HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

TASK FORCE

The Donald C. Hellmann Task Force Program

NATO: Building resiliency and integrity against Russian hybrid warfare threats

2019

HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

Faculty Advisor

Fredrick Lorenz, J.D, L.L.M.

Evaluator

Assistant Secretary General for Operations at NATO, Dr. John Manza

---

Coordinator and Editor

Nivedita Arvind

Sarah Nichols

Task Force Authors

Nivedita Arvind*

Sara Bak

Alex Buzzell**

Noah Durette**

Naomi Eguchi Faletti*

Sarah Nichols*

Sofija Raisys* **

Omar Tabuni

Jennifer Yan

** denotes a member of the design team*

*** denotes a section leader*

The Henry M. Jackson School of International Studies

jsis.washington.edu | Phone: (206) 543-6001 | Email: jsis@uw.edu

Acknowledgements

This Task Force would like to express our sincerest gratitude to our Task Force Coordinator, Professor Frederick Lorenz, for his guidance, wisdom, and devotion. Our success in completing this report is a direct consequence of his continued support. We would also like to thank Ambassador John Koenig for his contributions in making the Task Force Rome study abroad program an enlightening and fulfilling experience. We would like to thank Lone Kjelgaard for her stories, expertise, and mentorship. Finally, we would like to extend our utmost gratitude to Joan Lorenz, whose warm hospitality and kindness kept our spirits high.

We would also like to thank:

Lieutenant Colonel Ian Fletcher

Dr. Sergey Golubok

Colonel Ian Hope

Lieutenant Colonel Daniel Miller

Dr. Vira Ratsiborynska

U.S. Ambassador Kyle Scott

UW Rome Center

Table of Contents

Glossary of Acronyms

- **APT:** Advanced Persistent Threat
- **ASG:** Assistant Secretary General
- **ASG-I:** Assistant Secretary General for Intelligence
- **BI:** Building Integrity
- **BiH:** Bosnia and Herzegovina
- **CCD COE:** Cooperative Cyber Defense Center of Excellence
- **CDMA:** Cyber Defense Management Authority
- **CI:** Critical Infrastructure
- **CoE:** Center of Excellence
- **DHS:** Department of Homeland Security
- **DNC:** Democratic National Convention
- **DDoS:** Distributed Denial of Service
- **DoS:** Denial of Service
- **ESDP:** European Security and Defense Policy
- **EU:** European Union
- **EULEX:** European Union Rule of Law Mission in Kosovo
- **EUSR:** European Union Special Representative
- **FSB:** Russia's Federal Security Service
- **GRU**: Russian Military's Main Intelligence Directorate
- **KFOR:** Kosovo Force
- **KGB:** Russia's Committee for State Security
- **KLA:** Kosovo Liberation Army
- **MAP:** Membership Action Plan
- **MOD:** Russia's Ministry of Defense
- **NATO:** North Atlantic Treaty Organization
- **NCIRC:** NATO Computer Incident Response Capability
- **NGO:** Non-governmental organization
- **NHQSa:** NATO Headquarters Sarajevo
- **IFOR**: Implementation Force
- **PESCO:** Permanent Structured Cooperation

- **RAP:** Readiness Action Plan
- **RISS:** Russian Intelligence and Security Services
- **RS:** Republika Srpska
- **SCADA:** Supervisory Control and Data Aquisition
- **SFOR:** Stabilization Force
- **STRATCOM:** Strategic Communications
- **SVR**: Russia's Foreign Intelligence Service
- **UN:** United Nations
- **UNMIK:** United Nations Mission in Kosovo
- **UNPROFOR:** United Nations Protection Force
- **UNSCR:** United Nations Security Council Resolution
- **WWII:** World War II

This page intentionally left blank

Executive Summary

Hybrid threats are not a new concept. However, the resurgence of an aggressive Russia has led to an increase in dangerous activity and the practice of new techniques. Hybrid threats put NATO in a complicated position as most hybrid attacks fall under the Article 5 threshold. While malevolent actors such as Russia may not risk attacking a member state through conventional means, these subversive tactics can create chaos without initiating an armed retaliation.

Employers of hybrid warfare utilize "conventional capabilities, irregular tactics and formations, and terrorist acts including indiscriminate violence, coercion, and criminal activity."[1] Hybrid threats can take many forms, including energy security, state sponsored terrorism, and cyber warfare. This report will not explore all the possibilities of hybrid threats. Instead, we will be focusing on Russia's cyber capabilities, their use of religion and ethnicity to incite violence, and disinformation campaigns.

To begin, this paper will examine the difficulties of attributing cyber-attacks, compare NATO's current cyber defense capabilities with Russia's, and draw lessons from the cyber-attacks on Ukraine's critical infrastructure. This section will conclude by recommending increased information sharing among NATO members concerning cyber threats and increasing budget and training allocations for research and training of cyber defense.

The second section will look at the utilization of religion and ethnicity to instigate violence, separatism, and disorder in countries on the periphery of NATO. By using hybrid tactics such as disinformation and paramilitary training, Russia expects to keep NATO far away from its "near abroad." However, such strategies not only affect the target country, but the stability of the Alliance as a whole. Case studies of Kosovo, Ukraine, and Bosnia will be used to identify Russian threats in the region and how NATO can counter those threats. Recommendations will culminate by suggesting the consolidation of KFOR and NATO Headquarters Sarajevo to expand resources and reach in the Western Balkans, as well as consider the implementation of a Membership Action Plan for Ukraine.

[1] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid War*, (Arlington: Potomac Institute for Policy Studies, 2007), 20-22.

Due to the unconventional methods of hybrid warfare it is important for NATO to cooperate with other international institutions. This will be explored in our final chapter in which we will discuss avenues of NATO/EU cooperation. It is our goal for this paper to provide a framework for NATO to counter these threats and strengthen its institutions to proactively prepare itself for future attacks. This section will look at resilience and NATO/EU cooperation in the Baltics, NATO/EU cooperation concerning strategic communications, and reviewing how NATO and the EU can build resiliency in the Republic of North Macedonia. Recommendations for the chapter will include enhancing NATO/EU support for emerging alliance members and strengthening cooperation in deterrence and resilience building in shared member states.

Detailed policy recommendations are included at the conclusion of each section.

1. Improving NATO's Cyber Security

Introduction

One of the greatest threats NATO faces today lies in the cyber domain. Attacks on several member states have already occurred, many of which were attributed to Russia. Cyber threats have increased exponentially over the past few decades and NATO cannot be slow to respond. The complexities of cyber warfare now help the attacker evade the consequences of a traditional warfare attack. In order to improve its defense, NATO must build resilience and integrity within its cyber security sector.

To begin, chapter one will look at current attribution methods and the difficulty uncertain attribution poses to response to cyber-attacks. In particular, this chapter will analyze the attacks on the U.S. Democratic National Convention and lessons drawn from attributing the attack to Russia. NATO's mandate is limited to cyber defense capabilities, but member states can assist in an offensive cyber response if it is warranted. NATO should have a plan in place based on the severity of an attack and the degree of certainty of attribution so they can remain resilient and respond promptly to attacks on member states.

Chapter two will have two parts. First, it will give an overview on Russia's understanding of cyber, employment of cyber tools in real-world scenario, and their perceived cyber capabilities. The second part will consider current legal framework and show how NATO can improve collective cyber defense based on its presumed strengths and limitations. The volume and severity of malicious cyber activity posed by Russia against NATO and its member states has increased exponentially, undermining the national interests of Russia's political adversaries. To counter this strategy, NATO policymakers must increase their awareness of how Russia integrates cyberwarfare tools into its broader operations in achieving military and political objectives.

Chapter three will look at the cyber-attacks on Ukraine and the theory that Russia is using Ukrainian critical infrastructure to test their cyber capabilities. These weapons tested in Ukraine could be used in a direct attack on NATO member states. The Alliance should expand its research and development on cyber defense in Ukraine in order to contain and combat Russia's cyber capabilities from affecting NATO member states.

1.1 Attribution and Active Defense: Resilience in Response to Malicious Cyber Activity

Noah Durette

1.1.1 Introduction

It is essential to correctly identify the perpetrator when a cyber-attack is detected but attribution is often an inexact process. Analysts can be fairly certain they have correctly identified the bad actor, but there is no 100 percent guarantee. This makes determining the appropriate response to an attack a balancing act as attacks cannot go unchecked, but any retaliation can escalate the situation if the perpetrator is incorrectly identified. The first part of this chapter will look at current attribution methods for NATO and its members and how they can be improved. The second part of the chapter will focus on responses to cyber-attacks that have been attributed to the Russian government and the risk of escalation.

1.1.2 Attribution

The very first step that occurs after a cyber-attack is detected is to determine the nature and origin of the attack. When an attack is detected, groups of experts, either public cyber defense companies or the government, look for patterns, analyze the cyber forensics, and compile the results into what is called a "constellation of evidence.[2]" This constellation of evidence is used to attribute the attack to a certain actor or group, with varying degrees of certainty depending on the reliability and type of evidence gathered. Coding used by hackers' programs can often provide sufficient evidence for attribution as cultural references, including languages, phrases, and names are often used, mostly unintentionally. Kristofer Swanson, Vice President of the Forensic Services practice at Charles River Associates, refers to attribution as "a digital 'Sherlock Holmes' investigation.[3]" If evidence is gathered efficiently, an attack can be attributed with an extremely high level of certainty.

[2] Bruce Schneier. "Why Proving Source of a Cyberattack Is so Damn Difficult." CNN. January 06, 2017. https://edition.cnn.com/2017/01/05/opinions/proving-source-of-dnc-hacks-difficult-opinion-schneier/index.html.
[3] Christopher P Skroupa. "No Bit Sherlock—The Role of Forensics In Tracing The DNC Hack." Forbes. https://www.crai.com/sites/default/files/publications/FORBES_The-role-of-forensics-in-tracing-the-DNC-Hack.pdf

Over the past few years, several national governments, including those of the United States and Ukraine, have attributed a series of cyber-attacks to the Russian government. These claims have been supported by private cyber-defense corporations, who have provided additional research and evidence pointing to the Russian government as the perpetrators. *The Washington Post* reported that since much of the evidence used in attributing the attacks has not been made public, President Trump and other critics have questioned the legitimacy of these findings.[4] Without definitive proof presented to the public, it is natural that the issue would become political. What many don't understand is that much of the evidence used in attribution cannot be made public because it would reveal sensitive information on intelligence capabilities and current operations.[5] Even when intelligence agencies make an attribution with a high level of confidence, they generally cannot provide the necessary proof to satisfy the public.

The hacking of the United States Democratic National Convention (DNC) in 2016 has presented one of the most controversial cases of attribution in recent history. Not only has the identity of the perpetrator been questioned, but also the severity of the attacks. Over several months, the DNC staff ignored numerous warning signs that they had been hacked, until April 2016 when they finally admitted their systems had been breached.[6] This negligence on the part of the DNC staff allowed for information to be stolen over an extended period of time. While this attack was able to be accurately attributed, as more time passes after an initial attack, attribution can become much more difficult. After determining that there was a problem, the DNC called in CrowdStrike, an American cyber security technology company based in California, to investigate the attacks.[7] Using a program called Falcon, CrowdStrike observed every action that had been taken on the hundreds of devices at the DNC, and immediately

[4] Philip Bump. "Here's the Public Evidence That Supports the Idea That Russia Interfered in the 2016 Election." The Washington Post. July 06, 2017. Accessed February 02, 2019. https://www.washingtonpost.com/news/politics/wp/2017/07/06/heres-the-public-evidence-that-supports-the-idea-that-russia-interfered-in-the-2016-election/?utm_term=.3da6736cdc92.

