming international legal framework in order to counter the loopholes that grey zone activities exploit.

1. Binary security definitions

Delegates can consider changing the current UN definition of armed conflict and states of war, taking into account the conflict that non-direct measures can cause. Instead of using one black-and-white definition of countering armed conflict, multiple definitions and frameworks surrounding grey zone activities can be made. This way, different types of grey zone actions and the harm that they bring can be countered using a multilateral approach. The degree of danger that comes with different types of grey zone activities should also be addressed; for example, economic pressure may pose a different kind of threat compared to proxy military operations, and the international response to each would also be different. Delegates should evaluate various types of grey zone activities, and depending on their stance, draw the line for when simple interference becomes strategic conflict.

2. Accountability

Another key aspect of grey zone activities is the lack of accountability and the use of middleman actors to avoid responsibility. Delegates can consider creating international legal standards that address this issue through investigations and proper preventive actions, again setting a clear line that is able to point out the limitations of using these actors. The systems that already do this also need to become more efficient and work more quickly to address grey zone threats. Additionally, international standards for the prevention of disinformation and manipulation of propaganda in order to sway public opinion should be made to restrict its effect.

Integrated Deterrence

Nations are now creating security systems that utilise every tool of national power, including diplomatic resources, economic leverage and informational tools in order to counter grey zone activities. Grey zone actions are built on ambiguity, confusion, and hidden pressure, so the natural method to counter them effectively is to increase transparency, heighten awareness, and better detection. Delegates can consider building up international systems that enforce strategic exposure, quickening the declassification and publicising grey zone threats. Another solution would be to

increase public awareness of disinformation and create mechanisms that can track and counter disinformation online. These are some examples of defensive measures that ensure a country is always on alert to counter grey zone activities, particularly those using socio-economic soft power.

Past Actions

European Centre of Excellence for Countering Hybrid Threats

The Hybrid CoE is an example of a regional organisation that counters hybrid security threats through networking countries and promoting solutions. The autonomous organisation enables the EU and NATO to work on hybrid threats and conduct exercises together to implement various measures, aiming to become the principle expert organisation in the field encompassing the Euro-Atlantic area. Member states hold conversations on relevant research and exchange of the best countering practices. Delegates can consider drawing from this solution and how to create a similar international organisation or forum that would be able to help increase discussion around countering grey zone security threats on a global scale.

UN Group of Governmental Experts and the Open-Ended Working Group

The UN OEWG and GGE are two parallel groups that aimed to address the legal, technological, and political challenges of cyberspace in the context of international security. It consisted of experts representing UN member states that published reports on how to utilise international law in the context of cyberspace, and the international threats that it posed. This is an example of a specialised area that concerns grey zone security risks (i.e. informational warfare), and delegates can look into the solution to better understand its findings. More importantly, it is an example of how collaborative efforts by the UN can help to yield results that allow nations to better understand how to adapt to new technologies that are involved in grey zone activities.

Indo-Pacific Partnership for Maritime Domain Awareness

The IPMDA was a campaign launched by Australia, Japan, India, and the US to share satellite data on maritime activity with regional partners. The primary objective of the initiative was to enhance maritime security and domain awareness by equipping Indo-Pacific nations with emerging technologies and training support to enhance real-time maritime awareness capabilities. This regional scheme tackles a specific area of grey zone security risks, though it involves more emphasis on physical interactions with different countries on a maritime basis. Delegates can consider referencing similar actions, such as these, which help to strengthen regional security and target perpetrator nations of grey zone activities.

Of course, aside from the mentioned examples above, there are many more collaborative initiatives by countries in order to counter certain aspects of grey zone

security risks. However, there has yet to be a uniform initiative on a global scale that tackles grey zone security risks on an international level – hence delegates can consider the possibilities of creating such a measure, as well as the difficulties that this may pose.

Additional Events

Russian Annexation of Crimea (2014)

From February to March 2014, Russia carried out a military campaign in Crimea, which led to the illegal annexation of the region. It employed methods such as economic manipulation, spreading disinformation and even utilising social media in order to succeed. Most distinctively, Russian forces wore uniforms that did not have any insignia on their uniforms and seized key government and media infrastructure, and despite using Russian equipment, weapons, and uniforms, the Russian government initially denied that they were Russian soldiers, calling them 'local self-defence units'. They painted a narrative of the forces being there only to assist the local Russian-speaking population and were only in the region as lightly-armed 'volunteers'. In order to solidify this narrative, Russia flooded media platforms with pro-Russian sentiment, as well as cyberattacks that shut down Ukrainian government websites and news platforms, creating information vacuums that were filled by Russian propaganda. Russia was able to decisively take action while minimising the footprints that they left, moving quickly to achieve their objectives before foreign states were able to respond and retaliate.

