

FMUN 2018

North Atlantic Treaty Organization

Written by: Brenda Jones

Topic I: Further Development of Cyber Defense Capabilities

Topic II: NATO-Russian Relations

Dear Delegates,

Welcome to the 2018 Florida Model United Nations Conference! We are pleased to announce one of the committees at this year's conference is the North Atlantic Treaty Organization (NATO). My name is Brenda Jones, and I will be serving as your director of NATO for FMUN 2018. I am majoring in International Affairs, concentrating in Political Science, and minoring in Computer Science at Florida State University. This is my first year on staff for FMUN.

The topics under discussion for the North Atlantic Treaty Organization are:

- I. Further Development of Cyber Defense Capabilities
- II. NATO-Russian Relations

NATO is under the auspices of the Declaration of the United Nations but is a political and military alliance much different than any UN committee. NATO has addressed numerous security issues facing the Euro – Atlantic area such as Women in Peace and Security, counter-terrorism, counter-narcotics, cyber defense, and conflict resolutions just to name a few.

This Background Guide will be a key resource in beginning your understanding of the North Atlantic Treaty Organization, its functions, and the topics that will be discussed at the conference. Delegates are expected to expand their research beyond this background guide by using the footnotes and researching specifics about their Member State they will be representing. When writing their position papers, we will be looking for a complete understanding of their Member State's views regarding both topics along with solutions that can apply to the international community. When preparing for the conference delegates are encouraged to use the preparation tools on the website regarding research, position paper formatting and content, dress code, and what is expected on the day of the conference.

We look forward to your participation in Florida Model United Nations 2018!

Sincerely,

Brenda Jones, *Director*

Committee Overview

Introduction

The North Atlantic Treaty Organization (NATO) is a political and military alliance which has 29 member countries.¹ Militarily, NATO is committed to peaceful resolutions of disputes, but where diplomacy fails NATO has the military capacity to take action with crisis-management operations; these powers have been granted to the organization by NATO's founding treaty as well as the UN charter.² Politically, NATO promoted democratic values and facilitated consultation and cooperation between members on security-related issues and defense to help build trust amongst the members as well as solve problems and prevent conflict in the long run.³ All NATO member countries are in Europe with the exception of the United States, Canada, and Turkey (which connects Europe to the Middle East), and NATO membership is "open to any other European state in a position to further the principles of this treaty and to contribute to the security of the North Atlantic area."⁴

History

At the end of World War II disputes over reparations and peace agreements exacerbated tensions between Soviet and Western powers given their differences in political ideologies and conflicting interest in the region.⁵ When WWII ended Western forces began demobilizing their defense forces and reducing their establishments; In Eastern Europe, the Soviet Union was expanding their power in many countries.⁶ This expansion in Eastern Europe worried Western Europe, especially the United Kingdom, and lead to a call to action where a British Foreign Secretary claimed there was a need for a regional defensive alliance under the auspices of the UN charter.⁷ During this time the United States Senate adopted the *Vandenberg Resolution* which allowed the US to participate in mutual defense in times of peace constitutionally; this dramatically changed the course for US foreign policy, but the US would only allow military support as long as Europe was united.⁸ In response, the Western Union was created by the Brussels Treaty in 1948, and this included Belgium, France, Luxembourg, the Netherlands, and the United Kingdom.⁹ The Brussels Treaty became the basis of the Washington Treaty, otherwise known as the North Atlantic Treaty.¹⁰ On December 10th, 1948 the official discussions began with the signatories of the Brussels Treaty, the US, and Canada; during the final sessions Denmark, Iceland, Italy, Norway, and Portugal were invited.¹¹ The aspect of collective defense was always at the center of this new alliance, but there were many issues that could not garner a consensus by the end of these meetings.¹² Over the course of drafting the Washington Treaty topics such as the implementation of collective defense, political and military cooperation, the

¹ "What is NATO?", North Atlantic Treaty Organization.

² Ibid.

³ Ibid.

⁴ Ibid.

⁵ "Founding Treaty," North Atlantic Treaty Organization, 2017.

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid.

¹¹ Ibid.

