openhouse
choose to be better

Model United Nations 2020

NATO

Study Guide

Agenda: Countering Russian aggression in Eastern Europe and adapting NATO to technological and geopolitical changes

Chairperson: Raunakk Jalan

Vice Chairperson: Aakarsh Bafna

Director: Sahana Shiva

Chairperson's Address

Greetings delegates,

We feel privileged to introduce you to one of the most dynamic committees of the Open house Model United Nations – the North Atlantic Treaty Organization, 2019. NATO was established in 1948 after the scourge of the Second World War to bring about peace in Europe and North America and ensure the joint security of the Western Civilization. NATO became the largest fighting force in the world and a historic military bloc that ensured the survival of democracy, freedom, and liberty through the Cold War and brought about the collapse of the Soviet Union. In the 21st Century, NATO faces a completely changed geo-political scenario and faces the need to adapt to this century, especially with growing Chinese and Russian aggression.

It would be advisable for the delegates to research well for the committee as there will be a significant focus on debate in the committee. However, at the same time, the committee will face multiple crises that require delegates to think on their feet and make solutions to every crisis that is presented before them.

Although this study guide is pretty comprehensive, I would recommend that everyone conducts independent research into the foreign policy of their nations and understands their policies towards NATO – political, militaristic, and economic.

The freeze date for this committee is the **1st of October, 2019**.

Please feel free to contact us if you have any doubts or queries.

We hope you have a great experience at Open house Model United Nations Conference, 2020!

Regards,
Raunakk Jalan,
Chairperson,
North Atlantic Treaty Organization.

Raunakk Jalan (Chairperson), +91 9051167960, raunakkjalan2003@gmail.com

Aakarsh Bafna (Vice-Chairperson), +91 9163675550, aakarsh.bafna@gmail.com

Sahana Shiva (Director), +91 8296472687, sahanashiva17@gmail.com

The North Atlantic Treaty Organization

Ever since the Second World War, NATO has undoubtedly been the most influential and successful collective defense organization. Beginning in 1949, NATO's original purpose was to provide protection to European states against the growing influence of the Soviet Union. Now, more than 70 years later, NATO once again faces its old adversary as well as changing landscape of new security threats. In this committee, we will be discussing how NATO should address these pressing concerns as well as how NATO should position itself to remain relevant in this new global era.

The first major topic area in committee will be NATO's response to Russian aggression in Eastern Europe. Through social media disinformation campaigns, political subversion, and cyberattacks, Vladimir Putin has been orchestrating a pervasive campaign of hybrid warfare to destabilize countries in Eastern Europe. Furthermore, this aggression is more overtly apparent in Russia's annexation of Crimea as well as its military intervention in South Ossetia. In response to Russia's aggression, NATO states have levied economic sanctions on Russia and the alliance has increased military presence and activity in Eastern Europe. Delegates should consider ways in which to best manage the precarious situation, whether it be through taking more aggressive options or considering a more diplomatic approach. Furthermore, in this new era of hybrid warfare, delegates should consider ways in which NATO can successfully counter this devastating new technique of war.

The second topic will be about how NATO should prepare itself for the global and technological challenges that it faces going forward. With China growing and increasingly asserting itself as a global hegemon, it is clear that China is and will continue to be a major geo-political competitor to NATO. Delegates should consider how NATO should approach China through a potential combination of options such as increasing cooperation, engaging with other regional powers such as Japan, South Korea, and Australia, and managing China's investment in important industries related to military and technology of member states. Additionally, delegates should consider how NATO should keep up technologically. Since this has become a new important pillar of defence, it is important for NATO to keep up with the rapid pace of new military technologies.

History of NATO

The predecessor to NATO was The Treaty of Brussels, which was signed on 17 March 1948. When the Cold War began, this was a mutual defense treaty against the Soviet Union. The Western European Union's Defence Organization was created in September 1948, when the threat of the Soviet Union became immediate with the Berlin Blockade. In terms of military power, the partner states were quite weak compared to the USSR. In Czechoslovakia, a coup carried out by the Communists had overthrown a democratic government in 1948. In an attempt to prevent such coups from taking place in other countries of the West, British Foreign Minister Ernest Bevin intended to make a joint Western military strategy formed. The American state saw the situation in Italy and the Italian Communist Party as potential threats. The political developments, Soviet expansionism and anti-communist fervour in Europe proved to be driving forces for this idea.

The foundations of the NATO were officially laid down on 4 April 1949 with the signing of the North Atlantic Treaty, also known as the Washington Treaty. In 1949, the primary aim of the Treaty was to create a pact of mutual assistance to counter the risk that the Soviet Union would seek to extend its control of Eastern Europe to other parts of the continent. The Treaty also required members not to enter into any international commitments that conflicted with the Treaty and committed them to the purposes and principles of the Charter of the United Nations (UN). NATO members formed a unique community of key values committed to the principles of individual liberty, democracy, human rights and the rule of law.

The Treaty derives its authority from Article 51 of the United Nations Charter, which reaffirms the inherent right of independent states to individual or collective defence. NATO states its purpose as “to guarantee the freedom and security of its members through political and military means”. As a political entity, NATO “promotes democratic values and enables members to consult and cooperate on defense and security-related issues to solve problems, build trust and, in the long run, prevent conflict”. As a military entity, NATO exerts military power to manage crises when it is not possible to resolve a conflict through peaceful, diplomatic means.

Role of NATO in the 21st Century

The North Atlantic Treaty Organization was primarily founded in response to the threat posed by the Soviet Union. The Alliance's creation was part of a broader effort to serve three purposes: deterring Soviet expansionism, forbidding the revival of nationalist militarism in Europe through a strong North American presence on the continent, and encouraging European political integration.