This event is an important example of how governments can weaponise military ambiguity, in combination with isolating regions through cutting off information flow, in order to avoid taking responsibility and direct connection with grey zone activities. These tactics help to shape public opinion in favour of the intrusive state, while also delaying action taken by the international community and minimising confrontation and resistance.

Stuxnet (2010)

Stuxnet is a computer worm that was created with the goal of attacking Iran's nuclear facilities, attributed to joint creation by the US and Israel, leading to the self-destruction of mechanical equipment in Iran's Natanz uranium enrichment facility. This was a significant hit on Iranian military capabilities; again, the speed at which the virus struck left the state unable to react in time, showing how the effectiveness and efficiency of these attacks ultimately outweigh the discretion of originators. US and Israel were able to avoid responsibility through plausible deniability, and this particular cyberattack has become a landmark case of how non-violent and digital means of harm can be incredibly effective.

Cyberattacks similar to this event are being used more frequently as grey zone tactics by national powers and pose a significant threat to international cybersecurity. This is an especially pertinent issue due to the plausible deniability and the underdevelopment of regulatory frameworks / international enforcement mechanisms on this issue. Delegates will need to address how these activities, especially when conducted covertly and swiftly, with a severe need for a strong international framework on how to address such cases.

Iran's Axis of Resistance

The Axis of Resistance is a grey zone strategy that utilises non-state actors, mainly militias, in order to target enemies. It acts as a sphere of influence and extension of Iran by having a strong influence over the militia organisations of the region. The distinction between the national and regional levels allows these militias to adopt narratives to explain their military actions, using two different levels to avoid contradictions. For example, when they are actively attacking American forces, they claim to be part of the 'Axis of Resistance' as an overall Middle Eastern platform, but when they play a defensive part against American forces, they claim to be factions within the Hashd al-Shaabi, the official national Iraqi Iranian-backed entity. Many view the Axis, with its strong support from Iran, as a military instrument to counterbalance American and Israeli influence in the region, while maintaining complete detachment from official declarations of adversary and formal declarations of war.

This is an example of how nations can exert powerful influence over non-state actors that can help to shape the political and military landscape around the globe, all while the originator nation can maintain legal uninvolvement. Delegates will have to consider the use of these actors to maintain national and regional security, while also being manipulated by governments in order to avoid responsibility for provocative actions.

Guiding Questions

1. How is your country connected to grey zone security?
    a. Has your country utilised grey zone security methods in an active or defensive manner?
    b. To what extent are grey zone activities justified and necessary?
    c. Which aspect of grey zone security is the most influential or pertinent?
2. How would your country address grey zone security risks?
    a. Is directly countering grey zone security risks effective?
    b. Are the systems in place currently sufficient to address grey zone security risks?
        i. If not, how can they be changed to do so?

c. How has your country been affected (either positively or negatively) by grey zone activities?

Bibliography

Background Information

- https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/
- https://tnsr.org/2025/06/legal-deterrence-by-denial-strategic-initiative-and-international-law-in-the-gray-zone/#:~:text=Gray%20zone%20activities%20entail%20two,below%20the%20threshold%20of%20war.
- https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/
- https://www.jstor.org/stable/resrep20085?seq=1
- **https://specialforcestraining.info/docs/GrayZones-USSOCOM-WhitePaper9Sep2015.pdf
  The Cold War
- https://www.militarystrategymagazine.com/article/cold-wars-grey-zones-and-strategic-competition-applying-theories-of-war-to-strategy-in-the-21st-century/
- https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf
- https://www.jstor.org/stable/j.ctt130jg8g
- https://www.jstor.org/stable/j.ctt3fh8jd
- https://alphahistory.com/coldwar/coups-proxy-wars/
- https://www.hoover.org/news/hoover-military-experts-chart-history-proxy-wars-ancient-greece-ukraine-and-gaza#:~:text=Major%20ones%20included%20the%20Korean,that%20qualified%20as%20proxy%20wars.
- https://dh.scu.edu/exhibits/exhibits/show/cold-war-global/proxy-wars/cold-war-proxy-wars-s-historio
- https://www.osti.gov/servlets/purl/1456327
- https://polsci.institute/peace-conflict-studies/proxy-war-indirect-conflict-political-implications/
- https://www.history.com/articles/korean-war-causes-us-involvement
- https://www.marshallplan.at/2021-2016/2018/4/8/the-marshall-plan-and-its-meaning-for-today
- https://explaininghistory.org/2025/09/06/the-marshall-plan-strategic-assistance-and-the-reconstruction-of-postwar-europe/
- https://history.state.gov/milestones/1945-1952/marshall-plan
- https://moderndiplomacy.eu/2026/01/24/the-return-of-economic-coercion-how-global-power-is-being-redefined/
  Russian Annexation of Crimea