[5] Lily Hay Newman. "Hacker Lexicon: what is the attribution problem?" Wired. June 03, 2017. Accessed February 02, 2019. https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

[6] Chris Stokel-Walker. "Hunting the DNC Hackers: How Crowdstrike Found Proof Russia Hacked the Democrats." WIRED. September 28, 2017. Accessed February 02, 2019. https://www.wired.co.uk/article/dnc-hack-proof-russia-democrats.

[7] Dmitri Alperovitch. "Bears in the Midst: Intrusion into the Democratic National Committee." CrowdStrike. October 08, 2018. Accessed mFebruary 03, 2019 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

found evidence of several breaches.[8] CrowdStrike then reviewed their records to look for any correlations in hacking methods of the DNC hacks with previously identified attacks. After finding that data was exfiltrated to an IP address associated with a known group, misspelled URLs, and attacks coordinating to time zones consistent with working hours in Moscow, CrowdStrike realized that two advanced persistent threats (APT)[9] previously attributed to the Russian government were responsible.[10] Despite the fact that both APT groups found to be involved in the DNC hack were working on behalf of the Russian government, CrowdStrike found no evidence of collaboration between the two groups.[11] Instead, both groups ended up stealing much of the same data from the same systems.

In fact, Russia's intelligence agencies are often pitted against each other in competition, as their primary goal is to be seen as useful to the Kremlin. These agencies are divided by "bureaucratic turf wars," and often hinder rather than support each other's efforts.[12] Mark Galeotti, a Russia cyber expert, argues that Europe's understanding of this aspect of Russian intelligence services is outdated and lacking. Actions taken by these agencies can be countered by confronting Russia's governance weaknesses. To find these weaknesses, it is important to understand two of Russia's advanced persistent threat groups, APT28 and APT29.

APT28, also known as Fancy Bear, was the first of the actors discovered by CrowdStrike's investigations. Fancy Bear is a team of highly skilled experts working to collect intelligence on defense and geopolitical issues, and has previously targeted the Caucasus, Eastern European governments, and NATO member states.[13] Fancy Bear's goal appears to be to spread chaos among any groups hostile to the Russian government, and it has proven itself to be very successful. According to FireEye,[14] the

[8] Stokel-Walker, 2017
[9] An advanced persistent threat (APT) is a prolonged cyber-attack in which a group gains access to a network and remains undetected over an extended period of time.
[10] Stokel Walker, 2017
[11] CrowdStrike Editorial Team. "Who Is Cozy Bear (APT29)?" CrowdStrike. June 07, 2018.Accessed February 10, 2019. https://www.crowdstrike.com/blog/who-is-cozy-bear/
[12] Mark Galeotti. "Putin's Hydra: Inside Russia's Intelligence Services." European Council on Foreign Relations. May 11, 2016. Accessed February 10, 2019. https://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.
[13] "Advanced Persistent Threat Groups." FireEye. Accessed February 01, 2019. https://www.fireeye.com/current-threats/apt-groups.html
[14] Fireeye is a public cyber security company headquartered in California that pays special attention to APT groups attributed to an established nation state

type of intelligence gathered by APT28 would only be useful to a government and the presence of malware written in Russian was discovered. This led them to the conclusion that APT28 at the very least receives support from the Russian government. Various groups, including the National Cyber Security Center, have provided an advisory including technical frameworks for detecting malware used in APT28.[15] Public reports such as these are helpful in undermining the effectiveness of advanced persistent threats. According to Dan Arenson, a senior cyber analyst, APT28's method is to steal sensitive data that could "embarrass the targeted organization and thereby undermine its effectiveness." Despite its high level of efficiency, APT28's methods are not all that advanced. APT28 often relies on phishing[16] and domain doppelganging[17] to gain access to secure networks.[18] As effective as phishing attacks can be, they are preventable if the right precautions are taken. Due to the scope and frequency that APT28 has been encountered, it is essential for NATO member states to be able to detect and remove APT28 before it has time to cause damage.

The other advanced persistent threat discovered in the DNC case was APT29, nicknamed Cozy Bear. Cozy Bear has also been known to target a variety of other governments, organizations, and sectors including defense, energy, financial, legal, manufacturing sectors, Western European governments, think tanks, pharmaceutical, universities, and more.[19] According to FireEye, APT29 is one of the most technologically advanced and skilled threat groups, as it is flexible in a way that allows it to evolve and fix itself while constantly updating its malware to avoiding detection.[20] Cozy Bear also uses phishing to gain access to systems, but it "casts a wide net" by sending thousands of emails to a variety of targets. The emails appeared to be sent from officials at the U.S. Department of State, used a legitimate Department of State form as a decoy, and included links that appeared to be official Department of State forms but contained the

[15] "Indicators of Compromise for Malware Used by APT28." National Cyber Security Center. October 04, 2018. Accessed February 08, 2019. https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28.
[16] A Phishing attack is a fraudulent email sent with the intention of tricking someone into revealing private information or clicking on a harmful link
[17] Domain doppelganging is when an email address or link from the sender of a phishing attack is made to look like it came from a legitimate source
[18] Kate O'Flaherty. "Midterm Election Hacking -- Who Is Fancy Bear?" Forbes. August 23, 2018. Accessed February 08, 2019. https://www.forbes.com/sites/kateoflahertyuk/2018/08/23/midterm-election-hacking-who-is-fancy-bear/#18da2cdd2325.
[19] CrowdStrike, 2018
[20] "Advanced Persistent Threat Groups"

payload.[21] The payload contained a variety of tools that prevented it from being analyzed by a virtual machine or automatic debugger and is able to detect and avoid security software that may be installed on the targeted device. A recently discovered intrusion by APT29 used a payload called Cobalt Strike, which is commercially available and has disguised itself to look like Pandora music.[22] This means that APT29 usually requires manual detection by a human, and automatic defense software cannot be relied upon.

Looking at advanced persistent threats attributed to Russia shows the risk that negligence can play in creating cyber vulnerabilities. To reduce the effectiveness of phishing and other social engineering[23] tactics, increased education and training programs for all NATO officials is essential. NATO should also encourage the governments of its member states to follow the same procedures. Proper training should include non-technical classes on how to recognize a phishing attack, and incentives should be provided for government officials to be diligent in checking every email they receive to be sure it is from a legitimate source. Files should not be opened that are from a questionable source, and protocols should be in place for any potentially sensitive information to be shared via email. Other than phishing emails, another common tactic to breach systems is tricking government officials into using USB drives that are infected with a virus. All USB drives used with government devices or containing sensitive data should be tested to meet regulations before use. Any other potential tactic that could be used to breach systems should be made known to everyone with access to these systems. As many people have a tendency to let their guard down and become careless over extended periods of time with no incidents or reminders, regular workplace briefings should be mandatory. These meetings can be brief but would help individuals stay updated with new potential cyber tactics and keep them diligent and prepared.

[21] A Payload is the component that executes a malicious activity or contains the harmful virus
Seals, Tara Seals. "APT29 Re-Emerges After 2 Years with Widespread Espionage Campaign." The First Stop for Security News. November 20, 2018. Accessed February 10, 2019. https://threatpost.com/apt29-re-emerges-after-2-years-with-widespread-espionage-campaign/139246/.
[22] CrowdStrike, 2018
[23] Social engineering is a tactical strategy relying on human interaction to trick people into breaking security standards or revealing confidential information.

It is vital for all NATO members to be updated and on the same page about any and all cyber threats, increased information sharing between governments, intelligence agencies, and cyber security companies. While cyber forensics often contains classified information that cannot be revealed to the public, sharing intelligence among the government agencies of NATO member states should still be possible. While non-government cyber security firms can provide vital input on matters of attribution, information sharing should remain one way. Those cyber companies can provide their intelligence to government agencies, for a price if they insist, but government agencies need not feel compelled to reveal potentially sensitive information. Secret sharing is a vital aspect of trust among nations, so any nation that revealed intelligence shared in confidentiality would face disapproval from their allies. Increased information sharing also includes the need for an improved rapport between policy and technical aspects of cyber. Without communication, policy and technical aspects of cyber are often out of sync. Policy can either be too far ahead for the technology to keep up, or new capabilities may not be adequately utilized. Increasing communications has the potential to greatly improve the cyber capabilities of NATO and its members.

1.1.3 Response To Malicious Cyber Activity

After determining the attribution of malicious cyber activity, the next step is to determine the appropriate response. A scale based on the severity of attack and degree of certainty of attribution should be created to determine the appropriate response. When Russia is believed to be responsible for malicious cyber activity, but the certainty of attribution is relatively low, a response should be limited to admonishing statements and a warning to stop the cyber activity. Meanwhile, cyber analysts should adapt to any new methods and raise the level of certainty of attribution. When there is a very high degree of certainty of attribution, responses can vary based on the severity of an attack. For example, relatively innocuous cyber activity such as malign influence campaigns, while certainly unacceptable, do not warrant offensive retaliation. Responses can include sanctioning, which has already been a tool widely used by the West to discourage Russia’s actions.

Severe cyber-attacks, including attacks on any aspect of critical infrastructure, pose a much more serious challenge. NATO has already recognized cyber as an operational domain in which Article 5 can be invoked, and the definition of an “armed attack” remains deliberately vague, especially in the case of cyber.[24] Any attack on critical infrastructure of a NATO member state could be seen as an act of war and Article 5 of the North Atlantic Treaty can be invoked. If an attack warrants an offensive counter-attack, a variety of options are available to NATO. One option is to respond by initiating a cyber-attack on Russia, though because NATO only maintains cyber defensive measures, that would be in the hands of the member states. If Article 5 is invoked, member states could be asked to use their own cyber technology to stage an attack on behalf of NATO. Initiating cyber-attacks on Russia has a high risk of escalation and should be limited to hacking back.[25] Cyber-attacks on any of Russia’s assets other than their systems used to attack a NATO member state would escalate further, so a scenario in which NATO approves an attack on Russian critical infrastructure is highly unlikely. If cyber warfare reaches the level of both sides taking out critical infrastructure, there would be all-out war. While Article 5 allows for any form of military action in response to cyber activity deemed to be an “armed attack,” kinetic warfare[26] is the last resort as it would result in catastrophic loss of life.

War with Russia should be avoided at all costs, but if Russia feels backed into a corner, it may initiate a serious attack, in which case NATO would have no choice but to respond appropriately. Russia’s cyber threats must be handled with the utmost care to avoid escalation. Being fully prepared with plans in place should be one of NATO’s highest priorities. Cooperation between NATO members as well as their partners, would greatly improve NATO resilience and integrity in dealing with cyber threats from Russia.

[24] NATO. "Collective Defence - Article 5." NATO. June 12, 2018. Accessed February 11, 2019. https://www.nato.int/cps/en/natohq/topics_110496.htm?selectedLocale=en.
[25] Hacking back is the process of identifying the source of attacks on a system and directly attacking the source.
[26] Kinetic warfare is the use of physical force such as bombs, guns, explosions, impacts, etc.