NATO has always viewed itself as having three primary responsibilities- collective defense, crisis management, and collective security. The principle of collective defense enshrined in Article 5 of the Washington Treaty is at the very heart of NATO's founding treaty. NATO is viewed by members and non-members alike as Europe's "go-to" organization in those cases where the threat or use of force and is deemed appropriate in and around Europe has found its place as the premier security organization in Europe. It also proved to be more adept at meeting the needs and aspiration of central and eastern European countries yearning to become a recognized part of the west. NATO opened its doors to the east, inviting the Czech Republic, Hungary, and Poland to join while affirming that membership would remain open to all qualified European countries.

Since the end of the Cold War, NATO has slowly adopted a more global perspective. While enlarging its role within Europe through expansion to Eastern Europe and intervention in the Balkans, NATO also began building institutionalized partnerships with states in the former Soviet Union (Partnership for Peace), the Middle East (Istanbul Cooperation Initiative), and North Africa (Mediterranean Dialogue). In the 2000s, NATO had begun taking on more crisis management responsibilities and expanded its partnerships, particularly within the Middle East, and embarked on an extensive military operation in Afghanistan.

NATO's new Strategic Concept, published after the Lisbon Summit of 2010, states that when the alliance identifies threats beyond NATO borders, the organization will "engage where possible and when necessary to prevent crisis, manage crises, stabilize post-conflict situations and support reconstruction."

Emergence of Russia and China as Geopolitical Foes

The Chinese economy is the world's second largest, while its military is catching up with the forces of the US and Russia. NATO's intended role in the Asia-Pacific and the nature of its cooperation with China remain unclear because there is no formal NATO policy on this matter. Stoltenberg pointed out that NATO needs to understand the implications of China’s rise as Beijing expands its power around the world, including areas that may challenge members of the North Atlantic security body.

Great economic might enabled China to invest aggressively in the infrastructure of numerous countries, including its critical elements, putting Chinese in a better position to obtain political support in the questions of e.g. Taiwan and Tibet, and territorial disputes in the South China Sea and East China Sea. Increased naval power in particular makes this part of the Pacific Ocean much more difficult to control for China's potential opponents, primarily US. China is also investing heavily in critical infrastructure in Europe, has increased presence in the Arctic and also Africa, and in cyberspace through international cyberespionage campaigns and special services activities.

Some experts propose a NATO-China Council that would help shape a more cooperative and constructive relationship between China and the West. Already in 2010, former NATO Secretary General Anders expressed a desire for the establishment of a NATO-China Council and stated why NATO should engage China: “China is an emerging power, with a growing economy and increasing global responsibility for security.” Recognizing Chinese role at the world stage and actively approaching them, could help marginalize Russian influence, discouraging them from future actions similar to their involvement in the Ukraine.

Russian Intervention in Europe

The crisis in Ukraine began with protests in the capital city of Kiev in November 2013 against Ukrainian President Viktor Yanukovych's decision to reject a deal for greater economic integration with the European Union. After a violent crackdown by state security forces unintentionally drew an even greater number of protesters and escalated the conflict, President Yanukovych fled the country in February 2014.

In March 2014, Russian troops took control of Ukraine's Crimean region, before formally annexing the peninsula after Crimeans voted to join the Russian Federation in a disputed local referendum. Russian President Vladimir Putin cited the need to protect the rights of Russian citizens and Russian speakers in Crimea and southeast Ukraine. The crisis heightened ethnic divisions, and two months later pro-Russian separatists in the Donetsk and Luhansk regions of eastern Ukraine held a referendum to declare independence from Ukraine.

Violence in eastern Ukraine between Russian-backed separatist forces and the Ukrainian military has by conservative estimates killed more than 10,300 people and injured nearly 24,000 since April 2014. Although Moscow has denied its involvement, Ukraine and NATO have reported the build-up of Russian troops and military equipment near Donetsk and Russian cross-border shelling. In July 2014, the situation in Ukraine escalated into an international crisis and put the United States and the European Union (EU) at odds with Russia when a Malaysian Airlines flight was shot down over Ukrainian airspace, killing all 298 onboard. Dutch air accident investigators concluded in October 2015 that the plane had been downed by a Russian-built surface-to-air missile. In September 2016, investigators said that the missile system was provided by Russia, determining it was moved into eastern Ukraine and then back to Russian territory following the downing of the airplane.

Since February 2015, France, Germany, Russia, and Ukraine have attempted to broker a cessation in violence through the Minsk Accords. The agreement includes provisions for a cease-fire, withdrawal of heavy weaponry, and full Ukrainian government control throughout the conflict zone. However, efforts to reach a diplomatic settlement and satisfactory resolution have been unsuccessful.

In April 2016, NATO announced that the alliance would deploy four battalions to Eastern Europe, rotating troops through Estonia, Latvia, Lithuania, and Poland to deter possible future Russian aggression elsewhere in Europe, particularly in the Baltics. These battalions were joined by two U.S. Army tank brigades, deployed to Poland in September 2017 to further bolster the alliance's deterrence presence.

Ukraine has been the target of a number of cyberattacks since the conflict started in 2014. In December 2015, more than 225,000 people lost power across Ukraine in an attack, and in December 2016 parts of Kiev experienced another power blackout following a similar attack targeting a Ukrainian utility company. In June 2017, government and business computer systems in Ukraine were hit by the NotPetya cyberattack; the crippling attack, attributed to Russia, spread to computer systems worldwide and caused billions of dollars in damages.

The Donbass Region

A political movement calling for the Donbass region to be annexed to the Russian Federation has existed in the region since the late 1990s. This movement was previously made up numerous small, non-influential and disparate groups with diverse ideological and cultural orientations, including Cossacks, paratroopers, Orthodox activists, neo-Nazi-neo-pagans, and supporters of neo-fascist publicist Aleksandr Dugin. In March-April 2014, these ideologically motivated "separatists", to use the Ukrainian terminology, were pushed out of the political arena by the "militia".