¹² Ibid.

geographical scope of the alliance, membership of the alliance, colonial territories, and the duration of the treaty were debated upon.¹³

Mandate, Governance, and Functions

When it came to collective defense European countries and the United States were at odds. The US did not want to be obligated to enter into a conflict when another member country was attacked and wanted to act as was necessary; simply put the US wanted the ability to send aid to attacked countries and not have to declare war.¹⁴ European countries wanted a commitment made by the US that they would come to their aid militarily if a signatory came under attack, yet the US was concerned that public opinion would not allow for this.¹⁵ The US version of collective defense won out, and it was decided that each member country had the ability to choose what type of action they deemed should be taken.¹⁶ This was article 5 of the Washington Treaty.¹⁷

Article 2 of the Washington treaty addresses the political and economic objectives of NATO aside from the military aspect. To ensure peaceful international relations and the further development of those, the signatories of the treaty are to strengthen their free institutions continually; economic collaboration is also encouraged amongst members to eliminate conflict which will in return create conditions for stability.¹⁸ Article 4 encourages member countries to come together and consult one another on these improvements to strengthen the links between governments and knowledge through information sharing to agree on common policies.¹⁹

Membership to NATO was an issue of debate as well. In the beginning, the UK did not want to let in the peripheral countries while the US did because they did not want them to fall under Soviet influence.²⁰ Ultimately, the treaty states that, by a unanimous vote, any European state invited to join and agreed to further the objectives of the organization could deposit their instrument of accession with the government of the United States who would then inform each of the other parties.²¹

Within NATO there is a hierarchy of governmental structures. Every member country appoints a permanent delegation to their political headquarters in Brussels; these delegations are led by an ambassador who represents their home country in decision-making processes as well as consultations.²² The North Atlantic Council (NAC) is the key political body where each member has a seat, and it is chaired by the Secretary-General.²³ With the same authority as the NAC is the Nuclear Planning Group, but their scope is strictly nuclear policy issues.²⁴ There are a

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ "The North Atlantic Treaty (1949)", NATO, April 1949.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Ibid.

²² "What is NATO? – Working structure", NATO.

²³ Ibid.

²⁴ Ibid.

plethora of subordinate committees to the NATO delegations that have more narrow scopes of technical and political for their agenda.²⁵ When political decisions are made, and they have military implications the Military Committee is addressed.²⁶ The Military Committee is made up of each member countries Chiefs of Defense, the International Military Staff, the military committee's executive body, and the military command structure.²⁷ Within the command structure, you have the Allied Command Operations (ACO), they are responsible for the planning and execution of NATO operations.²⁸ The Allied Command Transformation is also part of the command structure, and they increase readiness and capabilities of NATO's posture by evaluating future threats, trends, and implementation of lessons learned.²⁹

²⁵ Ibid.

²⁶ Ibid.

²⁷ Ibid.

²⁸ "Allied Command Operations (ACO)," NATO, June 2018.

²⁹ "Allied Command Transformation (ACT)," NATO, February 2018.

I. Further Development of Cyber Defense Capabilities

Introduction

The first policy on cyber defense was established in 2008 after an attack on Estonia's private and public institutions; it was agreed that cyber-attacks could be used as a weapon for conventional warfare.³⁰ Cyber Defense is now part of NATO's core tasks and as of 2016 cyberspace was deemed the fourth domain (the others being land, air, and sea) of NATO's collective defense.³¹ To protect the common values and way of life, NATO must have a presence in cyberspace just as it does in the physical world.

The principal authority on cyber defense related crisis management is the North Atlantic Council (NAC).³² The NAC oversees all aspects of the implementation of cyber defense; the Cyber Defense Committee is under the auspices of the NAC.³³ The Cyber Defense Committee has the lead role in cyber defense policy and provides oversight to member countries of the alliance.³⁴ To coordinate cyber defense across the civilian and military bodies, there is the Cyber Defense Management Board (CDMB), as well as the NATO Consultation, Control, and Command (NC3) for consultations on technical implementation.³⁵ NATO Military Authorities operate NATO's cyber defense capabilities, and with the help of the NATO Communications and Information Agency, they respond to cyber incidences affecting NATO and member countries.³⁶