1.2 A Comparative Analysis of NATO & Russia's Cyber Capabilities

Jennifer Yan

1.2.1 Introduction

Over the past three decades, the rapid development and fast-growing availability of cyber technology[27] has created new threats and opportunities for cyber-based attacks, adding a new dimension to the global security landscape. The Russian Federation is believed to be a highly capable actor in cyberspace,[28] demonstrating impressive power and strategy. Despite its official statement of taking a purely defensive approach to cyber,[29] Russia appears to pursue a more offensive cyber strategy.[30] The volume and severity of malicious cyber activity against NATO and its member states by Russia has increased exponentially in recent years. With hybrid threats from Russia and other non-state actors increasing, it is important for NATO to enhance its cyber security strengths to counter future attacks.

This chapter compares NATO and Russia's cyber-related doctrine, adaptation, and cyber capabilities. The first part of this chapter will give an overview of Russian cyber doctrine, and will provide examples from Estonia, Georgia, and Ukraine of Russia's differing uses of cyber tools in these attacks. The second part of this chapter will focus on NATO's current legal framework and analyze how institutions have evolved to create structures and procedures within the alliance. It will assess NATO's cyber capability while considering the role of independent state actors, who have the potential to contribute their individual capabilities to the alliance when mutually agreed.

NATO's cyber capacity is purely defensive[31] which creates a comparative disadvantage over Russia. Unlike NATO, which is a collective organization of states with stringent standards, Russia operates independently and refuses to follow international norms and rules. NATO can respond by improving its integrity and building

[27] Cyber technology is any computer technology that involves internet, can be both hardware and software like communication, servers, security mechanisms and network classifications for various needs and processes in cyberspace.
[28] Frank Cilluffo, "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." *Testimony before the US House of Representatives, Committee on Homeland Security Subcommittee on Cyber security , Infrastructure Protection, and Security Technologies* (2013).
[29] Sergei Medvedev, 2015. "Offense-Defense Theory Analysis Of Russian Cyber Capability". *Calhoun.Nps.Edu*. Accessed February 10 2019. https://calhoun.nps.edu/handle/10945/45225.
[30] Ibid.
[31]"Brussels Summit Declaration," Press Release (2018), 074, NATO, July 11, 2018 https://www.nato.int/cps/en/natohq/official_texts_156624.htm

resilience against future attacks. In sum, this chapter will provide policy recommendations to NATO on future actions to improve resilience and integrity against Russian cyber threats. This will include increased risk assessment by training within the alliance, clarifying NATO's collective defense posture in cyberspace, and enhancing cooperation with other international organizations and partners to increase cyber defense capabilities.

In an increasingly interconnected and digital world, "cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks.[32]" Russia will remain a primary threat in the cyber domain,[33] its cyber capabilities will continue to expand, and its operations will become more sophisticated, and more difficult to track. Without understanding the underlying causes of Russia's behaviors in cyberspace through a comprehensive analytical framework, NATO policymakers will not be able to efficiently respond and defend against cyber-attacks.

1.2.2 Russia's Cyber Capabilities

Russia is undoubtedly one of the leading powers in the cyber arena, and its status rests on two pillars: its expertise of advanced technology and its willingness to use cyber tools to achieve political objectives. The *Information Security Doctrine of the Russian Federation*[34] published in 2000, sets the tone of Russia's official view of cyber power in its national security strategy and military doctrine. The doctrine identified information warfare from other states as potential threat to Russia's information security.[35]

Russia's definition of cyber warfare and its strategic use of cyber capabilities show how its view of cyber is different than that of its Western counterparts. The term

[32] European Commission, President Jean-Claude Juncker´s State of the Union address 2017, September 13, 2017, https://ec.europa.eu/commission/sites/beta-political/files/soteu-explained_en.pdf

[33] The recognition that cyberspace is a domain for military operations [1] has led to investigation of what constitutes key cyber terrain – "those physical and logical elements of the domain that enable mission essential warfighting functions". Bodeau, Deborah, Richard Graubart, and William Heinbockel. "Mapping the cyber terrain: Enabling cyber defensibility claims and hypotheses to be stated and evaluated with greater rigor and utility." MITRE, McLean, VA, Tech. Rep. MTR130433(2013).

[34] "Information Security Doctrine of the Russian Federation," Ministry of Foreign Affairs of theRussian Federation, last modified December 29, 2008, http://www.mid.ru/bdomp/nsosndoc. nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

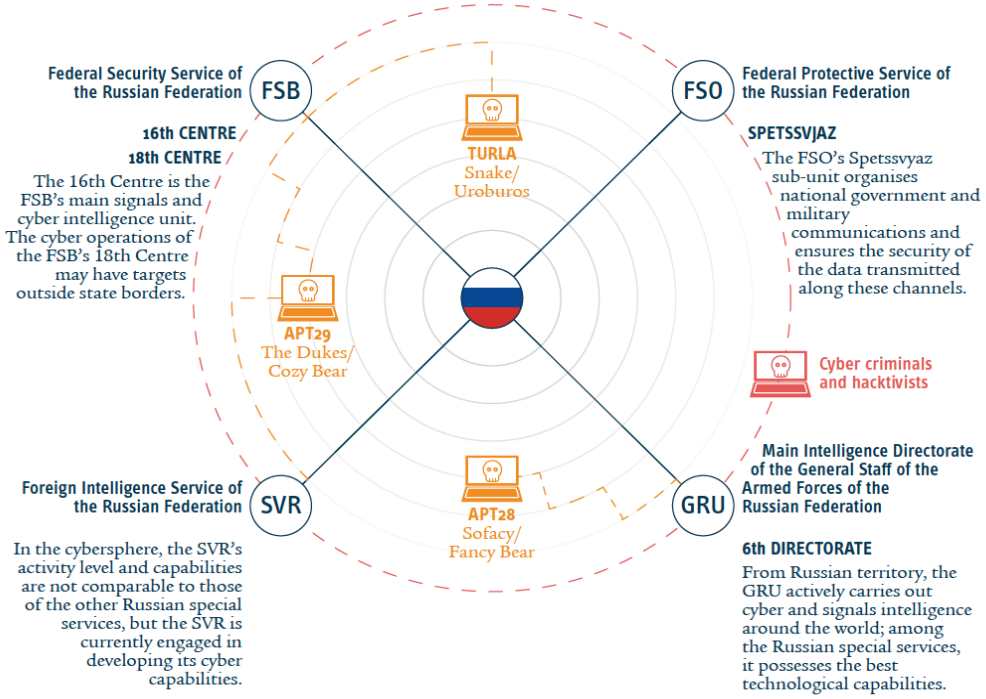
[35] Keir Giles, "'Information Troops' – a Russian Cyber Command?." Paper presented at the 3rd International Conference on Cyber Conflict. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2011. http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussia nCyberCommand-Giles.pdf

“cyber” (kiber) or “cyber warfare” (kibervoyna) is very rarely used in Russian discourse. Instead, they use the term “informationization”, which incorporates cyber operations into the broader concept of information warfare. This includes information-psychological operations, computer network manipulations, and electronic warfare. In other words, cyber is seen by Russia as a subcomponent of information warfare, which it considers a tool in its own operational domain.[36]

Although there are no offensive operations mentioned in this doctrine, there is compelling evidence of Russian attacks that suggest otherwise. Russian intelligence agencies are presumed to have some of the top-ranking cyber exploitation[37] capabilities in the world[38] (see Figure 1[39]). These powers are mainly held by multiple government and military security services. The Information Security Centre of the Federal Security Service (FSB) is the chief executive branch of Russian cyber security . In recent years, its responsibility has gone beyond protecting the government’s IT networks to include monitoring the media and internet, as well as overseas operations. The Foreign Intelligence Service (SVR), created from the Soviet-era KGB, is now also developing its cyber capabilities. The military’s Main Intelligence Directorate (GRU), is additionally a special force unit of the Russian military suspected of playing a major role in the 2008 Russo-Georgian conflict, 2014 Crimea Annexation, and the 2016 U.S. presidential election.[40]

[36] Michael Connell and Sarah Vogler. 2017. P3.
[37] Also known as “cyber espionage”, The Tallinn Manual on the International Law Applicable to Cyber Warfare, non-binding opinion of an independent group of experts on the legal aspects of cyber threats provides a narrow definition of cyber espionage: “Any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party to the conflict” (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012, p. 159)
[38] Michael Connell and Sarah Vogler. 2017.
[39] "Hacks, Leaks And Disruptions – Russian Cyber Strategies | European Union Institute For Security Studies". 2019. P54
[40] "What Is Russia's GRU Military Intelligence Agency?". 2019. U.S.. Accessed February 15 2019. https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-idUSKCN1MF1VK?curator=MediaREDEF

FIGURE 1 | Russian cyber espionage/attack actors



Data: Estonian Foreign Intelligence Service, 2018.

The Russian military, which experienced a steep decline in budget and prestige during the 1990s, is a relatively late addition to the cyber arena. However, after 2013, the Ministry of Defense (MOD) announced plans to establish its "cyber troops" made up of hackers, journalists, and equipped specialists. This proposal sought to improve the cyber capability of the Russian military, which lagged behind its peers. If the Russian military managed to develop its own offensive cyber capabilities successfully, the result could be an increase in use of cyber powers in future conventional military operations.[41]

Together, these institutions have constructed the Russian cyber strategy framework and coordinated most of the country's domestic and foreign cyber operations. These agencies keep their cyber practices highly-secretive, making it difficult for international analysts to assess their capabilities. This exemplifies the deep strategic thinking of Russian security services and how far Moscow's approach to both internal and external cyber policy has evolved since 2000.[42]

[41] "V Minoborone RF sozdali voiska informatsionnih operatsii" [Russia's Ministry of Defense set up information troops], Interfax, February 22, 2017, http://www.interfax.ru/russia/551054
[42] "Hacks, Leaks And Disruptions – Russian Cyber Strategies | European Union Institute For Security Studies". 2019. P15

State actors only represent the official facade of Russia's cyber approach. The foundation of Russia's global cyber capacity is built on its deployment of non-state actors. Malicious cyber activities coming from Russia are characterized by a unique connection of government, crime syndicates, proxy cyber-activists and even cyber technology companies. Although non-state actors possess relatively modest cyber technology, they control vast online resources and represent a significant part of Russian cyber capacity. As long as aggressive cyber operations are executed in a manner that supports Russian national interests and objectives, it does not matter if they are an official part of the Russian government.[43]

In 2002, a group of student hackers in Siberia attacked a pro-Chechen separatist website, forcing it to close. Their actions were enthusiastically praised and defended by the FSB. This attack signaled the Kremlin's new approach of outsourcing cyberattacks and hacking to non-state actors: proxies, criminal groups and hacktivists - some of which have been directly aided by the Russian security services.[44] This tactic allowed Russia to lower the cost of cyber operations, reduce reputational risks, and create plausible deniability, as governmental support behind perpetrators is much harder to detect.[45]

The 2007 events in Estonia were an example of Denial-of-Service (DoS) and Distributed Denial of Service (DDoS) attacks in retaliation over the controversial removal of a Soviet-era statue in Tallinn. The series of attacks disabled many government websites and critical infrastructure systems in the country, destabilizing Estonian society by "creating anxiety among people that nothing is functioning, the services are not operable".[46] This also created a far-reaching, large-scale psychological fear throughout the Estonian population and policy-makers. This has echoed Russia's recognition on the information-psychological aspect of information warfare.