These new actors who now appeared on the scene in the Donbass were largely unknown quantities, with no track record in politics or in public life more broadly. They proceeded to use violence as the primary means of solving political problems and eliminating their political opponents. In the first phase, marked by the armed seizure of power in several cities in the region from 12-20 April 2014, the pro-Russian fighters comprised several different groups. The main strike forces were primarily made up of gangs of minor criminals who purchased support amongst the stratum of disaffected and disadvantaged young people known colloquially as gopniki. These criminals had an interest not only in escaping prosecution by the Ukrainian authorities but also in displacing the old mafia bosses dominating the region. The billionaire Rinat Akhmetov is frequently mentioned in connection with the latter. The economic and political elite in the Donbass region, who are closely associated with Akhmetov and who formed the core support for the Party of Regions, clearly did not want the Donbass region to be annexed to Russia, as this would undoubtedly have undesirable ramifications for them, including the redistribution of assets. The lower-level ranks of the criminal and semi-criminal world, on the other hand, from gang leaders through to the corrupt militia officials linked to them at the district level, had much to gain from a radical upheaval of this kind.

The third major group of fighters who took part in the first phase of the "Donbass revolution" in April 2014 comprised special forces (spetsnaz) and GRU and FSB officers (as opposed, that is, to the undercover agents and residents of these same agencies mentioned above). Some of them took part personally in the storming of administrative buildings, while others provided technical and military support to the occupiers. It was members of this group that were responsible for the first two Ukrainian helicopters shot down over Sloviansk on 2 May using MANPADs (surface-to-air defence missiles) manufactured by Russia.

Once some of the airborne forces and spetsnaz troops killed in action could be identified, it became clear that April 2014 had not been the first time that they had visited Ukraine undercover, posing as Ukrainian citizens. Some of them had even posted photos of themselves wearing the uniform of the Ukrainian special police force Berkut on their social network pages. This would suggest that they may already have been operating in Ukraine from late 2013 and opens up the possibility that they may even have been involved in the shooting of the demonstrators on Maidan; certainly, they played a role in the occupation of Crimea.

The fourth group to be involved in the uprising in eastern Ukraine as early as in April 2014 comprised ideologically motivated Russian nationalists who, crucially, were also veterans of various wars and who had been mobilized during the events in Crimea. The best-known figure in this group is the retired FSB colonel Igor' Girkin from Moscow, a historical reenactment enthusiast with a particular passion for the 1918-20 Civil War period. Self-styled successor to a White General, he came to Ukraine accompanied by Cossacks from the radical right-wing organization Volch'ia sotnia (the "Wolves' Company")—a title that also has a connection to the Civil War period,24 and also to a World War Two Nazi collaborationist Cossack unit) from the city of Belorechensk in the Krasnodar region.

The most numerous subgroup amongst the nationalists were the Cossacks, operating primarily under the command of Ataman Nikolai Kozitsyn. Kozitsyn is both a Russian citizen and a native of the Donbass region. In the pre-perestroika era he worked as a guard at one of the region's prison colonies, and later became a prominent figure within the Cossack movement in Russia. The Cossacks played a key role in the seizure of cities in the Luhansk region near to the Russian border and claimed the city of Antratsit as their Cossack "capital".

Russian Disinformation campaigns in Eastern Europe

The European Commission has identified Russian disinformation campaigns as the EU's greatest threat because they are systematic, well resourced, and perpetrated on a larger scale than similar campaigns by any other country, including China, Iran, and North Korea.

According to the commission, disinformation is "verifiably false or misleading information created, presented and disseminated to achieve economic benefits or to intentionally deceive public opinion." The term "disinformation" was introduced to world dictionaries because of Soviet propaganda. In English, the older term "misinformation" was used to describe incorrect information transmitted with the intention of deceiving someone. But disinformation took this to a whole new state level, later abetted by digital reality and social media, which Russia has been quick to harness.

For many years, it was the Russian authorities who feared that Western technological achievements such as the internet, Google, Twitter, and Facebook could be used to impose foreign messages on Russian citizens. The turning point was the Arab Spring, which began in 2010–2011 when people communicated via social media to gather in groups to protest against their regimes. The Russian authorities associated these events with demonstrations in Moscow in 2011 and the prospect of another color revolution—similar to those that overthrew corrupt, authoritarian leaders in various countries during the 2000s.

At that time, then prime minister Vladimir Putin was campaigning for election as Russia's president. He considered the virtual sphere the most important challenge to the stability of his political system. The authorities convinced Pavel Durov, the creator of Vkontakte—the Russian equivalent of Facebook—to sell them shares in the company so the authorities could monitor what the people of Russia was talking about. Later on, the Kremlin demanded the encryption keys to Durov's next invention, the Telegram messaging app. For some time now, the authorities have also been trying to create a Russian internet—Runet—which would allow them to cut off the country from the global network and control society. Russia also uses the global virtual space to achieve foreign policy goals: Russian President Vladimir Putin has long recognized that the internet and social media

gives access to a global audience and to influencing political processes in various parts of the world.

In this way, Russia has gone far beyond the borders of its traditional influence in the post-Soviet region; it now threatens Western democracies and their social order. Russian disinformation is especially prevalent during election season—for example around the 2016 U.S. presidential election and the 2019 European Parliament elections—before key referendums such as the 2016 vote on Brexit, and during large-scale protests such as the ones in Catalonia in 2017 for independence and in France in 2018–2019 with the yellow vests—and now with the coronavirus pandemic.

Most often, the messaging questions the democratic legitimacy of the EU and other institutions and plays up sensitive topics in the public debate, undermining the trust in institutions and in political elites across European societies. In addition, the interpretation of historical events has become a favorite tool of Russian disinformation, mainly because it provokes strong emotional reactions, such as recently when Putin falsely accused Poland of starting World War II and participating in the Holocaust.

The goal is to weaken the EU by polarizing society within individual member states. Through these actions, the Russian authorities aim to influence internal EU processes to Russia's benefit, for example to abolish the economic sanctions imposed after Russia's annexation of Crimea and aggression against Ukraine and to include Russia in the public debate about European security. The Russian authorities' disinformation campaigns use both traditional media and online media, including social media platforms.

