North Atlantic Treaty Organisation

Countering the threat of hybrid methods of warfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Floor Runge

Forum: North Atlantic Treaty Organisation (NATO)

Issue: Countering the threat of Hybrid methods of warfare

Student Officer: Floor Runge

Position: Deputy President of the North Atlantic Treaty Organisation (NATO)

Introduction:

Hybrid methods of warfare are defined by the North Atlantic Treaty Organisation (NATO) to “combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces.” These forms of warfare are a threat to many countries, however the most outstanding modern example is the Crimean Crisis. In most cases, hybrid methods of warfare are used to target a country’s vulnerabilities; in the case of Crimea, a group of popular opposition sympathisers known as the “little green men,” were in fact Russian Special Forces with their insignia removed. These undercover Russian forces had used the trust and confidence that the Crimean people had granted them in order to confuse the opposition and convince people of the Russian goals. Since this crisis, both NATO and the European Union (EU) have offered their support to Ukraine through starting discussions regarding Russia’s actions in relation to hybrid methods of warfare. The difficulty in moving support further than simply initiating discussions lays in the nature of hybrid threats such as the one in Ukraine. This can be very clearly explained using the definition for hybrid methods of warfare proposed by the EU, which states that such threats “remain below the threshold of formally declared warfare.” Although the Crimean Crisis is a very clear example of this issue, there are a multitude of different crises where hybrid methods are used in order to target a specific weakness in order to incite unrest. For example, the Islamic State advancement into Syrian territory. In this case, the Islamic State of Iraq and the Levant use hybrid methods of warfare against the official Iraqi military. Another case where hybrid methods were used, was by the People’s Republic of China in the South China Sea against Taiwan; in both the examples propaganda and a strong online presence were used to confuse the targeted population, and create civil unrest.

Definition of Key Terms:

Hybrid Methods of Warfare:

The definition provided by NATO is that such methods, “combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations.” (NATO) In a variety of different statements, both the EU and NATO have been known to often refer to Hybrid threats as threats on democratic institutions.

Democratic Elections:

A democratic system allows for the citizens of a country that are of voting age, to vote for the person or party they wish to run their country. A person or party is often chosen based on political beliefs and ideas in order to assure that decisions and politics are implemented on the basis of those common beliefs.

Cyberattacks:

Cyber attacks are performed within cyberspace, and, with the use of one or more computers, attempt to steal information or disable a network. In the context of hybrid methods of warfare, this refers to an organisation or state stealing intelligence or spreading false information in order to undermine a targeted nation.

Collective Security:

When there is a cooperation amongst a group of allies in order to strengthen the security of each individual nation. A good example of collective security is NATO, where an attack on one ally means an attack on every ally. The military cooperation between each of NATO’s allies means increased security for each ally individually.

VKontakte:

VKontakte of “VK” is a Russian social media platform that experiences heavy influences from the Kremlin. VKontakte, originally inspired by apps such as facebook and twitter, is now used by over 100 million active participants, mostly Russian nationals. In 2014 liberal CEO Pavel Durov was fired and forced to leave the country because he had not been operating in the Kremlin’s favour. The new CEO, Alisher Usmanov, is known to be a close friend of Poutin’s and has been known to have granted Russian internal security

(FSB) full access to user's information. The Strategic Communications Centre of Excellence has been monitoring activity on VK over the past few years, and each quarter brings out a report on the quantity of bots and their actions circulating the platform.

General Overview:

History:

The most obvious example where hybrid methods of warfare were used in order to achieve a military or political goal was with the crimean crisis; although this example has already been explained above, a quote by NATO Secretary General Jens Stoltenberg very perfectly describes the goals of using such hybrid methods in a speech. He stated that, "[with the use of] proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability." These characteristics are not unique to the Crimean Crisis; both during the invasion of Syrian soil by ISIS, or the Chinese aggression in the South China Sea, methods of intimidation, propaganda and confusion were used to attain a certain goal.

What makes these methods of warfare so difficult to combat and take preventative measures against are the variety of different forms these methods occur in. Every threat is different and in most cases it toes the line between peace and wartime, which creates confusion amongst the targeted population especially because these threats are not always immediately recognised and categorised. The lack of international legislation regarding these methods is another factor that hinders a country's ability to counter a threat; hybrid threats have only recently become an important discussion on the international political stage, and so more antiquated military legislative systems such as the Geneva Convention have not defined nor set out guidelines for such threats.