[43] Medvedev, Sergei A. 2015. P17~32
[44] "Kremlin Accused of Opposition Phone Call Leaks," BBC, December 20, 2011, https://www.bbc.com/news/av/world-europe-16279131/kremlin-accused-of-opposition-phone-call-leaks; "Navalny's Private E-Mails Leaked," Moscow Times, October 27, 2001, https://themoscowtimes.com/news/navalnys-private-e-mails-leaked-10439; "Mikhail Klikushin, Former Russian Prime Minister Caught on Camera Having Sex With Opposition Leader," Observer, May 4, 2016, http://observer.com/2016/04/former-russian-prime-minister-caught-on-camera-having-sex-with-opposition-leader/
[45] "Russia Denies U.S. and UK Allegations of Global Cyber Attack," Moscow Times, April 17, 2018, https://themoscowtimes.com/news/russia-denies-us-and-uk-allegations-of-global-cyber-attack-61195
Jaak Aaviksoo "Looking West – Estonian Minister of Defense Jaak Aaviksoo," Jane's Intelligence Review, October 2007.

One year after a successful attempt to undermine Estonian government and society, the cyberattacks in Georgia marked the employment of cyberattacks as a tool in military conflict. This incident featured a new, sophisticated cyber espionage campaign that coincided with the beginning of military conflict in Georgia and is attributed to the Russian security services.[47] A malware, WIN32/ Georbot, was used to collect classified, sensitive information related to national security in the Georgian state networks. The 2008 attacks led to a shift in military thinking and conventional military conflicts that "now have a cyber dimension".[48]

The scale and impact of cyber espionage campaigns in Ukraine from 2014 to 2017 was unprecedented. Along with many DDoS attacks and website damages, a series of malware affiliated to Russian attackers[49] was also detected. The destructive cyber-attacks were carried out against critical infrastructure, including the energy, transportation, and financial sectors, creating wide-ranging economic loss and extensive damage to digital infrastructures for Ukraine. It seems these attacks deliberately targeted specific countries and their infrastructure and were meticulously planned.[50]

Through a close analysis of the successive cyber-attacks conducted by Russian-backed hackers in Estonia, Georgia and Ukraine in a ten-year timeframe, it can be concluded that Russia has drawn lessons from past experiences to refine its cyber techniques and is able to operate at three levels of cyber-offensive actions. The first level includes classic information-gathering methods, but what distinguishes Russia from other major cyber actors is the way it operates at its two highest levels. The second level takes information collected through cyber exploitation and utilizes it in targeted information campaigns to create disruption and destabilization for Russian adversaries and vulnerable countries. The third level aims to destruct critical infrastructure as a military tool in an armed conflict.

[47] LEPL Date Exchange Authority and the Ministry of Justice linked the cyberattacks to "Russian Official Security Agencies". See "Cyber Espionage against Georgian Government. Georbot Botnet," CERT.gov.ge, http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf

[48] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," SCMagazine, August 2

[49] Snake/Uroburos/Turla, RedOctober, MiniDuke, NetTraveler, "Hacks, Leaks And Disruptions – Russian Cyber Strategies | European Union Institute For Security Studies". 2019. P56

[50] "Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says". 2019. *Defense One*. Accessed February 21 2019. https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/.

1.2.3 NATO Capacities and Limitations

The increasingly hostile actions by Russian government and non-state actors have undermined the stability of countries near Russia, creating urgency in the international community to rethink cyber security posture and international cyber norms.[51] As an organization representing multilateral security cooperation with sturdy institutional support, NATO has responded to this fast-evolving threat with several measures.

NATO is not new to the concept of cyber security and its implications in the international sphere. The concept of "cyber security" was first recognized at the 2002 NATO Summit in Prague, where member states committed to the "initiation of measures to strengthen defense against cyber-attacks".[52] In order to establish institutions to combat this growing threat, NATO Computer Incident Response Capability (NCIRC) and NATO Cyber Defense Program were formed. In 2008, the NATO Cooperative Cyber Defense Center of Excellence (CCD CoE) was established at the initiative of Estonia after the 2007 cyber-attacks. CCDCoE is a multinational cyber defense hub providing expertise to NATO by coordinating education and training, researching solutions, and maintaining legal communication in cyber-related area.[53] NATO's next landmark of institutional adaptation took place at the 2016 Warsaw Summit, following the Enhanced Cyber Defense Policy endorsed by the alliance at the Wales Summit in 2014.[54] This policy states that malicious cyber activity, on a case-by-case basis, may lead to invocation of a collective Article 5 response.[55] In 2016, cyberspace was officially recognized as a NATO operational domain, requiring NATO to be able to defend itself in cyberspace as it does in air, land and sea. As stated in the Warsaw summit declaration:

[51] "Hacks, Leaks And Disruptions – Russian Cyber Strategies | European Union Institute For Security Studies". 2019. *Iss.Europa.Eu*. Accessed February 14 2019. https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-%E2%80%93-russian-cyber-strategies.
[52] NATO, 2003. The Prague summit and NATO's transformation [online]. NATO Public Diplomacy Division. Available from: http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf[Accessed 29 March 2013].
[53] "About Us". 2019. *Ccdcoe.Org*. Accessed February 14 2019. https://ccdcoe.org/about-us/.
[54] NATO, 2014. NATO launches industry cyber partnership [online]. Available from: http:// www.nato.int/cps/en/natohq/news_113121.htm [Accessed 23 February 2015].
[55] "The North Atlantic Treaty". 2019. *NATO*. Accessed February 14 2019. https://www.nato.int/cps/ie/natohq/official_texts_17120.htm.

> "This will enable the Alliance to better protect its networks, missions and operations, with more focus on cyber training and planning. NATO's cyber posture remains defensive, but this is a clear sign that the Alliance is strengthening its collective defense in all areas. Allies also pledged to strengthen their own cyber defenses and share more information and best practices as a matter of priority."[56]

NATO's institutional adaptability and strength provide useful tools for dialogue, policy development, and decision making on cyber issues. The Tallinn Manual, published in 2013, has advanced NATO's legal thinking and strategic vision on critical cyber issues, providing non-binding possible responses to cyber-attacks under existing international law.[57] However, it is still unclear what level of cyber-attack will be considered an armed attack that can be met with an Article 5 response, and what a NATO collective response would look like. Russia has exploited this ambiguity with its continued aggressive behavior.[58]

NATO has adopted a pragmatic defensive role in its cyber security posture. It is not involved in developing offensive capabilities, which is defined as possession of any cyber weapons that can be used to manipulate, disrupt, degrade or destroy targeted information systems and computers.[59] NATO's defense capability relies on the resources and assets voluntarily provided by individual member states and allies.[60] The developments of offensive cyber capacity remain in the realm of national institutions and intelligence agencies of individual member states. The Alliance's main role has been focused on defending its own institutional infrastructures and computing networks in the North Atlantic region. On August 2018, at NATO's newly established operation center in Belgium, the U.S., Estonia and the UK offered their cyber warfare capabilities to assist NATO on a case-by-case basis.[61]

---

[56] "NATO Warsaw Summit 2016 Declaration". 2019. *Msz.Gov.Pl.* Accessed February 14 2019. https://www.msz.gov.pl/en/c/MOBILE/foreign_policy/nato_2016/documents/nato_warsaw_summit_2016_declaration.
[57] Fleck, D., 2013. Searching for international rules applicable to cyber warfare – a critical first assessment of the new Tallinn Manual. Journal of conflict & security law, 18 (2), 331–351.
[58] Robert McLaughlin and Michael Schmitt, "The Need for Clarity in International Cyber Law", Policy Forum, September 18, 2017, https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/
[59] Smeets, Max. "Integrating offensive cyber capabilities: meaning, dilemmas, and assessment." defence Studies 18.4 (2018): 395-410.
[60] Jamie Shea, "How is NATO Meeting the Challenge of Cyberspace," PRISM, Vol. 7, No 2, December 21, 2017, http://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/.
[61] "US To Offer Cyberwar Capabilities To NATO Allies". 2018. *CNBC*. Accessed February 15 2019. https://www.cnbc.com/2018/10/03/us-to-offer-cyberwar-capabilities-to-nato-allies.html.

Deterrence of cyber-attacks is difficult to achieve, since it is an area where large-scale damage can be done with an extraordinarily limited amount of time and investment. The pressure to defend NATO member states will only increase in the coming years with increased risk of Russian cyber espionage. One of NATO's current core objectives increasing security to prevent hackers from infiltrating NATO's system and denying them access to achieve their intended goals.[62] Similar to other areas of security, NATO has so far relied on cooperative external and internal relationships, to study and follow international cyber security laws and solve cyber-related problems.[63] This creates challenges for NATO in dealing with a state actor like Russia that does not follow international norms and rules.

NATO has obtained a certain level of cyber capability that has defended the organization's information networks relatively well over the past decade and has set up a mechanism to facilitate further improvement and intelligence exchanging between allies. After Russia's illegal annexation of Crimea, many NATO member states-imposed sanctions on the country. Deterred from using further military action in Ukraine, Russia began to implement its cyber tactics. 2017 saw the outbreak of the NotPetya malware attack, which was officially attributed to Russia in February 2018 by Australia, Denmark, Japan, Canada, New Zealand, the U.K. and the U.S. This event demonstrates a global coalition in cyber terrain joined by NATO allies and some of the alliance's close partners, proving that intelligence sharing and collective attribution are feasible in a short amount of time.

1.2.4 Looking Ahead: Russia's Possible Future Strategy and Next Steps for NATO

Russia will continue to develop its cyber capabilities and increase assertiveness in cyberspace as critical tools to expand its spheres of influence and control worldwide. Given Russia's interest in hindering Western integration in the Western Balkans, the next location of Russian cyber operations will likely be in this region. The use of cyber tools by Russia to create tension and disruption is likely to increase. In order to maintain

[62] Healey, J. and van Bochoven, L., 2012. NATO's cyber capabilities: yesterday, today, and tomorrow [online]. The Atlantic Council. Available from: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf [Accessed 28 March 2013].
[63] Burton, Joe. 2015. "NATO's Cyber defense: Strategic Challenges and Institutional Burton, Joe. Burton, Joe. 2015. "NATO's Cyber defense: Strategic Challenges and Institutional Adaptation." defense Studies 15 (4): 297–319.

security and stability against this challenging background, NATO should consider the following steps to increase integrity and resilience against cyber threats from Russia:

Formalize the cyber deterrence strategy to create greater cohesion. This could be through advances in the consultation process within the alliance to implement clear, top-down guidance. Due to the need for a rapid response in the case of a cyber-attack, policymakers from member states need to consider making cohesion a priority in order to create a collective response. This can be done by sharing data, reporting cyber incidents, synchronizing assets among the allies, and by clearly defining national minimum standard in cyber capabilities.

Work closely with partners to expand the range of responses. NATO's strength in cyber defense comes from partnerships with international organizations and cooperation with NATO partner countries. When facing cyber threats, greater cooperation is critical to integrate efforts that are outside of NATO's domain. As highlighted by the recent attributions of NotPetya attacks, a global will for collaboration between non-NATO and NATO states, when any country is under attack, is achievable. There are many things the EU can do to help further NATO's security goals, such as cyber security -certificated devices imported into European markets.