In 2014 at the NATO Wales Summit members of the Alliance came together where a comprehensive policy and action plan were adopted.³⁷ The Wales Summit Declaration recognizes the large technological advances that have been made and are sure to come; with this in mind it is important that NATO policy reflects this, and that cyber capabilities are improved upon continually.³⁸ NATO is responsible for the defense of its networks, but in the spirit of unity, it is important that Allies are equally prepared in their cyber defense capabilities nationally.³⁹ This declaration also highlighted the important aspect of establishing bilateral and multinational relations to cooperate on advancing capabilities as they are vital to addressing cyber threats; this includes consulting industry leaders and integrating cyber defense into contingency planning and enhance information sharing.⁴⁰ The importance of the commitments made at the Wales Summit was reiterated at the Warsaw Summit in 2016, and sharing best practices in this area is a matter of priority.⁴¹ Not only did these two summits lay the groundwork for a strong defensive posture of NATO in cyberspace they also pushed for cooperation with the European Union (EU) as to enhance their cyber capabilities which are equally as important as national cyber capabilities.⁴² In 2016, the number of cyber attacks initiated on NATO networks

³⁰ Ibid.

³¹ "Cyber Defence" NATO, July 2018.

³² Ibid.

³³ Ibid.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Ibid.

³⁸ "Wales Summit Declaration," NATO, August 2018.

³⁹ Ibid.

⁴⁰ Ibid.

⁴¹ "Warsaw Summit Key Decisions," NATO, February 2017.

⁴² Ibid.

averaged about 500 per month which is an increase of 60% from the previous year.⁴³ Not only have these attacks become more frequent but they have expanded to softer targets such as personal devices and networks, and this rapid evolution of cyber-attacks illustrates the need for around the clock monitoring.⁴⁴ In Supreme Headquarters Allied Powers Europe (SHAPE) is the NATO Computer Incident Response Capability (NCIRC); this facility is where 200 experts conduct round-the-clock cyber defense support for NATO networks.⁴⁵

International and Regional Frameworks

To ensure an Allied-wide common approach of the development of cyber defense capabilities NATO outlines targets for implementation.⁴⁶ These targets are set in the *NATO Defence Planning Process* and were agreed upon by defense ministers.⁴⁷ The Alliance is always looking for ways to improve defense capabilities, but efficiently and cost-effectively; this encourages Allies to work together in generating modern defense capabilities including in cyberspace.⁴⁸ These initiatives are part of NATO's *Smart Defence*, and a major component of this is coordination with the EU specifically the European Defence Agency, and there are a few projects underway regarding cyber defense.⁴⁹

The Malware Information Sharing Platform (MISP) is one of these projects; it is an opensource platform where a trusted community can exchange information on the technical characteristics of malware without releasing details of an incident.⁵⁰ A benefit of MISP is that many of the same attacks are observed across different organizations, and all of these organizations spend time analyzing these, but with MISP if a member has shared information on this same malware it removes duplication of analysis.⁵¹ When new information is shared with MISP, all members of the community are notified which means faster threat detection.⁵²

The Multinational Cyber Defence Capability Development (MN CD2) project promotes cooperation between countries to acquire and develop capabilities.⁵³ MN CD2 allows countries to work within their monetary restraints by focusing on joint funding which allows for efforts in specific areas of their choice.⁵⁴ Participating countries coordinate all aspects of capability development including research, design and engineering, testing and experimentation, verification, procurement preparation, and procurement.⁵⁵ Currently, the participating countries are Canada, Denmark, the Netherlands, Norway, and Romania.⁵⁶

⁴³ "NATO Cyber Defence Factsheet," February 2018.

⁴⁴ Ibid.

⁴⁵ Ibid.

⁴⁶ "Cyber Defence," NATO, July 2018.

⁴⁷ Ibid.

⁴⁸ "Smart Defence," NATO, February 2017.

⁴⁹ "Cyber Defence," NATO, July 2018.

⁵⁰ "Malware Information Sharing Platform," NCI Agency,

⁵¹ Ibid.

⁵² Ibid.

⁵³ "MN CD2 – Cyber Defence Capability Development About", NCI Agency

⁵⁴ Ibid.

⁵⁵ Ibid.

⁵⁶ Ibid.