Increasing Relevance/Cooperation:

Debate on the topic of hybrid methods of warfare became relevant in NATO circles with a speech by NATO Secretary General Anders Fogh Rasmussen at the Atlantic Council of the United States in Washington in July of 2014. This speech referred to Russian aggression in the Baltic States as a good example of hybrid methods of warfare, which since then, referring to the Crimean Crisis, has become a topic that is very commonly discussed during conventions by NATO regarding hybrid warfare.

This speech also highlights the necessity of a very important aspect of the discussions after 2014, which is the cooperation with the European Union; this is due to the hybrid nature of such methods, meaning there is a simultaneous use of political and military measures. As the EU is a political organisation whose member states align mostly with NATO's allies, this partnership between politics and economics will be vital to combat hybrid threats especially those in the european theatre.

Cooperation is not only vital between organisations such as NATO and the EU, but global cooperation in creating international legislation and systems to allow for resilience and prevention. A good example of such a cooperation is between Finland and the EU/NATO; Finland has hosted a multitude of conferences and discussions regarding this issue, and has aided in the creation of the hybrid Centre of Excellence, this has allowed for international experts, think tankers and political/military leaders to work together which has allowed for the creation of viable.

An example of a think tank involved with legislation regarding hybrid methods of warfare is the group Politikon Network in Montenegro; this group has a myriad of projects on the topic of hybrid methods of warfare, however, the most outstanding at the moment is, "New Perspectives on Shared Security – NATO's Next 70 Years: Wars of ideas. Hybrid warfare, political interference and disinformation." This project is funded by the NATO Public Policy Division and has been allocated 8010 euros. The first panel discussion was held in June of 2019, however there have been no detailed publications of the discussions since.

Major Countries and Organisations Involved

Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats:

The Hybrid CoE is one of the many CoE's established by NATO, in order to provide a platform for experts to discuss topics relevant to NATO's goals. This centre focuses on the prevention of hybrid attacks, and works towards helping countries develop their military-civil capabilities in preventing and countering a hybrid attack.

As of now, the Hybrid CoE has three communities of interest (COI). The first is the Hybrid Influence COI; this COI looks at how hostile states actors attempt to sow seeds of instability within a targeted nation in order to undermine a country's sovereignty. The goal of this COI is to prepare and instruct nations on how to "respond and deter hybrid attacks." (Hybrid CoE) The second community under this centre of excellence is the

Vulnerability and Resistance COI, which identifies a country's vulnerabilities and aids in the protection of those areas of weakness in order to eliminate possible grounds for a hybrid attack. The last community is the Strategy and defence COI which “aims at discovering the essence and nature of hybrid warfare as well as the logic and pattern of hybrid strategies in order to develop an analytical framework for the assessment of current and future hybrid warfare situations and their practical implication.” (Hybrid CoE)

The Hybrid CoE hosted its first conference in June of 2019, which was attended by 22 EU and NATO nations including Georgia, Singapore and Australia. The topics discussed at this “deterrence conference” included, “the value of attribution, private-public partnerships and collaborative working,” where attribution refers to assigning the cause of an event to a person or thing. The conclusions drawn from the discussions held at this conference are very similar to those drawn previously at conferences such as the *Critical Connections, Continuity and Supply* conference in 2019 and are not worth commenting on in depth.

The Hybrid Centre of Excellence also functions as a neutral facilitator between the European Union and NATO in continuing talks and discussions regarding protection and resilience of countries against hybrid methods of warfare, which remains vital in order to maintain a framework for establishing common policy across member states of both organisations and their allies.

Other Centers of Excellence:

The Strategic Communications Centre of Excellence:

Located in Riga, Latvia, the Strategic Communications Centre of Excellence, focuses on starting and continuing conversations regarding what they have called, “robottrolling,” and frequently brings out publications regarding these topics. It is clear from these publications that Russian social media platforms such as “VK” are often the subject of their investigations. This centre of excellence is greatly focused on the public image of NATO and its operations, most importantly influencing the perception, attitude and behaviour, affecting the achievement of political and military objectives with the use of a strategic online presence.

The Cooperative Cyber Defence Centre of Excellence:

This NATO based centre of excellence focuses on “research, training and exercises in four core areas: technology, strategy, operations and law.” The most important and effective focus of this centre is training all NATO bodies, including both member nations and allies, in detecting cyber attacks, preventing cyberattacks through policy making, and protecting information infrastructure in their country. This CoE prides itself on both its interdisciplinary nature and international cooperation which functions as both an asset and a challenge. Because experts and policymakers from over 20 nations are

involved, it is often difficult to reach a common conclusion, however this also allows any conclusions made to be very widely implemented.