Russian pro-government traditional media have a large reach and budget. Two of those outlets, RT and Sputnik, operate in 100 countries and broadcast programs in thirty languages. RT's annual budget of around €270 million allows it to compete on the global news scene with BBC World and France 24, which have similar budgets.

Then there is the Internet Research Agency, which was revealed to be a so-called troll factory owned by Yevgeny Prigozhin, a close associate of Putin. The agency conducts online information operations and is an important part of Russian disinformation activities. Operating since 2013, it has a monthly budget of around €1 million and employs about eighty people divided across foreign sections. The task of the employees—the "trolls"—is to set up fake social media accounts and conduct discussions online with people from all over the world with the goal of inducing extreme emotions and riling up people.

Most often, their posts on social media (Twitter, Facebook, Telegram) and other online platforms (YouTube, Google) question the EU's democratic legitimacy and play up sensitive topics in public debate such as migration, national sovereignty, and values. The channels and disinformation strategies they use depend on the target country and target group of their message, and the effectiveness of it depends on the resilience of societies to counter information, manipulation, and provocation.

With its various methods and channels, Russian disinformation remains a strong tool for contesting the order in Europe. And knowing the strategic goals of Russia's foreign policy, it won't end anytime soon; the European Union must prepare for a long-term campaign of disinformation. Russia is engaged in an active, worldwide propaganda campaign. As part of this campaign, Russia disseminates propaganda to Russian speakers in the Baltics, Ukraine, and other nearby states through a variety of means, including traditional and social media. In some cases, it has used this outreach to sow dissent against host and neighboring governments, as well as the North Atlantic Treaty Organization and the European Union.

The purpose of this study was to examine Russian-language content on social media and the broader propaganda threat posed to the region of former Soviet states that include Estonia, Latvia, Lithuania, Ukraine, and, to a lesser extent, Moldova and Belarus. In addition to employing a state-funded multilingual television (TV) network, operating various Kremlin-supporting news websites, and working through several constellations of Russia-backed "civil society" organizations, Russia employs a sophisticated social media campaign that includes news tweets, non-attributed comments on web pages, troll and bot social media accounts, and fake hashtag and Twitter campaigns. Nowhere is this threat more tangible than in Ukraine, which has been an active propaganda battleground since the 2014 Ukrainian revolution. Other countries in the region look at Russia's actions and annexation of Crimea and recognize the need to pay careful attention to Russia's propaganda campaign.

The Kremlin aims to leverage shared elements of the post-Soviet experience in order to drive wedges between ethnic Russian or Russian- speaking populations who reside in these states and their host governments. Farther abroad, the Kremlin attempts to achieve policy paralysis by sowing confusion, stoking fears, and eroding trust in Western and democratic institutions. To conduct these campaigns, Russia experts argue, Russia employs a synchronized mix of media

that varies from attributed TV and news website content to far-right blogs and web- sites (with unclear attribution), as well as non-attributed social media accounts in the form of bots and trolls.

Russia has been using non-state actors to conduct cyber-attacks on NATO nations to ensure that it is not possible to track it legally to them. These methods have been used to hack critical systems in Eastern Europe, Western Europe, and North America. We strongly suggest that participants research

We would strongly recommend that delegates go through RAND Corporation's study on Russian disinformation campaigns. RAND Corporation is a US Department of Defense associated firm and its research is supported by the Government and can be viewed as extremely credible.

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf

NATO Cyber-Security Frameworks

Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive and coercive. NATO will continue to adapt to the evolving cyber threat landscape. NATO and its Allies rely on strong and resilient cyber defenses to fulfil the Alliance's core tasks of collective defense, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

To keep pace with the rapidly changing threat landscape and maintain robust cyber defences, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the Wales Summit in September 2014. An updated action plan has since been endorsed by Allies in February 2017. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace, seeks to further develop NATO's and Allies' capabilities, and intensifies NATO's cooperation with industry. The top priority is the protection of the networks owned and operated by the Alliance.
The policy also reflects Allied decisions on issues such as streamlined cyber defence governance, procedures for assistance to Allied countries, and the integration of cyber defence into operational planning (including civil preparedness). In addition, the policy defines ways to take forward awareness, education, training and exercise activities, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations. It also foresees boosting NATO's cooperation with industry, including on information-sharing and the exchange of best practices. Allies have also committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber-attacks.
NATO's cyber defence policy is complemented by an action plan with concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships. At the Warsaw Summit in 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. As most crises and conflicts today have a cyber dimension, treating cyberspace as a domain enables NATO to better protect and conduct its missions and operations. At Warsaw, Allies also pledged to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance.

Developing the NATO Cyber Defense capability

The NATO Computer Incident Response Capability (NCIRC) based at SHAPE in Mons, Belgium, protects NATO's own networks by providing centralized and round-the-clock cyber defense support. This capability is expected to evolve on a continual basis and maintain pace with the rapidly changing threat and technology environment. To facilitate an Alliance-wide and common approach to cyber defense capability development, NATO also defines targets for Allied countries' implementation of national cyber defense capabilities via the NATO Defense Planning Process. Cyber defense has also been integrated into NATO's Smart Defense initiatives. Smart Defense enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to free resources for developing other capabilities. The Smart Defense projects in cyber defense include the Malware Information Sharing Platform (MISP) and the Smart Defense Multinational Cyber Defense Capability Development (MN CD2) project. The Multinational Cyber Defense Education and Training (MN CD E&T) project recently concluded its work. NATO is also helping its Allies by sharing information and best practices, and by conducting cyber defense exercises to help develop national expertise. Similarly, individual Allied countries may, on a voluntary basis and facilitated by NATO, assist other Allies to develop their national cyber defense capabilities.