The final *Smart Defence* project is the Multinational Cyber Defence Education and Training (MN CD E&T).⁵⁷ This project is important to ensuring the constant maintenance and advancement of cyber defense capabilities at all levels, for NATO and Allied nations.⁵⁸ The MN CD E&T projects aim to address shortfalls in education and training by making new initiatives as well as establishing a platform to act as the central point of coordination for a plethora of education and training activities.⁵⁹ At the latest workshop, the Participating Nations were asked to propose national solutions for education and training, and six new initiatives were identified, cyber defense awareness course, cyber defense international master, cyber defense and cybersecurity law master, cyber intelligence course, cyber defense staff officers' course, and the cyber defense capability development course.⁶⁰

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is an integral part of cybersecurity as they host annual cybersecurity conferences, cybersecurity exercises, cyber defense workshops, and offer courses in many facets of cybersecurity.⁶¹ The concept of cyber defense centre was proposed by Estonia in 2004, shortly after their accession into NATO, and two years later it was approved and in 2007 negotiations were held with potential sponsoring nations.⁶² The most recent cybersecurity conference held by the CCDCOE was CyCon X; this is the 10th anniversary Conference on Cyber Conflict.⁶³ CyCon is attended by opinion-leaders, decision-makers, law and technology experts within governments, academia and industry, and military from almost 50 countries.⁶⁴ Those who attend come to discuss current cybersecurity challenges and this year members of the cybersecurity community were asked to shape the focus of CyCon X with what they believed to be the most topical issues; thus CyCon X emphasized maximizing effects in cyberspace.⁶⁵

The CCDCOE also organizes Locked Shields, “the world’s largest and most advanced international technical live-fire cyber defence exercise,” these exercises are held annually with the focus of training national security experts in the IT field who protect national networks.⁶⁶ Locked Shields is a collaborative effort between Estonian Defence Forces, Finnish Defence Forces, Swedish Defence University, British Joint Army, United States European Command, Air Operations COE, and Tallinn University of Technology.⁶⁷ During this exercise, teams are given the task of maintaining the networks and services of a fictional country while being bombarded by realistic and cutting-edge cyber-attack methods.⁶⁸ The 2017 Locked Shields exercise will be tremendously more advanced; teams will be given the task of maintaining the networks and systems of a fictional military base where they will encounter specialized system attacks.⁶⁹ These specialized attacks will be on a power grid system, military command and control systems,

⁵⁷ "Cyber Defence," NATO, July 2018.

⁵⁸ "MN CD E&T," Ministry of Defense Portugal.

⁵⁹ Ibid.

⁶⁰ Ibid.

⁶¹ "Events," CCDCOE, 2018.

⁶² "History," CCDCOE, 2018.

⁶³ "Events," CCDCOE, 2018.

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ Ibid.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Ibid.

unmanned aerial vehicles, and other operational infrastructure.⁷⁰ 25 nations and about 800 participants were in attendance for the 2017 exercise, and more teams used the secure online access to the exercise networks from their home bases.⁷¹

Case Study: Estonia

In 2007, a decision was made to relocate a Soviet-era statue in Estonia.⁷² Shortly after this decision, Estonia became a victim of a politically motivated cyber attack campaign in the form of distributed denial of service attacks.⁷³ These types of attacks bombard servers to the point of failure and results in loss of service.⁷⁴ In the case of Estonia, the attacks began on non-essential services like government websites and e-mails, but some were more targeted, there were a few more detrimental attacks that targeted online banking systems, and Domain Name Servers (DNS).⁷⁵ Months after the attack no organization or group have come out to claim responsibility for the attacks.⁷⁶ Although, after the announcement of the relocation of the statue Russia stated that, “removing the statue would be disastrous for Estonians.”⁷⁷ This is one of the first cases of a politically motivated cyber-attack.⁷⁸ The decision to move the WWII Bronze soldier was met with distention from those who wanted to keep it there, while others believed it marked the occupation of the Soviets in Estonia.⁷⁹ ON April 26th, 2007, Estonia exploded into two nights of riots where 1000 people were detained; this is when the cyber-attack began.⁸⁰

⁷⁰ Ibid.

⁷¹ Ibid.

⁷² “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective”, Otis, R. CCDCOE, 2008.

⁷³ Ibid.

⁷⁴ Ibid.

⁷⁵ Ibid.

⁷⁶ Ibid.