The Energy Security Centre of Excellence:

This centre of excellence based in Latvia, focusses on the development of energy efficient military forces, and the protection of energy infrastructure. This centre, unlike the other two, isn't focused as much on detecting hybrid attacks, but rather on protecting nations from them, and developing a viable military force against them. This CoE won the Energy Transition Trophy in 2016, which, as stated by Deputy Director of NATO ENSEC COE Lieutenant Colonel Nicolas Henry, “is validation and recognition of our work and international cooperation. This project was recognised by experts from civilian organizations, therefore it means that Energy Transition is essential not just for civilian world but also for military.”

European Union and NATO:

The European Union defines hybrid warfare as, “methods or activities used by hostile state or non-state actors in a coordinated manner in order to target the vulnerabilities of democratic states and institutions, while remaining below the threshold of formally declared warfare.” (EU Council) In this definition, only democratic states and institutions are elected as victims of a type of threat, which is an opinion that is shared with NATO. This becomes clear in a speech by NATO Deputy Secretary General Mircea Geoana, who “states that, “cyber-attacks and hybrid attacks, disinformation campaigns, attempts to interfere with our democratic processes.” (Mircea Geoana). From these two definitions of hybrid attacks by the EU and a representative of NATO, it has become clear that these organisations experience hybrid warfare as an attack on the foundation of democracy.

Another thing that is clear for both these organisations is their focus on the Russians with regard to this topic. This becomes increasingly clear when reviewing the publications by the NATO-run Strategic Communications Centre of Excellence, but also in the new conclusions of countering hybrid attacks adopted by the European Union Council in December 2019. This could be due to the increasingly un-democratic and militaristic behaviour on behalf of the Kremlin - for example the illegal annexation of Crimea, the deployment of new nuclear-capable missiles, or the recent passing of a referendum allowing Putin and extra 12 year term - which is making organisations such as the EU and NATO uncomfortable. This increasingly abnormal monitoring of the Russian situation with regards to this issue could also explain why both the EU and NATO have explained hybrid warfare to be an attack on democratic beliefs.

Finland:

Although Finland is not a NATO member, its involvement in this issue is extensive. As the sponsor and host state of the Hybrid CoE, Finland is the instigator and host to many conferences regarding hybrid warfare. For example, Finland was one of the co-hosts of the *Critical Connections, Continuity and Supply* conference in 2019. Its recent heavy involvement with this issue is due to the election of Finnish president, Sauli Niinistö, whose goal is to strengthen EU member states' capacity to prevent and respond to hybrid methods of warfare, by primarily spreading and increasing awareness on the topic.

Timeline of Events

July 2014	Speech by NATO Secretary General Anders Fogh Rasmussen
March, 2014	Crimea Crisis
June, 2014	ISIL advance into Syria
July, 2016	Warsaw Summit NATO
July, 2016	Establishment of the Joint Intelligence and Security Division
July 2018	Brussels Summit NATO
19 April, 2019	EU introduces new conclusions on countering hybrid threats
November, 2019	Critical Connections, Continuity and Supply Conference Finland
December 2019	New conclusions adapted on hybrid threats for use by the EU Council

Relevant Treaties and Events

Critical Connections, Continuity and Supply

A conference co-hosted by the Finnish Presidency of the Council of the EU and the EU Institute for Security Studies. Although Finland, as the sponsor for the Hybrid CoE, is not a NATO ally, it has been known to work very closely with NATO on this issue, which was exemplified even more by its president and his very clear interest in the subject.

This summit brought together representatives of NATO, the European Council, members of the Private Sector and international think tankers. This international cooperation is highly necessary in order to accomplish the goal of encouraging cross-border and cross-sectoral cooperation in the EU, which was decided is necessary in order to combat hybrid methods of warfare.

2016 Warsaw Summit (NATO)

During this summit it was decided that there would be an effort to increase the cooperation between the European Union and NATO in order to increase maritime security and countering hybrid and cyber attacks. Although it was decided to increase cooperation, a motion by Romania to increase NATO presence in the Black Sea was opposed by Turkey and therefore was not seen through. This motion would have directly increased maritime security in the area which completely aligns with the motives agreed on during the summit. The increased cooperation in this area would work towards solving issues such as the ones posed by China in the South China Sea. During this summit it was also decided to increase aid to Ukraine, especially in countering hybrid threats of warfare through strategic advice and assistance.