Increasing NATO cyber defense capacity

Recognizing that cyber defense is as much about people as it is about technology, NATO continues to improve the state of its cyber defense education, training and exercises. NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defense elements and considerations into the entire range of Alliance exercises, including the Crisis Management Exercise (CMX). NATO is also enhancing its capabilities for cyber education, training and exercises, including the NATO Cyber Range, which is based at a facility provided by Estonia. To enhance situational awareness, an updated Memorandum of Understanding (MOU) on Cyber Defense was developed in 2015. This updated MOU is being concluded between NATO and the national cyber defense authorities of all Allies. It sets out arrangements for the exchange of a variety of cyber defense-related information and assistance to improve cyber incident prevention, resilience and response capabilities.

The NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE) in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defense education, consultation, lessons learned, research and development. Although it is not part of the NATO Command Structure, the CCD CoE offers recognized expertise and experience. The NATO Communications and Information Systems School (NCISS) in Latina, Italy provides training to personnel from Allied (as well as non-NATO) nations relating to the operation and maintenance of NATO communications and information systems. NCISS is relocating to Portugal, where it will provide greater emphasis on cyber defense training and education.

The NATO School in Oberammergau, Germany conducts cyber defense-related education and training to support Alliance operations, strategy, policy, doctrine and procedures. The NATO Defense College in Rome, Italy fosters strategic thinking on political-military matters, including on cyber defense issues.

Cooperating with partners

Because cyber threats defy state borders and organisational boundaries, NATO engages with a number of partner countries and other international organisations to enhance international security. Engagement with partner countries is based on shared values and common approaches to cyber defence. Requests for cooperation with the Alliance are handled on a case-by-case basis founded on mutual interest. NATO also works with, among others, the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). Cyber defence is one of the areas of strengthened cooperation between NATO and the EU, as part of the two organisations' increasingly coordinated efforts to counter hybrid threats. NATO and the EU share information between cyber crisis response teams and exchange best practices. Cooperation is also being enhanced on training, research and exercises.

Cooperating with industry

The private sector is a key player in cyberspace, and technological innovations and expertise from the private sector are crucial to enable NATO and Allied countries to effectively respond to cyber threats. Through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry. This partnership includes NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information-sharing activities, exercises, training and education, and multinational Smart Defence projects are just a few examples of areas in which NATO and industry have been working together.

Engaging with the Russian Federation

The North Atlantic Treaty Organization has incredible negotiating power when it comes to negotiating with adversaries like Russia. NATO, with a united approach, can counter Russian cyberattacks in Eastern Europe by tracking back all non-state actor attacks to their nation of origin and pursuing action against Russia on the international stage. This also means that Europe needs to reduce its dependence for natural gas on Russia so as to remove the biggest leverage that Russia has that prevents robust NATO action.

NATO should exercise greater economic diplomacy as well bringing about sanctions and coordinating with bodies like OECD, EU, etc.

It will be upon the delegates to come up with technocratic and policy frameworks that work to engage with Russia to ensure that there is continued peace and stability in Europe. Russian disinformation campaigns have brought about political instability in Europe, especially in Ukraine, Albania, Moldova, Serbia, and Greece. It is also widely believed that Russia also promoted instability in the European Union by influencing the Brexit vote.

Budget of the North Atlantic Treaty Organization

Indirect – or national – contributions are the largest and come, for instance, when a member volunteers' equipment or troops to a military operation and bears the costs of the decision to do so. Direct contributions are made to finance requirements of the Alliance that serve the interests of all 30 members - and are not the responsibility of any single member - such as NATO-wide air defense or command and control systems. Costs are borne collectively, often using the principle of common funding. Within the principle of common funding, all 30 members contribute according to an agreed cost-share formula, based on Gross National Income, which represents a small percentage of each member's defense budget.

Common funding arrangements are used to finance NATO's principal budgets: the civil budget (NATO HQ running costs), the military budget (costs of the integrated Command Structure) and the NATO Security Investment Programme (military capabilities).
Projects can also be jointly funded, which means that the participating countries can identify the requirements, the priorities and the funding arrangements, but NATO provides political and financial oversight. The funding process is overseen by the North Atlantic Council, managed by the Resource Policy and Planning Board, and implemented by the Budget Committee and the Investment Committee.

When the North Atlantic Council (NAC) unanimously decides to engage in an operation, there is no obligation for each and every country to contribute to the operation unless it is an Article 5 collective defense operation, in which case expectations are different. In all cases, contributions are voluntary and vary in form and scale, from for instance a few soldiers to thousands of troops, and from armored vehicles, naval vessels or helicopters to all forms of equipment or support, medical or other. These voluntary contributions are offered by individual Allies and are taken from their overall defense capability to form a combined Alliance capability.

The 2% Defense Investment Guideline

In 2006, NATO Defense Ministers agreed to commit a minimum of two per cent of their Gross Domestic Product (GDP) to spending on defense. This guideline principally serves as an indicator of a country's political will to contribute to the Alliance's common defense efforts. Some Allies may need to spend more than this to develop the capabilities that the Alliance asks of them. Additionally, the defense capacity of each member country has an important impact on the overall perception of the Alliance's credibility as a politico-military organization.

The combined wealth of the non-US Allies, measured in GDP, exceeds that of the United States. However, non-US Allies together spend less than half of what the United States spends on defense. This imbalance has been a constant, with variations, throughout the history of the Alliance and more so since the tragic events of 11 September 2001, after which the United States significantly increased its defense spending. The gap between defense spending in the United States compared to Canada and European members combined has therefore increased.