Organize cyber decision-making procedures. To enable the alliance to respond promptly in an emergency, NATO needs to consider how cyber operations can be integrated into its readiness plan, and fully become part of NATO's military structure. Therefore, cyber warfare needs to be part of the strategic plan. Information and technology sharing within the alliance should be promoted to increase cooperation, thus facilitating the strategic decision-making process.

1.2.5 Conclusion

At the 2018 Brussels Summit, Heli Tiirmaa-Klaar, Estonia's first cyber ambassador, claimed that the alliance is only at roughly "ten percent of readiness" in terms of understanding and preventing cyber threats.[64] The lack of readiness creates vulnerabilities that hostile actors can take advantage of. The Russian government's

[64] Catherine Stupp, "Estonia's First Cyber Ambassador Seeks to Improve Global Cyber Defense," The Wall Street Journal, September 7, 2018,
https://www.wsj.com/articles/estonias-first-cyber-ambassador-seeks-to-im....

sophisticated cyber weapons arsenal indicates an offensive approach is playing a greater role in Russian cyber capability.[65] Its effectiveness lies in its ability and willingness to use aggressive cyber tactics as part of its conventional military operations, blurring the lines between domestic and international policy. Western countries are concerned with securing confidential and personal data and critical infrastructure as the primary goal in cyber security policy. Russia considers information security and Internet control a main priority.[66] From 2007 to 2017, Russia has demonstrated steadily evolving cyber capability as part of its conventional military operations. The conflicts in Ukraine have provided testing ground for Russia to refine their novel techniques.

Since its founding in 1949, NATO's goal has been to maintain collective defense and provide military security in the transatlantic space. Its tasks have shifted to emerging international security challenges over time. Russia has forced NATO to develop a strategic framework to confront challenges in the uncharted area of cyberspace. Allies are committed to enhancing information-sharing and mutual assistance within the organization in preventing, mitigating and recovering from cyber-attacks.

However, ambiguity remains due to a lack of consensus within the alliance on how to integrate cyber into NATO's overall deterrence posture, and no clear design of a cyber deterrence posture.[67] Unlike Russia, which is a single entity with high efficiency and consistent policy, NATO is an organization consisting of many independent state actors, and it is each nations responsibility to ensure its response is in compliance with international law. Some have already speculated this may pose disadvantages and constraints to NATO's actions in comparison to Russia.[68] It is time to address what NATO could and should do in response to this sophisticated threat. As a collective defense organization, NATO must develop a deterrence posture with advanced

[65] Connell, Michael, and Sarah Vogler. Russia's approach to cyber warfare. Center for Naval Analyses Arlington United States, 2017.
[66] "Hacks, Leaks And Disruptions – Russian Cyber Strategies | European Union Institute For Security Studies". 2019.
[67] Stefan Soesanto, "In Cyberspace, Governments Don't Know How to Count," *Defense One*, September 27, 2018, https://www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/.
[68] "Only states that are injured may impose countermeasures: This means that a victim state's allies may not impose 'collective countermeasures' on the wrongdoing state if only the victim state was actually injured." Ashley Deeks, "Prime Minister May's Use-of-Force Claim: Clarifying the Law That Governs the U.K.'s Options', Lawfare, March 13, 2018, https://lawfareblog.com/prime-minister-mays-use-force-claim-clarifying-law-governs-uks-options

strategic thinking, more assertive cyber strategies, and increase its capabilities to respond to attacks.

1.3 The Ukraine Cyber Attack: Sandworm and Critical Infrastructure

Omar Tabuni

1.3.1 Introduction

Ukraine and Russia are historically and culturally bound together. Despite this bond, Ukraine has increasingly voiced its interest in joining Western institutions such as NATO and the EU. In response, Russia has repeatedly stated their opposition to Ukraine's aspirations. Tensions between the two countries peaked in 2014 after the annexation of Crimea resulting in a serious downturn of relations between Russia and the West. Russia has utilized hybrid warfare tools to destabilize Ukraine, further eroding international norms.[69] Moscow's use of malicious cyber activity specifically targeting Ukraine's critical infrastructure (CI) is a key example of Russia's hybrid warfare.[70]

Critical infrastructure is "an asset or system which is essential for the maintenance of vital societal functions.[71]" While not everything concerning CI falls under cyber security, many essential elements do. Banks, railroad systems, and energy suppliers are all vulnerable to cyber-attacks. By destroying or hindering CI, malevolent actors threatens the national security of the target country. Much like other hybrid threats, attacks on CI are difficult to attribute and reprimand the assumed culprits.

The NATO Computer Incident Response Capability (NCIRC) unit is focused primarily on strengthening and protecting its internal CI systems. This allowed member states to individually secure and protect their own infrastructure. The 2007 cyber-attacks in Estonia revealed limitations in NATO's cyber defense capability. The NCIRC was overwhelmed by frequent malicious activity launched against NATO's network infrastructure to defend and protect allies' CI. This forced the Alliance to take a series of steps to ensure a continuation of resilience and deterrence mechanisms. In 2008, NATO presented a new defense policy which extended its cyber defense capacities.[72] This new policy set up the Cyber Defense Management Authority (CDMA), a fast

[69] "NATO-Russia Relations: The Background." NATO. April 2018. Accessed February 26, 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_04/20180426_1805-NATO-Russia_en.pdf.
[70] Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." Wired. April 13, 2018. Accessed February 21, 2019. https://www.wired.com/story/russian-hackers-attack-ukraine/.
[71] "Critical Infrastructure." European Commission Migration and Home Affairs. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
[72] Vincent Joubert "Five years after Estonia's cyber attacks: lessons learned for NATO?" Published by: NATO Defense College (May. 1, 2012)

response center to defend against malicious activity on members' critical national infrastructure and NATO bodies. The CDMA is responsible for “initiating and coordinating immediate and effective cyber defense action where appropriate”[73]. The defense policy also established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) to research and develop cyber deterrence and provide training to cyber defense staff.

The CDMA, however, failed to prevent the Russian cyber-attack known as Notpetya from spreading across NATO member States[74]. According to the CCD CoE, the massive attack infected thousands of devices across European countries and the malicious code hit major industries and critical infrastructure.[75] NATO needs advanced real time monitoring capabilities in Ukraine to tackle complex challenges stemming from the evolution and advancement of Russian cyber capabilities in Ukraine’s virtual environment.

1.3.2 NATO’s Cyber Defense Policy in Ukraine

Despite improvements in NATO’s cyber defense capabilities, the 2017 “NotPetya” cyber-attack on Ukraine highlight vulnerabilities in CI that could be exploited by Russia. The NotPetya attack affected computers running the Microsoft Windows operating systems in Ukraine and consequently spread across Europe[76]. The malware used in this attack was programmed to damage operating systems beyond repair, could spread on its own, and avoid human intervention. The NotPetya attack was built with a level of sophistication commonly attributed to high level state intelligence. This is significant to NATO since the NotPetya attack started in Ukraine in 2017, and soon after spread across Europe negatively affecting various sectors of CI in industries such as banks, government, retail, and power systems.[77] This is why NATO needs to ensure that Ukraine is able to deal with these attacks, as it was a testing ground for Russian cyber tactics that could affect the whole alliance. To strengthen deterrence and

[73] Nato. "Cyber Defence." NATO. Accessed March 05, 2019. https://www.nato.int/cps/en/natohq/topics_78170.htm.
[74] "NATO CCD COE Attributed the Massive NotPetya Attack to a 'state Actor' and Call for a Joint Investigation." Security Affairs. October 14, 2017. Accessed March 05, 2019. https://securityaffairs.co/wordpress/60603/cyber-warfare-2/nato-notpetya-state-actor.html.
[75] Ibid
[76] NOTPETYA TECHNICAL ANALYSIS LogRhythm Labs. July 2017. https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical-analysis-logrhythm-labs-threat-intelligence-report.pdf 2
[77] NATO CCD COE “Notpetya and wannacry call joint response from international community”. Jun 30, 2017

resilience, NATO and the Computer Emergency Response Team of Ukraine (CERT-UA) need a joint incident response team to operate under the Technical Arrangement framework to deter malicious activity and provide both organizations the ability to study the cyber-attacks in their virtual environment to enhance resiliency and mitigate cyber threats.

1.3.3 Case Study: Ukraine Power System Attacks in 2014

Since 2014, Russia has broadened its activities by meddling in Ukrainian internal affairs via hybrid warfare.[78] Russian intelligence has also tested a new form of malware known as Blackenergy3 to enhance cyber-enabled techniques on Ukraine. Russia has continued "a digital blitzkrieg that has pummeled Ukraine for the past three years—a sustained cyber assault unlike any the world has ever seen".[79] Russia's cyber espionage activity has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, energy. The initial creation of BlackEnergy was a simple Trojan, mainly used to execute denial of service attacks. The authors of this malware enhanced the second and third version of Black Energy. The third variant has improved capabilities building on the previous features and adding newer advanced features that can accelerate and diversify the attack. Some distinctive features of Blackenergy3 includes encryption and code compression which protects the malicious code from emulation.

Early deployments of industrial control components (CSI) in CI facilities prior to the internet were stand-alone systems not connected to networks. However, with the modernization of technology, cyber threats emerged as a predominant issue for CI, as was true in the case of the Ukrainian cyber-attacks.[80] The reports released by TSN Ukrainian News outlet, the U.S. Department of Homeland Security (DHS), and numerous other agencies have concluded that the cyber-attack breached the power infrastructure from the outside. The attack utilized BlackEnergy3 and other related malware as tools for their cyber tactics. The perpetrators conducted preliminary

[78] Ibid.
[79] Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." Wired. April 13, 2018. Accessed February 24, 2019. https://www.wired.com/story/russian-hackers-attack-ukraine/.
[80] L., Ronald. "Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." Homeland Security Digital Library. March 01, 2016. Accessed February 18, 2019.

scanning to breach the system and demonstrated capabilities in executing attack tools and components. This included: dropping malware payloads and spear phishing campaigns, obtaining access control of SCADA nodes,[81] sending command shutdown messages to destroy SCADA system and slow down system recovery, disrupt service calls (denial-of-service attack), and launching information warfare.[82]

On December 23rd, 2015 Kyivoblenergo, a regional Ukrainian electricity distribution company, experienced power outages from a security breach into the company's computer and SCADA systems. At approximately 3:35 p.m. local time, seven 110 kV and 23 35 kV substations were disconnected from the internet for three hours. Additional updates into the situation illustrated that the malicious activity spread to other portions of the distribution grid and created a fluster. The Ukrainian TSN media outlet investigating the incident determined that external cyber-attackers remotely controlled the SCADA distribution management system. The report detailed three regional electric power distribution companies impacted by the malicious activity which affected approximately 225,000 customers. The cyber-attack indicated that the malicious actors intended to paralyze eastern Ukraine and shut down all critical government systems. The cyber-attack was later attributed to the Russian Intelligence Cyber espionage team by the Ukrainian government.[83]

In 2015-16, "Sandworm," an espionage group, was attributed by the Ukrainian authorities to have undertaken malicious cyber activity against the government and other companies. SandWorm has been classified as a Russian state actor that has exploited vulnerabilities and malwares to carry out attacks against political targets. The attacker breached the networks of media outlets, railway firms, and others by inserting malicious code and damaging terabytes of data. The attacks followed a malicious seasonal pattern. In the winters of both years, Sandworm caused widespread power outages—the first recorded blackouts committed by hackers.[84] This was unique because malicious actors demonstrated multidimensional capabilities, ranging from