⁷⁷ “10 Years after the Landmark Attack on Estonia, is the World Better Prepared for Cyber Threats”, Tamkin, E. Foreign Policy, 2017.

⁷⁸ Ibid.

⁷⁹ “How a Cyber Attack Transformed Estonia,” McGuinness, D. April 2017.

⁸⁰ Ibid.

II. NATO-Russian Relations

Introduction

The origin of NATO is well known, but in 1991, at the end of the Cold War, Russia joined the North Atlantic Cooperation Council; In 1994 Russia was the first country to join NATO's Partnership for Peace Program (PfP) this was a place for practical and bilateral cooperation between NATO and partner countries.⁸¹ The mission of the PfP "expanding and intensifying political and military cooperation in Europe, increasing stability, diminishing threats to peace, and building strengthened security relationship."⁸² In 1997, a formal basis for relations was created by the NATO-Russia Founding Act.⁸³ This act showed the determination of NATO and Russia in establishing a long-lasting and inclusive peace in the Euro-Atlantic area.⁸⁴ The Founding Act was created on the principles of democracy and cooperative security; the idea was to establish goals on peacekeeping, counter-terrorism, arms control, counter-narcotics, and theatre missile defense.⁸⁵ The Founding Act also stated that both NATO and Russia must refrain from the threat or use of force against one another and other states; they were to base their cooperation on the principles of civil liberties and human rights.⁸⁶ It was also important to establish a forum where both parties could come together for consultations on security issues and direct cooperation, so in 2002 the NATO-Russia Council (NRC) was created.⁸⁷ This forum for dialogue is incredibly important as to increase predictability and decrease misunderstanding.⁸⁸ This privileged partnership was only offered to Russia.⁸⁹ This cooperation in the NRC led to more collaboration in counter-terrorism and counter-narcotics training for an officer in Asia.⁹⁰

Conflicts: Georgia, Ukraine, and Syria

Georgia

In 2008 Russia was strengthening ties with South Ossetia, who previously claimed their independence from Georgia in the early 1990s, and this angered Georgia.⁹¹ Russia was also concerned with Georgia's soon to be admission into NATO and European Union.⁹² Within the coming months both sides were accusing the other of a military build-up; later, that year Georgian troops and separatist fighters clashed.⁹³ This clash between Georgia and South Ossetia was extremely heightened after Georgia began their concerted ground and air campaign on South Ossetia.⁹⁴ Russia began sending troops into South Ossetia under the guise of bringing aid to the citizens, but a few days later Russia managed to establish control and push Georgians out of the

⁸¹ "Relations with Russia," NATO, September 2018.

⁸² Ibid.

⁸³ Ibid.

⁸⁴ Ibid.

⁸⁵ Ibid.

⁸⁶ Ibid.

⁸⁷ Ibid.

⁸⁸ "NATO-Russia Council," NATO, 2018.

⁸⁹ Ibid.

⁹⁰ Ibid.

⁹¹ "Europe's Forgotten War: The Georgia Russia Conflict explained a decade on," Harris, C. Euronews, 2018.

⁹² Ibid.

⁹³ Ibid.

⁹⁴ Ibid.

territory and even attacked surrounding suburbs.⁹⁵ On August 12th, 2008, a ceasefire was negotiated, and Russia recognized South Ossetia's and another region's, Abkhazia, independence (only a few countries would do this); Russian troops were eventually pulled out of Georgia but continued to occupy separatist regions.⁹⁶ By the end of this conflict, it was discovered, by an official EU fact-finding mission, that 800 lives were lost in this five days war.⁹⁷ The military actions carried out by Russia led to the suspension of cooperation in certain areas and the cancellation of formal meetings of the NATO-Russia Council.⁹⁸ Allies are still calling on Russia to reverse their acknowledgement of the Georgian regions of South Ossetia and Abkhazia as independent states.⁹⁹ In April of 2009, the Alliance leaders acknowledge the many disagreements with Russia about Georgia, but went ahead and restarted practical and political cooperation.¹⁰⁰