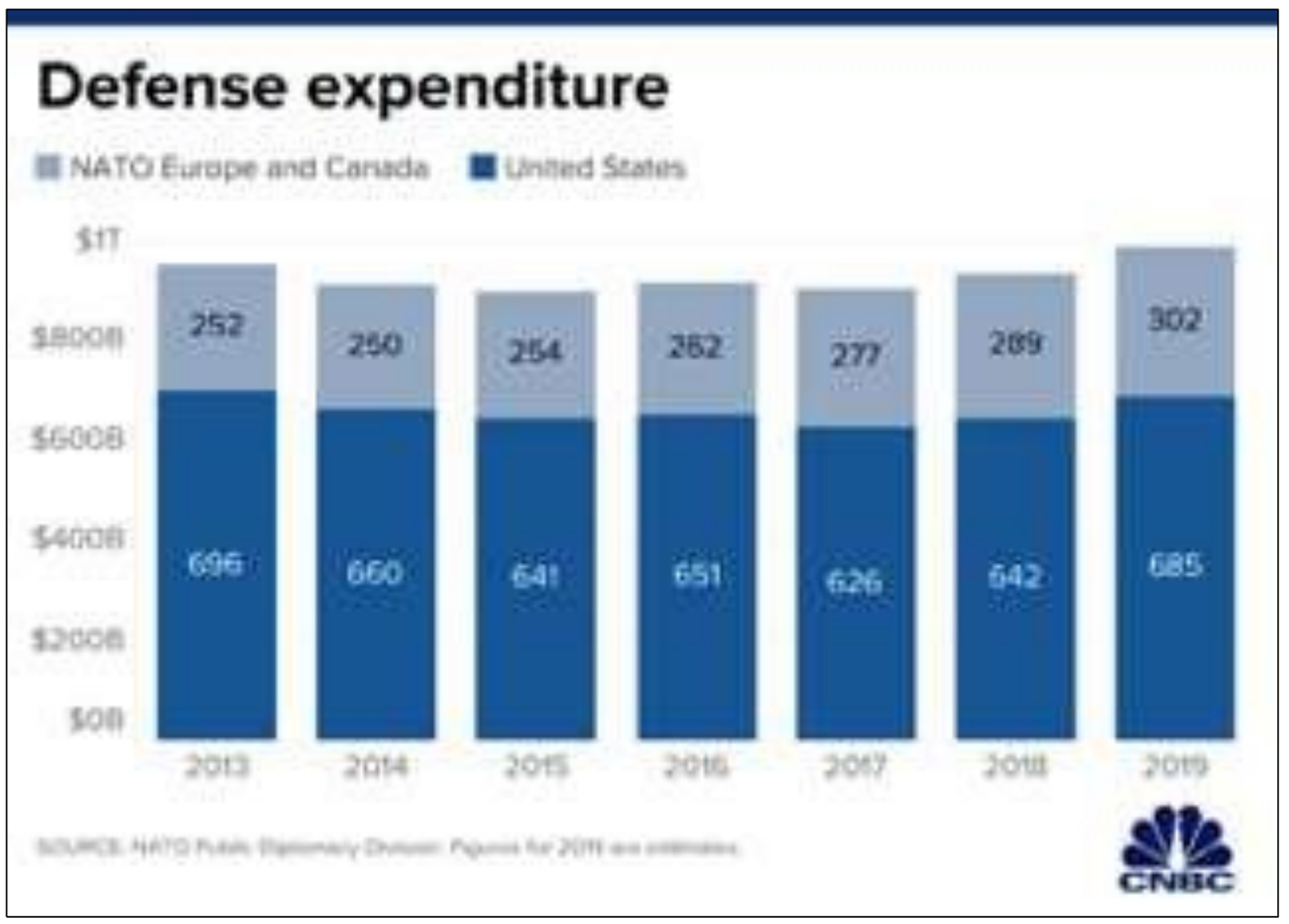
Today, the volume of the US defense expenditure represents more than two thirds of the defense spending of the Alliance as a whole. This is not the amount that the United States contributes to the operational running of NATO as an organization, including its headquarters in Brussels and its subordinate military commands (see table on common funding arrangements for 2020 below). Moreover, the United States' defense budget covers commitments outside the Euro-Atlantic area. However, it should be noted that the Alliance relies on the United States for the provision of some essential capabilities, including for instance, in regard to intelligence, surveillance and reconnaissance; air-to-air refueling; ballistic missile defense; and airborne electronic warfare.

The effects of the financial crisis and the declining share of resources devoted to defense in many Allied countries, up to 2014, have exacerbated this imbalance and also revealed growing asymmetries in capability among European Allies. France, Germany and the United Kingdom together represent more than 50 per cent of the non-US Allies defense spending, which creates another kind of over-reliance within Europe on a few capable European Allies. Furthermore, their defense spending is under increasing pressure, as is that of the United States, to meet deficit and indebtedness reduction targets.
At the Wales Summit in 2014, NATO leaders agreed to reverse the trend of declining defense budgets and decided:

- Allies currently meeting the 2% guideline on defense spending will aim to continue to do so;

- Allies whose current proportion of GDP spent on defense is below this level will: halt any decline; aim to increase defense expenditure in real terms as GDP grows; and aim to move towards the 2% guideline within a decade with a view to meeting their NATO Capability Targets and filling NATO's capability shortfalls.

While the 2% of GDP guideline alone is no guarantee that money will be spent in the most effective and efficient way to acquire and deploy modern capabilities, it remains, nonetheless, an important indicator of the political resolve of individual Allies to devote to defense a relatively small, but still significant, level of resources at a time of considerable international uncertainty and economic adversity. In 2014, three Allies spent 2 per cent of GDP or more on defense; this went up to nine in 2019 and a majority of Allies have national plans in place to meet this target by 2024.



President Trump castigated the leaders of NATO allies to their faces during his trip to Europe this week, suggesting that many of them "owe massive amounts of money" to the alliance. Mr. Trump has a point, but he mischaracterizes the way it works.

What is Mr. Trump's complaint?

"NATO members must finally contribute their fair share and meet their financial obligations, for 23 of the 28 member nations are still not paying what they should be paying and what they're supposed to be paying for their defense," he said. "Many of these nations owe massive amounts of money from past years and not paying in those past years," Mr. Trump said. "Many of these nations owe massive amounts of money from past years and not paying in those past years," Mr. Trump said.