[81] A SCADA (Supervisory, Control, And Data Acquisition) server is a node that loads a process database in memory and collects process information from one or more control devices
[82] "New Wave of Cyberattacks against Ukrainian Power Industry." WeLive Security. January 21, 2016. Accessed February 11, 2019. https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/.
[83] ICS.SANS. "Analysis of the Cyber Attack on the Ukrainian Power Grid". March 18, 2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[84] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired. December 07, 2018. Accessed February 11, 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

spear phishing campaigns, variants of the BlackEnergy3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain “backdoor” access into the information technology (IT) networks of the electricity companies. The main victims of these attacks include NATO and Ukrainian-governmental organizations.[85] John Hultquist, senior manager of cyber-espionage threat intelligence for iSIGHT, has said "We can confirm that NATO was hit; we know from several sources that multiple organizations in Ukraine were targeted […] we have seen them using Ukrainian infrastructure as part of their attacks".[86]

1.3.4 Conclusions

Ukraine’s government has struggled to defend itself against Russia’s cyber-attacks, despite NATO assistance.[87] This case study shows how Russia utilizes Ukraine as a testing ground for enhancing their cyber-attack capabilities. The NotPetya attack that was initially targeted at Ukraines CI, however, based on its replicating features, it eventually spread to parts of the EU and to NATO member states. NATO and Ukraine face similar challenges in protecting CI against the growing threat of Russian cyber-attacks and capabilities. Therefore, it is in NATO’s best interest to establish a Technical Arrangement on Cyber Defense between the NCIRC, CCD COE, CDMA, and the (CERT-UA)[88]. This allows the joint incident response team to deal directly with threats in real time before they escalate into national-level or regional emergencies. The Technical Arrangement framework between the CDMA, NCIRC, CCD, and CERT-UA would include but are not limited to: bringing situational awareness and early warning, advanced cyber intelligence and information security, cyber-attack attribution capabilities, and information and intelligence sharing across organizations in real-time. The Technical Arrangement provides a framework for exchanging information and

[85] Finkle, Jim. "U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage." Reuters. January 08, 2016. Accessed February 28, 2019. https://www.reuters.com/article/us-ukraine-cyber security -sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108.
[86] Lemos, Robert. "Suspected Russian "Sandworm" Cyber Spies Targeted NATO, Ukraine." Ars Technica. October 14, 2014. Accessed February 28, 2019. https://arstechnica.com/information-technology/2014/10/suspected-russian-sandworm-cyber-spies-targeted-nato-ukraine/
[87] "How Ukraine's Government Has Struggled to Adapt to Russia's Digital Onslaught." Council on Foreign Relations. Accessed February 27, 2019. https://www.cfr.org/blog/how-ukraines-government-has-struggled-adapt-russias-digital-onslaught.
[88] Ukrinform. "Ukraine's Foreign Intelligence Service Helps Thwart Another Massive Cyber Attack." Ukrinform News. January 01, 2100. Accessed March 05, 2019. https://www.ukrinform.net/rubric-economy/2581788-ukraines-foreign-intelligence-service-helps-thwart-another-massive-cyber-attack.html.

sharing best practices between emergency response teams. NATO should improve resilience and integrity in cyber defense mainly in Ukraine to ensure stability and security in Europe. It is vital for NATO to monitor malicious activity with the cooperation of CERT-UA in their virtual environment. Russia currently utilizes Ukraine as a testing ground for new cyber technologies. Therefore, NATO needs to be prepared and ready to tackle complex challenges stemming from the evolution and advancement of Russian cyber capabilities.

The Technical Arrangement framework would allow NATO and Ukraine to collectively discuss and tackle cyber defense-related issues at the operational, strategic and political levels. In addition, having a NATO a joint incident response team committed and focused on cyber space provides an essential basis for comprehensive review and analysis of specific cyber issues in key areas. This helps the Alliance understand the evolution of the cyber environment and identify the strategic issues involved, underlining the importance of continuing investment in research and capability development**.** If NATO fails to effectively establish a technical arrangement with CERT-UA to ensure deterrence and resiliency, Russia will continue to use Ukraine as testing ground for cyber capabilities the may spread to NATO member states, thus threatening the security of the alliance.[89]

[89] Unian. "NATO Helping Ukraine with Strengthening Cyber Defenses." Information Agency. October 03, 2018. Accessed February 27, 2019. https://www.unian.info/politics/10285461-nato-helping-ukraine-with-strengthening-cyber-defenses.html.

Conclusion

Russia's increasingly aggressive use of malicious cyber activity has undermined the integrity of NATO members, and will continue to do so unless NATO takes action. Focusing on attribution can allow blame to be accurately laid on Russia when their government is behind an attack and is essential in identifying the ideal response. As we have seen, there is minimal legal framework restricting operations in the cyber domain, but NATO retains only defensive measures. This puts more reliance on cooperation between member states and intelligence agencies in responding to attacks when a cyber offensive is warranted. A detailed plan for response should be developed in advance based on degree of certainty of attribution and scale of the attack. Russia's actions thus far have been unacceptable, but if they were to attack the critical infrastructure of a NATO member state directly, NATO members must be prepared to launch a counter-offensive. This is of course a last case scenario, as avoiding escalation with Russia should be NATO's top priority in maintaining their resilience and integrity.

Cyber Security Policy Recommendations:

- Improve attribution technology
- Increase information sharing between intelligence agencies in relation to cyber-threats
- Increase communication between policymakers and technical experts related to cyber
- When an attack is attributed with high accuracy and certainty, an appropriate active defense response is necessary to limit escalation. These can include sanctions or hacking-back.
- Enhance core collective defense in the cyber domain.
- Create a more developed legal framework to respond to cyber threats; deterrence of malicious cyber activities needs to be conducted with strategic rethinking.

- Provide greater funding and support to the cyber defense organizations such as CCD CoE and aid in their expansion.
- Increase budget allocation to the research of cyber defense to improve threat assessment and risk analysis.
- Create a Technical Arrangement between NATO and CERT-UA to provide a real-time operational capability for both organizations and mitigate Russian cyber threats.
- Expand research and development on cyber defense in Ukraine in order to contain and combat Russia’s cyber capabilities from spreading to NATO member states

2. Ethnicity, Religion, and Their Role in Hybrid Threats

Introduction

Hybrid threats are constantly evolving. Because of this, it is important to understand an often-ignored instrument in the hybrid toolbox: the utilization of religion and ethnicity to create chaos and division. Each chapter in this section will examine a European country affected by this threat and how this affects NATO's integrity. Chapter One examines the case of Kosovo, its history, and how Russia used tensions between Kosovar Serbs and Albanians to gain influence in the Western Balkans. It will also examine NATO's role in the conflict to better understand what could be done to improve the effectiveness of the current mission.

Chapter Two looks at the case of Ukraine by exploring the history of the Crimean conflict and why the conflict has not been resolved - to the favor of Russia. It considers the problem of ethnic identity within Ukraine and how Russia utilized this to their advantage. It also examines the current rift in the Orthodox Church which is intimately tied to the political rift between Russia and Ukraine and how Russia used religion to influence Ukraine.

Chapter Three looks at Bosnia and Herzegovina, examining its current position in the world and analyzing its role as a possible next conflict zone for Russia to exploit. It also explores how Russia exploits ethnic ties, especially with ethnic Serbs, to push its agenda in the Balkans. These examinations on ethnic and religious identity on the borders of NATO will assist the organization in its current missions and help identify future problem areas for the Alliance.

2.1 Kosovo

Nivedita Arvind (Coordinator)

2.1.1 Introduction

Kosovo has endured decades of religious and ethnic conflict, resulting in a series of international interventions starting in 1999. Kosovo was the center of the medieval Serbian Empire and is still considered by many ethnic Serbs to be the center of Serbian heritage and their Eastern Orthodox religion. However, following Kosovo's incorporation into the Ottoman Empire, the ethnic and religious composition shifted as Islam gained prominence and the population of ethnic Albanians increased. Although Kosovo was reintegrated into Serbia (and later into the Republic of Yugoslavia) in the 20th century, the regional demographics continued to shift to an Albanian majority with a Serbian minority, resulting in decades of religious violence.[90]

In 1974, Kosovo became an autonomous province of Serbia within the Federal People's Republic of Yugoslavia. As such, Kosovo was granted similar rights to the six constituent republics of Yugoslavia. However, it is important to emphasize that Kosovo was not a republic in and of itself but remained a part of Serbia. In 1981, ethnic and religious violence escalated when Kosovar Albanians demanded sovereignty. During this period, Slobodan Milosevic propelled himself to power by exploiting the fears of minority Kosovar Serbs and revoked autonomy of the province in 1989. His anti-Albanian propaganda during the 1990s instigated an armed resistance by the Kosovo Liberation Army (KLA) in 1997. In 1998, Milosevic unleashed a brutal police and military campaign against the KLA, which resulted in the ethnic cleansing of the Kosovar Albanians.[91] This triggered an international humanitarian crisis.[92]

On May 12th, 1998, NATO foreign ministers specified two major objectives in relation to the Kosovo issue: to help achieve a peaceful resolution of the crisis by contributing to the response of the international community and to promote stability and

[90] Malcolm, Noel. "Noel Malcolm: Is Kosovo Serbia? We Ask a Historian." The Guardian. February 26, 2008. Accessed March 04, 2019. https://www.theguardian.com/world/2008/feb/26/kosovo.serbia.
[91] "TIMELINE: Key Dates in Kosovo's Recent History." Reuters. February 17, 2008. Accessed March 04, 2019. https://www.reuters.com/article/us-serbia-kosovo-timeline/timeline-key-dates-in-kosovos-recent-history-idUSL3143246620080217.
[92] Kosovo Profile - Timeline." BBC News. January 17, 2018. Accessed February 11, 2019. https://www.bbc.com/news/world-europe-18331273.

security in neighboring countries with particular emphasis on Albania and the former Yugoslav Republic of Macedonia (now the Republic of North Macedonia). Following the failure of peaceful diplomatic measures on June 12th, 1998, a NATO defense ministers' meeting led to the assessment of military measures to control the escalating conflict in Kosovo. On October 13th, 1999, NATO authorized a military air-strike to pressure the Serbian government to cease fire in Kosovo.[93]

After Milosevic's failure to agree to the Rambouillet Accords, NATO initiated a military campaign to halt the violence in Kosovo. It consisted of aerial bombings to halt the violence and lasted from March - June 1998. Milosevic conceded 78 days later. The UN Security Council ratified Resolution 1244 which suspended Serbian governance of Kosovo, placed Kosovo under the administration of the United Nations Interim Administration Mission in Kosovo (UNMIK) and authorized a NATO peacekeeping force.[94] Resolution 1244 envisioned a political process designed to determine Kosovo's future status under an international regime.[95]

NATO's objectives in relation to the conflict in Kosovo were set out in the statement issued at the Extraordinary Meeting of the North Atlantic Council held at NATO on April 12, 1999 and were reaffirmed by heads of state and government in Washington on April 23, 1999. These objectives aimed to end all military action, to return all refugees and displaced persons, and to establish a political framework for Kosovo based on international law.[96] These objectives formed the framework for any future international intervention and were regarded by the alliance as a prerequisite to ending the violent conflict in Kosovo.