- https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important#:~:text=Countries%20working%20out%20how%20to,take%20action%20against%20the%20belligerents.
- https://www.brookings.edu/articles/watch-out-for-little-green-men/
- https://www.bbc.com/news/world-europe-26532154
  Stuxnet
- https://www.trellix.com/en-hk/security-awareness/ransomware/what-is-stuxnet/
- https://jasoninstitute.com/in-the-fog-of-cyber-enabled-grey-zone-theyre-not-hiding-anymore-and-thats-the-point/
  Iran's Axis of Resistance
- https://eismena.com/en/article/between-the-hashd-al-shaabi-and-the-axis-of-resistance-the-grey-zone-2024-05-03

Potential Clashes

Binarism
- https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final2-web.pdf
- https://www.thearticle.com/our-binary-understanding-of-war-and-peace-is-not-fit-for-the-21st-century
- https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf
- https://www.icrc.org/sites/default/files/document/file_list/what_is_ihl.pdf
- https://www.aspi.org.au/report/qdr-future-hybrid-warfare/
  Liberalism
- https://www.carlsbergfondet.dk/en/what-we-have-funded/CF17-0723
- https://www.brookings.edu/articles/democracy-playbook-2025/
  Legality
- https://main.un.org/securitycouncil/en/content/purposes-and-principles-un-chapter-i-un-charter#rel2
- https://legal.un.org/repertory/art51.shtml
- https://ccdcoe.org/research/tallinn-manual/
- https://tnsr.org/2025/06/legal-deterrence-by-denial-strategic-initiative-and-international-law-in-the-gray-zone/
  Plausible Deniability
- https://en.kims.or.kr/publication/issue-focus/if-240115/
- https://globaltaiwan.org/2021/06/escalating-clarity-without-fighting-countering-gray-zone-warfare-against-taiwan-part-2/
- https://www.armedgroups-internationallaw.org/2025/06/03/revisiting-plausible-deniability-putins-admission-and-the-wagner-group-paradox/
- https://www.cisa.gov/news-events/cybersecurity-advisories

Key Stakeholder

United States

- **https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf
- https://www.scspi.org/en/dtfx/1571134316
- https://www.aei.org/op-eds/economic-defense-unit-how-the-u-s-military-wins-in-the-gray-zone/
- https://www.bbc.co.uk/bitesize/articles/zg6tg2p
- https://apnews.com/article/national-defense-strategy-hegseth-trump-china-greenland-08fdbe1f8e3f557d688f289fbf4a2c84
- https://abcnews.go.com/US/wireStory/new-us-defense-strategies-differ-traditional-priorities-129516120
- https://abcnews.go.com/US/wireStory/new-us-defense-strategies-differ-traditional-priorities-129516120

Russia

- https://www.canada.ca/en/security-intelligence-service/corporate/publications/hybrid-methods-in-the-grey-zone/military-aspects-russian-grey-zone-activities.html
- https://www.geopoliticalmonitor.com/russias-gray-zone-warfare-campaign-in-europe/
- https://www.rusi.org/explore-our-research/publications/commentary/deterring-kremlin-grey-zone-aggression-against-nato

China

- https://www.csis.org/analysis/signals-swarm-data-behind-chinas-maritime-gray-zone-campaign-near-taiwan
- https://thesoufancenter.org/intelbrief-2025-july-10/
- https://www.sciencedirect.com/science/article/pii/S0308597X24002446

Iran

- https://www.sciencedirect.com/science/article/pii/S0308597X24002446
- https://www.sealight.live/posts/iran-s-maritime-gray-zone-tactics-threats-and-the-strait-of-hormuz
- https://www.sealight.live/posts/iran-s-maritime-gray-zone-tactics-threats-and-the-strait-of-hormuz
- https://www.sealight.live/posts/iran-s-maritime-gray-zone-tactics-threats-and-the-strait-of-hormuz
- https://www.cnas.org/publications/reports/countering-iran-gray-zone#:~:text=Executive%20Summary,conflict%20with%20the%20United%20States

Past Actions

Hybrid CoE

- https://www.hybridcoe.fi/who-what-and-how/
- https://www.eeas.europa.eu/node/33119_en

UNOEGW and GGE

- https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

IPMDA

- https://pacforum.org/publications/pacnet-48-a-work-in-progress-the-indo-pacific-partnership-for-maritime-domain-awareness/