It is important for the delegates to understand the multitude of issues surrounding budgetary contributions by member countries to NATO and the utilization of those funds. These issues highlight the need for financial reform within the NATO, and delegates are expected to discuss this in committee, since an optimal budget needs to be attained in order to fully adapt to the technological and geopolitical changes around the world.

Considering the fact that the 2% contribution recommendation is merely a guideline and not a requirement enforced by the NATO charter, an important issue for discussion in committee is whether or not percentage contributions proportional to the GDPs of member states must be made a legal requirement.

Emergence of China as a Geopolitical Foe

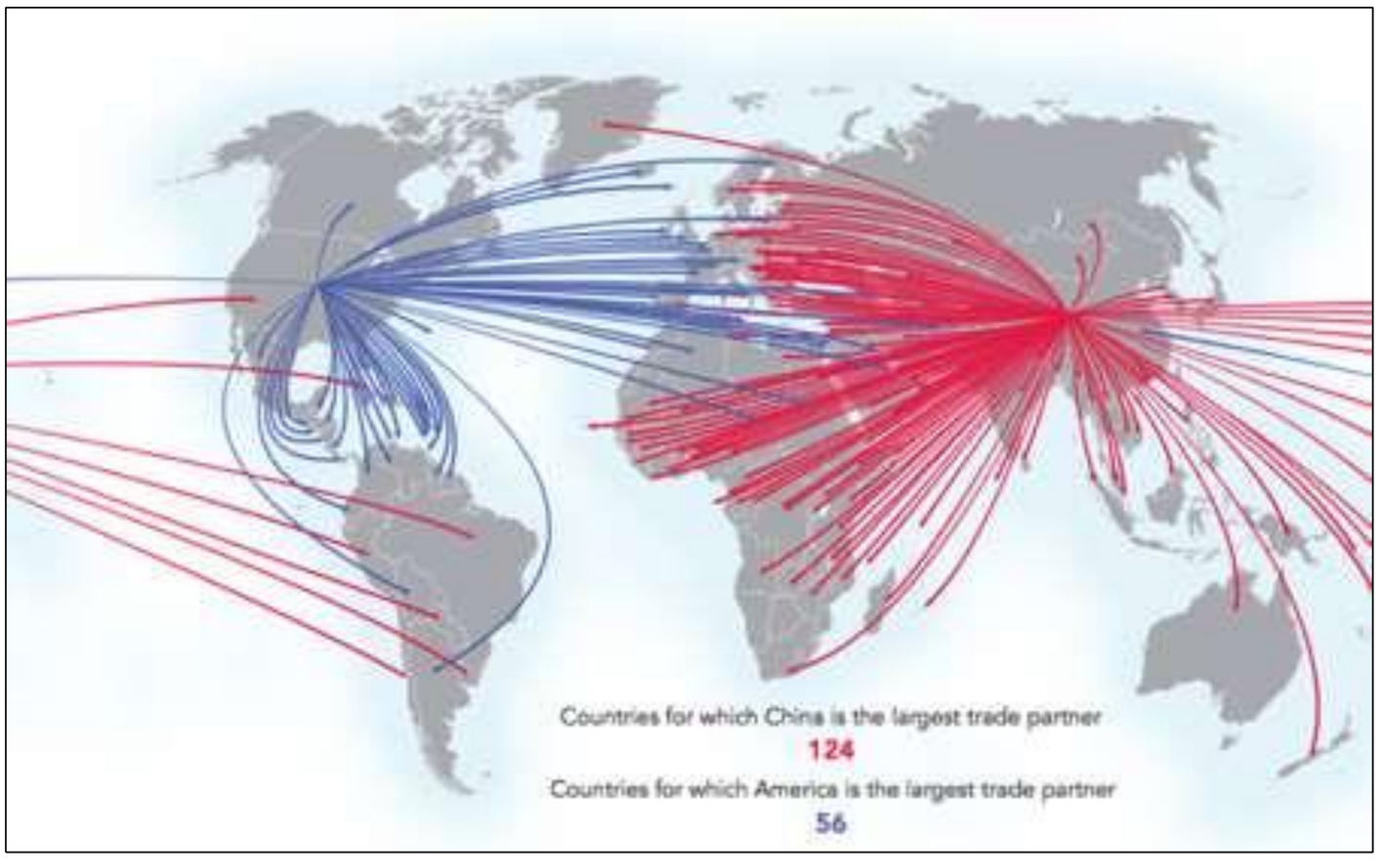
World order refers to dominant values, rules, and norms that define the terms of global governance and give shape and substance to international society at any given time. Historically, great powers have been the rule-makers of world order to reflect their values and interests, weak states the takers, and dissatisfied emerging powers the breakers, pursuing alternative principles to conform to their distinctive preferences.

After the end of WWII, the US as the rising hegemon was in a unique position to construct the rules and institutions that have had a profound impact upon the development of the world order. While the US has benefited immensely, its allies blossomed economically and continue to enjoy the benefits of the post-1945 order. China is also a beneficiary after Deng Xiaoping started reform and open-up in the late 1970s.

Rising as a great power in the 21st century, China has to decide whether it can live with the US-led order or creates a new order to sit alongside or even overtake it. China's rise, therefore, has led to the debate if China will become a stakeholder or a dissatisfied-revolutionary power. While the liberal view assured that "the rise of China does not have to trigger a wrenching hegemonic transition" because the world order built under the US leadership is based on rules and norms of non-discrimination and market openness, creating conditions for rising states to advance their expanding economic and political goals within it, many in the US and globally have increasingly worried that a rising China may want to challenge the US leadership and overhaul the underlying rules of the existing world order.