Following UNSCR 1244, NATO implemented a rapid deployment of a military force. As agreed in the Military Technical Agreement, the deployment of the Kosovo security force, KFOR, was coordinated with the departure of Serb security forces from Kosovo. By June 20th, the Serb withdrawal was complete and KFOR was well established in Kosovo. KFOR is a multi-national security force unified and commanded

[93] NATO "The Situation in and around Kosovo - Statement Issued at the Extraordinary Ministerial Meeting of the North Atlantic Council..." NATO. Accessed February 10, 2019. https://www.nato.int/cps/en/natohq/official_texts_27435.htm?selectedLocale=en.
[94] Resolution 1244. Accessed March 05, 2019. http://www.unmikonline.org/Pages/1244.aspx.
[95] Security Council Resolution 1244." Security Council Report. June 10, 1999. http://www.securitycouncilreport.org/atf/cf/{65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9}/kos SRES 1244.pdf
[96] NATO. "The Situation in and around Kosovo - Statement Issued at the Extraordinary Ministerial Meeting of the North Atlantic Council..." NATO. Accessed February 10, 2019. https://www.nato.int/cps/en/natohq/official_texts_27435.htm?selectedLocale=en.

by NATO members and partners. The KFOR is a peace enforcement operation authorized by the UN and provided by NATO to "deter renewed hostility and threats against Kosovo by Yugoslav and Serb forces; establish a secure environment and ensure public safety and order; demilitarize the Kosovo Liberation Army; support the international humanitarian effort; and coordinate with and support the international civil presence.[97]" This effort was crucial in maintaining peace and stability but KFOR has limits on its overall capacity. It is purely a security operation and has no mandate for political interference. Instead, NATO complements other international organizations in re-building Kosovo. Initially, the lead party in Kosovo was UNMIK, the official United Nations mandated mission that was given executive power over Kosovo. This task was "unprecedented in complexity and scope; the Council vested UNMIK with authority over the territory and people of Kosovo, including all legislative and executive powers and administration of the judiciary[98]." In addition to formal institutions, there is also the Contact Group, an informal grouping of states that monitors and supervises international policy and development in Kosovo. This group consists of the U.S, U.K, France, Germany, Italy, and Russia. Following Serbia's withdrawal from Kosovo, the contact group established the "guiding principles"[99] in 2005 for the resolution of Kosovo's future status. Some important principles included no changing of the borders of Kosovo, no return to the status before 1999, and no partition or union with neighboring states. The presence and leadership from these organizations helps stabilize and de-escalate tensions among Kosovars.

On May 20th, 2008, Kosovo declared independence from Serbia. Following this, the UNMIK mission was reduced in scope to only include the promotion of security, stability, and respect for human rights in Kosovo.[100] Immediately, Kosovo's declared independence caused further unrest and instability in the Balkan region. Serbia and Russia failed to recognize Kosovo as a sovereign state while the U.S. backed the Kosovar Albanians to create a democratic institution. Kosovo today is still not a fully recognized state and lacks representation in international institutions.

[97] Nato. "NATO's Role in Kosovo." NATO. Accessed February 10, 2019. https://www.nato.int/cps/en/natolive/topics_48818.htm.
[98] "UNMIK." UNMIK. Accessed February 21, 2019. https://unmik.unmissions.org/.
[99] "Guiding Principles of the Contact Group for a Settlement of the Status of Kosovo." Kosovo Contact Group. Guiding principles of the Contact Group for a settlement of the status of Kosovo.
[100] ibid

2.1.2 Reactions to Kosovo's Independence

Following Yugoslavia's fall, the various republics sought to affirm and develop their own national identities. Other Balkan states could leave the Republic, but Kosovo presented a complex issue. Not only was it considered the epicenter of Serbian identity, but it was also a province instead of a republic. Since Kosovo was part of Serbia during the collapse of Yugoslavia, most Serbs consider Kosovo as Serbian territory.
In response to Kosovo's independence, Russia stood by the Serbs. One reason for Russian loyalty is their shared Slavic identity and Russia's commitment to protect all Slavs. Serbia is one of Russia's greatest partners due to their shared culture, ethnicity, and ideologies. After Kosovo declared independence in 2008, the Russian Foreign Ministry stated that the move was illegal. The Ministry declared, "Kosovo's provisional institutions of self-government declared a unilateral proclamation of independence of the province, thus violating the sovereignty of the Republic of Serbia, the Charter of the United Nations, UNSCR 1244, the principles of the Helsinki Final Act, Kosovo's Constitutional Framework and the high-level Contact Group accords".[101] Russia demanded the UN re-examine Kosovo's case and restore territorial integrity to Serbia. Russia's Foreign Ministry also backed the Kosovar Serb minorities, blamed the Kosovo government for reigniting ethnic and religious tensions, and urged the international community to prevent further escalation of the conflict. As a result of this partnership, many Serbs see Russia as their friend and protector. However, Russia's actions are not always altruistic. As of late, Russia has been utilizing this region in hopes of reasserting its position as a superpower. By increasing tensions among Kosovar Serbs and Albanians, Russia can gain leverage over Serbia while impeding the U.S.'s influence in the Western Balkans.

Apart from Russia, seventy-nine countries do not recognize Kosovo as a sovereign state for varying reasons.[102] Certain European states do not recognize Kosovo as a result of internal separatist issues. One such example is the issue between

[101] Commission Staff Working Document: Serbia 2007 Progress Report." Commission Of The European Communities Sec(2007), no. 1435 (November 6, 2007). https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2007/nov/serbia_progress_reports_en.pdf
[102] "Countries That Have Recognized Kosovo As An Independent State." Be In Kosovo. Accessed February 21, 2019. http://www.beinkosovo.com/countries-that-have-recognized-kosovo-as-an-independent-state/.

Catalonia and Spain. Catalonia is one of Spain's most wealthy and productive regions, having a history dating back almost a millennium. Following the civil war in 1978, Catalonia was granted autonomy under Spain. In 2006, the region was granted even more autonomy under new statues and was considered a "nation." Two years later, following the economic crises, separatist tensions ignited in a prosperous Catalonia. Subsequently, in 2010, Spain's Constitutional Court reversed much of Catalonia's autonomy. Similarly, other states such as China and Romania do not recognize Kosovo due to the fear of igniting internal separatist movements.[103] The indecisiveness on Kosovo's status creates problems among many international institutions such as NATO and the EU. These institutions must be cautious that the debate concerning Kosovo does not weaken their resolve. This would allow Russia to exacerbate the Kosovo debate to Russia's advantage.

2.1.3 Threats from Russia

Russian military and political experts have stressed the importance of an approach that influences the population of target countries through information operations, proxy groups, and other influence operations. The Commander of the U.S.-European Command (and SHAPE NATO) General Scaparrotti said, "Russia already is a competitor that operates in domains particularly below the level of war, by using malicious cyber activity, social media, disinformation campaigns, and troop exercises to threaten and bully other countries".[104] These tactics of destabilization can be seen in pro-Western states that are a part of Russia's "near abroad."

NATO has been actively engaged in maintaining peace and stability in the region since 1999. Yet, their activity comes at a cost as NATO's enlargement impedes Russia's relationship with the West. Russia claims that NATO and EU expansion puts Russia's territorial integrity, spheres of influence and national sovereignty at risk.[105] Further harming the relationship is NATO's involvement in Kosovo, which directly

[103] "Catalonia's Bid for Independence from Spain Explained." BBC News. January 31, 2018. Accessed February 14, 2019. https://www.bbc.com/news/world-europe-29478415.
[104] Kitfield, James, and James Kitfield. "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti." Breaking Defense. October 02, 2018. Accessed February 10, 2019. https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter-russians-gen-scaparrotti/.
[105] J. L. Black, "Russia and NATO Expansion Eastward: Red-Lining the Baltic States." International Journal 54, no. 2 (1999): 249-66. doi:10.2307/40203375.

threatens Russia's mission to regain former spheres of influence.[106] NATO's integral presence in Balkan security (especially in Kosovo) combined with their perceived involvement in Russian domestic affairs increases hostility and feeds into the Russian dogma.

To complicate matters, Serbs continue to express their loyalty to Russia over the West. In a survey taken in 2014, 70% of the citizens of Serbia chose to align with Russia while 30% voted for EU accession.[107] Therefore they "decidedly support close relations with Russia instead of joining the EU".[108] Serbia's view of state foreign policy aligns more closely with that of Russia than Western consensus. Secondly, Russia is offering important support for military and economic operations for countries that are not a part of the EU and other Western institutions.

Serbia has always contradicted the Western positions on sovereignty, especially on the Kosovo issue. They argue that Kosovo is an integral part of its territory and a symbol of national identity, hence reiterating Kosovo's territorial integrity as being inherently Serbian[109]. This contrasts with the EU where 23 out of 28 member states and 24 out of 28 NATO member states have recognized Kosovo's independence.[110] Russia, on the other hand, has strongly supported Serbia on Kosovo. The Russian Foreign Ministry released a statement in 2008 saying that the legitimization of Kosovo's independence would destabilize the Balkans and the international order. Thus, by supporting the minority Kosovar Serbs, the Russian-Serbian relationship is further consolidated. Russia has also demonized the West by accusing them of destabilizing and disrespecting non-Western ideas and abandoning principles of international law. [111] Russia utilizes pro-Serbian policies, especially in Serb minority neighboring countries such as Bosnia and Herzegovina, Montenegro, and Kosovo. This has been a large

[106] Zofia Studzińska, "How Russia, Step by Step, Wants to Regain an Imperial Role in the Global and European Security System." Connections 14, no. 4 (2015): 21-42. http://www.jstor.org/stable/26326416.
[107] "Serbia Caught between Two Chairs? Does Serbia Want to Be Part of the Russian Sphere of Influence or Join the European Union?" Heinrich Böll Stiftung Serbia, Montenegro, Kosovo. Accessed February 11, 2019. https://rs.boell.org/en/2014/12/10/serbia-caught-between-two-chairs-does-serbia-want-be-part-russian-sphere-influence-or.
[108] "COMMISSION STAFF WORKING DOCUMENT: SERBIA 2007 PROGRESS REPORT." COMMISSION OF THE EUROPEAN COMMUNITIES SEC(2007), no. 1435 (November 6, 2007). https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2007/nov/serbia_progress_reports_en.pdf
[109] Why Is Kosovo so Important for Serbs. Accessed February 13, 2019. http://www.ptt.rs/korisnici/i/v/ivstar/quickhistory.htm.
[110] Ramani, Samuel. "Why Serbia Is Strengthening Its Alliance with Russia." The Huffington Post. February 12, 2017. Accessed February 11, 2019. https://www.huffingtonpost.com/samuel-ramani/why-russia-is-tightening-_b_9218306.html.
[111] COMMISSION STAFF WORKING DOCUMENT: SERBIA 2007 PROGRESS REPORT." COMMISSION OF THE EUROPEAN COMMUNITIES SEC(2007), no. 1435 (November 6, 2007). https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2007/nov/serbia_progress_reports_en.pdf

focus of Russia's use of hybrid warfare to destabilize the Balkans and prevent Trans-Atlantic alliances with Serbia.