Ukraine

In November of 2013, President Viktor Yanukovich or Ukraine denied a deal for Ukraine to integrate into the European Union; this integration was supported by popular opinion within Ukraine.¹⁰¹ This move made by Yanukovich sparked massive protest which he put down violently, and with the support of Russia whereas the protestors were supported by the US and the European Union.¹⁰² These anti-government protestors eventually toppled the Yanukovich regime, and he fled the country.¹⁰³ A month later, most likely due to the loss of influence in Ukraine, Russia invaded and annexed Crimea; and not too long after pro-Russia separatist rebels were cropping up in eastern Ukraine and began seizing territory.¹⁰⁴ In July, separatist rebels shot down a Malaysian Airline plane which killed 298 people; most people believe this to be an accident.¹⁰⁵ After these events, fighting between Ukrainian forces and rebels was getting more brutal, but the rebels were losing ground; this urged Russia to invade eastern Ukraine to support the rebels in an overt fashion.¹⁰⁶ The figures so far are more than 10,000 civilian casualties and 1.6 million internally displaced people in Ukraine.¹⁰⁷

In response to the annexation of Crimea in 2014 NATO foreign ministers made the decision to suspend all practical cooperation with Russia, but this did nothing to deter Russia from continually acting aggressively in Ukraine including destabilizing eastern Ukraine.¹⁰⁸ This continued aggression has posed a security threat and has encouraged NATO to enhance their defense and deterrence posture, but the political dialogue will remain open.¹⁰⁹ At the Warsaw Summit in 2016, it was made clear that NATO and Russian relations could not be improved until

⁹⁵ Ibid.

⁹⁶ Ibid.

⁹⁷ Ibid.

⁹⁸ Ibid.

⁹⁹ Ibid.

¹⁰⁰ "Relations with Russia," NATO, September 2018.

¹⁰¹ "Everything you Need to Know about the Ukraine Crisis," Fisher, M. Vox, 2014.

¹⁰² Ibid.

¹⁰³ Ibid.

¹⁰⁴ Ibid.

¹⁰⁵ Ibid.

¹⁰⁶ Ibid.

¹⁰⁷ "Global Conflict Tracker: Conflict in Ukraine," Council on Foreign Relations, 2018.

¹⁰⁸ "Relations with Russia," NATO, September 2018.

¹⁰⁹ Ibid.

“a clear and constructive change in Russia’s actions – one that demonstrates compliance with international law and Russia’s international commitments.”¹¹⁰ During this conflict, the NATO-Russia Council was never suspended, and lines for communication remained open; the meetings contribute to transparency within relations, and issues such as force posture and military exercises are making progress.¹¹¹ Military-to-military lines of communication remain open and promote transparency and predictability in military activities.¹¹²

Syria

In Syria Russia began their involvement in 2015 when they carried out their first airstrikes in Syria; they said they are targeting ISIL and ensuring the Assad regime does not get removed by outside forces.¹¹³ Much of the west and Syrian opposition believe that the Russians are overwhelmingly targeting anti-Assad rebels.¹¹⁴ After years of Russia offering air support in getting back Aleppo, Homs, and Palmyra from rebel forces these three (Russia, Iran, Turkey) involved parties agreed to a ceasefire between the government and non-Islamist rebels.¹¹⁵ In October of 2015, when Russia began their military intervention, Allies called on Russia to ceasefire immediately on Syrian opposition and civilians, and to concentrate on fighting ISIL.¹¹⁶ Allies also emphasized the importance of working towards a solution through a political transition.¹¹⁷

Salisbury attack

On March 14th, 2018, in Salisbury (United Kingdom) a former Russian spy and his daughter were poisoned with a nerve agent.¹¹⁸ The men responsible for this attack were linked to the Russian military intelligence service or GRU, but Russia denies any connection to these attacks.¹¹⁹ This was seen as a breach of international norms; intensive consultations were held amongst the Allies, and they concluded that 150 Russian diplomats were to be expelled from 25 nations.¹²⁰ The maximum size of the Russian mission to NATO was dropped to 20, the withdrawal of accreditation for seven staffers to the Russian mission, and the denial of three pending accreditations were all repercussions of Russia’s reckless behavior.¹²¹ Although relations are strained between NATO and Russia the actions taken have been proportionate, and NATO has still committed to the two-track approach; an open dialogue and strong defense.¹²²

¹¹⁰ Ibid.

¹¹¹ Ibid.

¹¹² Ibid.