There is a tremendous difference between views, perception about views, and perception from the media and the reality. It is true that China is rising, both economically and militarily, and at the same time, it is growing its assertiveness with other nations. The most important problems include high and rising inequality, corruption and persistence of poverty, environmental pollution, and over dependency on non-renewable resources. All these problems could loom so large that China may become vulnerable to various crises. World Bank reports that, China's GDP is about 5 percent (14 percent in PPP terms) of the world total but it consumes more than one-third of the world's outputs of coal, steel, and cement. China's past pattern of industrial growth is unlikely to be sustainable in the future. In addition to that, China is spending high on its military, but the country is still behind the most powerful militaries in the world in terms of equipment and training. Equally important is the lack of combat experience, as China hasn't engaged in combat with a foreign enemy

since Vietnam in 1979. The lack of experience in comparison to countries such as the US, UK, and Russia places China at a disadvantage. However, rising inequality and corruption are two majors social and political issues which can render China vulnerable
to social and political unrest, causing unwanted disruption to its economic progress. Although China's economy is ranked as the second largest economy in the world, its per capita income is still low. A significant segment of the population still lives in poverty. Moreover, China is an export-oriented economy. It relies on its exports to increase on its growth. Also, the United States economy is by far larger than that of China with over 20 percent of the world output. Geographically, China's potential for territorial growth is
severely limited by geography. To the west, it faces the Barren Tibetan plateau and Gobi district. To the south, the Himalayan Mountains present an imposing barrier to the Indian subcontinent. To the north, vast and largely empty grasslands known as the Steppes provide a buffer with Russia. And to the east stretches the world's largest ocean. So aside from the hapless Vietnamese who share the southern coastal plain and China's historical claim to Taiwan, there is not much opportunity for wars of conquest on China's periphery.



China's rising dominance in trade:

The infrastructure override-The AIIB (Asian Infrastructure Investment Bank), which was officially launched at the end of last year. Initially proposed by China, the bank now has over a $100 billions of capitalization and 57 founding member states. While this shows China's push for infrastructure specially to coincide with its new Silk Road, there is another very interesting detail: Beijing controls 26.06% of the votes, essentially giving it veto power as most bank decisions need 75% of the votes to pass. In other words, only infrastructure projects that benefit Chinese trade will likely get the nod from Beijing.

Guidelines for Delegates

1. Events in the world outside the committee may change as the crises at hand progress, which the members of the NATO may have to react to.

2. Each session of the committee shall have the right to invite an outside observer or representative.

3. Delegates will be allowed to communicate with their, as well as other nations' governments, - even third parties if they wish to - through means of communiqués. This can enable them to take decisive action on their own. However, these actions should be realistically achievable and detailed.

4. For the purpose of productive debate and discussion, the Executive Board may deviate from standard procedure, in accordance with the provisions of the UNA-USA Rules of Procedure.

5. While drafting communiqués, please keep them as practical and pragmatic as possible. The Executive Board will not look favorably upon communiqués that cannot in any way be implemented in reality.

6. While communiqués are important, they will not be given as much weightage as speeches and points. Please keep in mind that the Executive Board will mark you on the basis of quality, not sheer quantity

We hope you have a wonderful time at the committee. Delegates are free to contact the Executive Board to clear any doubts they may have.

Paperwork in Committee

1. Position Papers

A position paper is the first piece of paperwork submitted by a delegate for the conference. It is a summary of the stance of the country the delegate is representing on the agenda of the concerned committee.

The structuring of the Position Papers is intended to elicit responses from the delegates that provide a clear picture of a nation's stance on a particular topic area. By providing an outline of a Position Paper, we hope that delegates will be able to illustrate clear knowledge of their country's policies and interests instead of simply regurgitating parts of the Study Guide. However, all delegates should also read the section on Position Papers in their study guides and heed their Executive Board's specific instructions.

A Position Paper should include three sections, outlined below:

Brief statement of issue:

In your country's opinion, what are the main elements of the problem, and what caused it?

Your country policy on the agenda:

What are your national interests in the situation?

What are your nation's policies on the topic?

What steps would you like to see taken to deal with the problem?

Proposed solutions:

What does your nation believe needs to be done to solve the problem?

What do you predict will be the main opposition to your proposals?

2. Communiques

These are official messages, formal diplomatic requests, proposals, or demands to other states, non-state actors, individuals, or entities and the committee itself. A communique must be issued, for example, to officially propose some sort of agreement or accord to another organization.

A communique is of two types :

Private Communiques :
A private communique is not disclosed to the committee. Only the Executive Board Members are privy to it and reply accordingly.

Public Communiques :
A public communique is read out in the committee.

Communiques, both public and private, are not voted upon. They are implemented as per the discretion of the Executive Board.

Examples of Communique's:

COMMUNIQUE I

From: Hugh Dalton, Minister of Economic Warfare, Churchill's War Cabinet
To: Section X of the Special Operations 'Executive, operating in Berlin.
Speak with Klaus in Berlin. Activate our spy network.
Follow Hitler's nephew studying in the National Political Institute of Education, who is also secretly involved with the Luftwaffe.

COMMUNIQUE II

From: Delegate of the United States of America
To: Director of the National Security Agency Content:
Say "hello" to Angela Merkel and Dilma Rousseff.
Note: Say "hello" is the code-word to wire-tap a conversation between two entities.

Recommended Topics for Research

- NATO charter
- Military structure of NATO
- Budget of NATO in the 2010s
- Technological capabilities of NATO
- Russian Aggression in the Donbass region
- Ukraine Political Structure
- Rise of Far-Right movements in Poland
- Russian bot farms and cyber warfare
- Russian use of non-state actors to conduct cyberwarfare
- Use of Oil Supply by Russia to leverage Europe
- Use of financial instruments like debt instrument ownership by China
- Trade Dominance strategies conducted by China

These topics are just a recommendation from the Executive Board for research. Research on these topics will help delegates in committee and for all forms of paperwork. These topics may be raised for discussion in committee. However, it is the recommendation of the Executive Board that research on these topics be used to augment other topics.

For any clarifications whatsoever, feel free to contact any of us.