2018 Brussels Summit (NATO)

This Summit in Brussels reacknowledges the Ukrainian struggle against hybrid threats and proposes to support Ukraine in building up resilience against these threats by “intensifying activities under the NATO-Ukraine Platform on Countering Hybrid Warfare.” Clause 21 of this summit also highlights the increasing threat that hybrid methods of warfare pose to the international community. It is stated that in the case of an armed attack, article 5 of the Washington Treaty could be invoked, which states that an attack on one nation is an attack on all allies. During this summit, the creation of the Counter Hybrid Support Teams was also announced, which will become a team that works to provide tailored assistance to allies in order to prevent or deter hybrid attacks.

Previous Attempts to Solve the Issue

European Union:

Wishes to take “a comprehensive approach with more cooperation, more coordination, more resources and more technological capacities in order to address this challenge.” (Council of the EU) This includes increased cooperation with international partners and allies, in particular the EU-NATO cooperation which will prove to be vital in

dealing with hybrid warfare in the European neighborhood. Another goal of the new EU council conclusions on this topic includes taking into consideration the possibility of hybrid attacks “when developing and using new and emerging technologies, including artificial intelligence and data-gathering techniques, and when assessing the impact of foreign direct investment or future legislative proposals.” This goal will require increased cooperation amongst states, and continued communication and transparency amongst nations globally. The last point that is discussed by the EU in their conclusions, is the protection and reinforcement of both international and national infrastructure, in order to be able to be protected from but also counter hybrid attacks.

NATO:

NATO places the primary responsibility of dealing with a hybrid attack on the targeted nation; despite this, NATO will assist any ally in countering such attacks as this is part of the collective defense clause. During the 2018 NATO summit in Brussels, NATO leaders agreed to construct a counter-hybrid system which will work to provide “tailored targeted assistance to Allies upon their request.” (NATO) This, just as was the case with the EU conclusions, will require extensive cooperation amongst not only the allies but also with separate partners.

In 2017, the establishment of the Joint Intelligence and Security Division marked a significant turnaround for the course of debate surrounding the countering of hybrid attacks. The goal of the JISD was to “establish a professional workforce, and initiate a broad series of reforms to improve the quality and utility of intelligence provided to NATO’s most senior political and military leaders.” (Arndt von Loringhoven) This made the transfer of information swifter and more efficient, and eventually allowed for better and more effective policy making.

Possible Solutions

1. Complete Transparency

Allow for valuable military information regarding hybrid attacks to be shared amongst nations in order to create awareness and allow nations to prepare for similar attacks. This could be done through the establishment of an international database, or specialised centres of excellence such as the European Centre of Excellence for Countering Hybrid Threats; this can only be possible through full international

cooperation, which is something emphasised by both NATO and the EU during the Warsaw and Brussels Summit.

2. Clear international laws and regulations

Initiate discussions with world leaders to create new international rules and regulations, or amend antiquated rules and regulations, to allow for the definition of hybrid methods of warfare in conventions such as the Geneva Convention. In many cases hybrid methods of warfare blurs the thin line that separates peace and wartime. This is what makes these methods so powerful because it creates such an extent of uncertainty and confusion in a country. If hybrid methods of warfare are clearly defined internationally, this aspect of confusion is eliminated.

In every case it is important to take into consideration that hybrid methods of warfare are neither categorised as war nor peace between nations, therefore, every solution or precaution that is taken must be non-violent, diplomatic and peaceful; this is vital in order to prevent unnecessary conflict. NATO strives “to safeguard the freedom and security of all its members by political and military means,” this freedom would be taken away if a nation were to plummet into war because overly aggressive measures were taken.

Bibliography:

“Council Conclusions on Countering Hybrid Threats.” *Consilium*, 19 Apr. 2016, www.consilium.europa.eu/en/press/press-releases/2016/04/19/fac-conclusions-hybrid-threats/.

“The European Centre of Excellence for Countering Hybrid Threats.” *Hybrid CoE*, www.hybridcoe.fi/communities-of-interest/.

Loringhoven, Arndt Freytag von. “A New Era for NATO Intelligence.” *NATO Review*, Nato Review, 29 Oct. 2019, www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html#:~:text=The%20most%20significant%20reform%20came,(JISD)%20at%20NATO%20Headquarters.&text=The%20establishment%20of%20the%20JISD,military%20division%20at%20the%20Headquarters.

“The NATO Cooperative Cyber Defence Centre of Excellence.” *Training*, ccdcoe.org/training/.

“NATO Strategic Communications Centre of Excellence Riga, Latvia.” *StratCom*, 9 Dec. 2019, www.stratcomcoe.org/.

“Shifting Paradigm of War: Hybrid Warfare.” *Hybrid Warfare*, msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf.

“Warsaw Summit Key Decisions.” *North Atlantic Treaty Organisation*, 2017, Warsaw Summit Key Decisions.