¹¹³ "Syria Profile – Timeline," BBC, 2018.

¹¹⁴ Ibid.

¹¹⁵ Ibid.

¹¹⁶ "Relations with Russia," NATO, 2018.

¹¹⁷ Ibid.

¹¹⁸ "Nerve Agent Poisoning," Adam, K. Washington Post, 2018.

¹¹⁹ Ibid.

¹²⁰ "Relations with Russia," NATO, 2018.

¹²¹ Ibid.

¹²² Ibid.

Citations

- “Nerve Agent Poisoning,” Adam, K. Washington Post, 2018. Retrieved from. https://www.washingtonpost.com/world/europe/britain-charges-two-russians-with-attempted-murder-of-ex-spy-with-nerve-agent/2018/09/05/db99c5c8-b0f7-11e8-a20b-5f4f84429666_story.html?noredirect=on&utm_term=.6ddd1fc92a82
- “Syria Profile – Timeline,” BBC, 2018. Retrieved from. <https://www.bbc.com/news/world-middle-east-14703995>
- “Everything you Need to Know About the Ukraine Crisis,” Fisher, M. Vox, 2014. Retrieved from. <https://www.vox.com/cards/ukraine-everything-you-need-to-know/what-is-the-ukraine-crisis>
- “Global Conflict Tracker: Conflict in Ukraine,” Council on Foreign Relations, 2018. Retrieved from. <https://www.cfr.org/interactives/global-conflict-tracker#!/global-conflict-tracker>
- "Europe's Forgotten War: The Georgia – Russia Conflict Explained a Decade on," Harris, C. Euronews, 2018. Retrieve from. <https://www.euronews.com/2018/08/07/europe-s-forgotten-war-the-georgia-russia-conflict-explained-a-decade-on>
- “Relations with Georgia,” NATO, 2018. Retrieved from. https://www.nato.int/cps/ie/natohq/topics_38988.htm
- “NATO – Russia Relations: The Background,” NATO, 2018. Retrieve from. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_04/20180426_1805-NATO-Russia_en.pdf
- “Relations with Russia,” NATO, 2018. Retrieve from. https://www.nato.int/cps/en/natolive/topics_50090.htm#
- “Cyber Defense,” NATO, 2018. Retrieved from. https://www.nato.int/cps/en/natohq/topics_78170.htm
- “NATO Cyber Defence Factsheet,” NATO, 2018. Retrieved from. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf
- “Before the Gunfire, Cyberattacks,” Markoff, J. 2008. Retrieved from. <https://www.nytimes.com/2008/08/13/technology/13cyber.html>
- “10 Years after the landmark attack on Estonia, Is the World Better Prepared for Cyber Threats,” Tamkin, E. 2017. Retrieved from. <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>
- “Wales Summit Declaration,” NATO, 2018. Retrieved from. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm
- “Warsaw Summit Key Decisions factsheet,” NATO, 2017. Retrieved from. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

- “Smart Defence,” NATO, 2017. Retrieved from.
https://www.nato.int/cps/en/natohq/topics_84268.htm
- “MN CD2 – Cyber defence Capability Development,” NATO. Retrieved from.
<https://mncd2.ncia.nato.int/pages/about.aspx>
- “Malware Information Sharing Platform,” NCI Agency. Retrieved from.
[https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20\(MISP\).pdf](https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf)
- “MN CD E&T,” Republic of Portugal. Retrieved from. <http://mncdet.wixsite.com/mncdet-nato/et-iniciatives>
- “Events: Locked Shields,” CCDCOE, 2017. Retrieved from. <https://ccdcoe.org/locked-shields-2017.html>
- “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective,” CCDCOE, 2008. Retrieved from. <https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html>
- “How a Cyberattack Transformed Estonia,” McGuinness, D. BBC, 2017. Retrieved from.
<https://www.bbc.com/news/39655415>
- “What is NATO?” NATO, 2018. Retrieved from. <https://www.nato.int/nato-welcome/index.html>
- “Founding treaty,” NATO, 2017. Retrieved from.
https://www.nato.int/cps/en/natolive/topics_67656.htm
- “The North Atlantic Treaty,” NATO, 1949. Retrieved from.
https://www.nato.int/cps/en/natohq/official_texts_17120.htm