The Western Balkans is of importance to Russia for two reasons. First, it is a region of increased visibility due to Western intervention. Second, it is a key region for the control of energy supply routes to the EU, thus making this area integral to strengthen Russia's dominance in the energy sector. In 2008, Russian gas conglomerate Gazprom took control of Serbian fuel company NIS. This gave them full control over the Serbian oil processing sector and a strong position in gas distribution channels. This deal allowed Moscow to send more natural gas to Europe through its South Stream pipeline. This deal hindered the EU's Nabucco pipeline project to build a 2000-mile-long pipeline to bring gas to Europe from Iran and Azerbaijan via Turkey[112]. This pipeline was conceived to reduce the EU's energy dependence on Russia. Analysts blamed the EU's inability to promptly resolve the Kosovo issue with Serbia as a key reason for Russia's increased dominance in the energy sector. Today, the Russian company Gazprom owns 56.15 % of the share capital of NIS.[113]

Russia exerts large amounts of political and economic pressure on Serbia to maintain crucial ties to the Balkans. Russian owned companies and subsidiaries amount to 13% of the total revenues generated by the national economy. Serbia is almost fully dependent on Russia for natural gas imports. This issue is seemingly unresolvable as political intermediaries prevent supply diversification and market liberalization. Russia is also a large accumulator of Serbian debt for gas. Serbian domestic companies are highly dependent on exports to Russia and loans such as the Agrokor's subsidiaries.[114] Additionally, Russia has used direct government-government loan schemes to enhance its presence in the Serbian economy.[115] Finally, Russia has compounded its economic clout in Serbia by utilizing soft power to schemes to leverage pro-Russian principles using pan-Slavic propaganda and pan-orthodox values.

[112] Dempsey, Judy. "Russia's Gazprom Takes Control of Serbian Oil Monopoly." The New York Times. January 23, 2008. Accessed February 10, 2019. https://www.nytimes.com/2008/01/23/world/europe/23serbia.html.
[113] "About." NIS. Accessed February 10, 2019. https://www.nis.eu/en/about-us/our-business/energy.
[114] Russian Economic Footprint in Serbia Policy Brief No. 72." Center for the Study of Democracy 72 (2018). doi:10.6027/anp2018-832.
[115] "Russian Economic Footprint in Serbia Policy Brief No. 72." Center for the Study of Democracy 72 (2018). doi:10.6027/anp2018-832.

Similarly, Russia has followed similar principles in countries like Bosnia and Herzegovina to maintain instability in the Balkans and to counter EU expansion.

EU Presence in Kosovo: EULEX

UNMIK was the official mandated mission by the United Nations following the ratification of UNSCR 1244. UNMIK had authority over all territory and people, including the legislative, judicial and executive bodies of the government. However, it was ineffective in achieving its goals. For example, the justice system created by UNMIK in Kosovo proved to be unsuccessful due to inherent biases amongst the judicial officials.[116] Additionally, high levels of corruption present in Kosovo's government resulted from UNMIK's failure to establish an effective operational framework.[117] Currently, UNMIK's day-to-day operations are relatively minor following Kosovo's declaration of independence in 2008. UNMIK handed over most of its functions to the Kosovar parliament and the EU's rule of law mission (EULEX) in Kosovo.[118] The European Union has played an active role in Kosovo since 1999 and Kosovo has aligned itself with the European Union over Russia. However, Kosovo is unable to petition for membership due to its officially unrecognized status. The EU is active in Kosovo through its Special Representative (EUSR), and the European Security and Defense Policy (ESDP) mission in the Kosovo rule of law area (EULEX). The EULEX office in Kosovo plays a key role in implementing the EU agenda internally by promoting European norms. The office also ensures permanent political and technical dialogues between the EU and Kosovo. [119]

[116] "Has the UN's Kosovo Mission Become Obsolete?" Balkan Insight. January 15, 2019. Accessed February 28, 2019. https://balkaninsight.com/2018/12/18/has-the-un-s-kosovo-mission-become-obsolete-12-17-2018/.
[117] Beha, Adem, and Gëzim Selaci. "Statebuilding without Exit Strategy in Kosovo: Stability, Clientelism, and Corruption.
[118]"Has the UN's Kosovo Mission Become Obsolete?" Balkan Insight. January 15, 2019. Accessed February 28, 2019. https://balkaninsight.com/2018/12/18/has-the-un-s-kosovo-mission-become-obsolete-12-17-2018/.
[119] "Kosovo* and the EU - EEAS - European External Action Service - European Commission." EEAS - European External Action Service. November 02, 2019. Accessed February 11, 2019. https://eeas.europa.eu/delegations/kosovo_en/1387/Kosovo and the EU.

The ESDP/EULEX project is of key importance in promoting security and stability in Kosovo. The EULEX helps assist the Kosovar authorities in the rule of law, the police, judiciary, and customs. ”EULEX is a technical mission that mentors, monitors and advises while retaining a number of limited executive powers.”[120]

Arrested people	2012	2013	2014	2015
Human trafficking	121	91	66	48
Enabling prostitution	39	35	35	37
Prostitution	61	26	49	70
Other acts	7	30	11	23
TOTAL	228	182	161	178

Table 7- Statistics of the arrested people 2012-2015

Kosovo 2018 report, main areas: (European Commission)

	Progress	Level of preparation
Judiciary	Some	Early
Fight Against Corruption	Some	Early
Organised Crime	Some	Early
Economic Criteria	Good	Early
Freedom of Expression	Some	Some
Public administration	Some	Some

There have been several critiques of the EULEX in meeting its mission to bring about peace and stability. Kosovo is the hub for organized crime reaching the EU[121] and it faces high levels of unemployment and other economic factors encourage criminal activity. Kosovo is also used as an ally to smuggle drugs into the EU. Human trafficking is another major humanitarian crisis that has plagued Kosovo which acts as a hub to enable trafficking into the EU. Although the EULEX has succeeded in prosecuting criminals, it has failed in arresting high ranking Kosovar officials on charges of organized crime.[122] The EULEX justified its position by stating their official view is to establish the rule of law rather than work on policing issues.[123]

2.1.4: Recent Security Concerns:

In December 2018, the Kosovar parliament voted to create its own army despite criticisms raised by Serbia, NATO, and the EU. Kosovo vowed that it would still be able to unilaterally protect its Kosovar Serbian population. All 107 lawmakers present in

[120] Pio. "About EULEX." EULEX Report to the UN - EULEX Kosovo. Accessed February 11, 2019. https://www.eulex-kosovo.eu/?page=2,60.
[121] Burghardt, Tom. "Kosovo: Europe's Mafia State. Hub of the EU-NATO Drug Trail." Global Research. December 22, 2010. Accessed February 21, 2019. https://www.globalresearch.ca/kosovo-europe-s-mafia-state-hub-of-the-eu-nato-drug-trail/22486.
[122] Bytyci, Fatos. "EU Justice Mission Leaves Kosovo, Accused of failing Its Mandate." Reuters. June 14, 2018. Accessed February 11, 2019. https://www.reuters.com/article/us-kosovo-eu-justice/eu-justice-mission-leaves-kosovo-accused-of-failing-its-mandate-idUSKBN1JA1WH.
[123] ibid

Kosovo's 120-seat Parliament (dominated by ethnic Albanian parties) voted to "back the government's plan to transform the 3,000-strong, lightly armed Kosovo Security Force into an army that would grow to 5,000 active troops and 3,000 reservists in the next decade".[124] The KSF vote is also significant as none of the Serbian representatives in the Kosovar parliament voted. The Kosovo Security Force is the successor of the Kosovo Protection Corps, which was created after the demilitarization of the Kosovo Liberation Army (KLA). The KLA has a long history of alleged criminal activity, former KLA members are still summoned to the Special War Crimes Prosecutor's Office in the Hague.[125]

The EU, NATO and the UN have created various multilateral mechanisms to prevent volatile situations in the Balkans. Since 1999, KFOR has been the only armed force allowed to operate in Kosovo based on UNSCR 1244. Its troops disbanded the KLA, the guerilla Albanian force that fought the Serbian Army during the war. Secretary-General of NATO, Jens Stoltenberg, expressed his concerns over this decision by stating that he regrets "that this decision was made despite the concerns expressed by NATO… while the transition of the Kosovo Security Force is in principle a matter for Kosovo to decide, we have made clear that this move is ill-timed".[126] He also stated that NATO's highest decision-making body will re-examine its participation in Kosovo. Currently, Kosovo's decision to remilitarize the state despite the loss of NATO's support is a substantial threat to Balkan security.

Since the formation of the Kosovo security force, the EU has become an important factor in maintaining peace and stability in Kosovo. The US has backed Kosovo's creation of an army, although the executive body of NATO opposes this endeavor. In 2018, KFOR participated in a "quick response"[127] exercise in Bosnia and Herzegovina led by the European Union security force to enhance mutual cooperation

[124] Surk, Barbara. "Kosovo Parliament Votes to Create an Army, Defying Serbia and NATO." The New York Times. December 14, 2018. Accessed February 11, 2019. https://www.nytimes.com/2018/12/14/world/europe/kosovo-army-serbia-nato.html.
[125] Telegraf.rs. "From KLA, over the Kosovo Protection Corps, Kosovo Security Force, and Then to "army": Development of Terrorism on Kosovo." Telegraf - Najnovije Vesti. December 14, 2018. Accessed February 11, 2019. https://www.telegraf.rs/english/3015810-from-kla-over-the-kosovo-protection-corps-kosovo-security-force-and-then-to-army-development-of-terrorism-on-kosovo.
[126] Nato. "Statement by the NATO Secretary General on the Adoption of the Laws on the Transition of the Kosovo Security Force." NATO. Accessed February 11, 2019. https://www.nato.int/cps/en/natohq/news_161631.ht m?selectedLocale=en.
[127] Nato. ""Enduring Commitment" for the Stability of the Western Balkans Area." NATO KFOR - Conflict Background. Accessed February 26, 2019. https://jfcnaples.nato.int/kfor/media-center/archive/news/2018/enduring-commitment-for-the-stability-of-the-western-balkans-area.

amongst international security organizations. The Quick Response 2018 exercise in Bosnia gave KFOR the opportunity to test its capability to intervene outside Kosovo when necessary in order to support the wider stability of the Western Balkans.[128] The EULEX mandate in June 2018 was tailored to "to assist the Kosovar authorities in establishing a sustainable and independent rule of law institutions." [129] NATO must influence its members to deploy ESDP assistance to control and stabilize Kosovo as it still sees high levels of corruption, especially in the executive body of its government. NATO should suggest that the ESDP improve its capacity in the region, including EULEX. NATO should adopt an enhanced military response mechanism such as the formation of a NATO Headquarters in the Western Balkans to control the situation and enhance regional stability in the Balkans.

[128] ibid
[129] Pio. "EULEX NEW MANDATE." EULEX Report to the UN - EULEX Kosovo. Accessed February 26, 2019. https://www.eulex-kosovo.eu/?page=2,10,836.

2.2 Lessons from Ukraine

Alex Buzzell

2.2.1 Introduction

Since the ending of the Cold War in 1991, many scholars argued this era ushered in a unipolar world with the United States as the sole superpower. In the intervening decades with the rise of China and the resurgence of the Russian state, modern scholars argue that the world has shifted into a multipolar world. Richard Haas has argued against this hypothesis, claiming that the world was in fact in a “non-polar” world.[130] This hypothesis stems from the observation that the multipolar world of today is much different than that of the multipolar world of pre-WWII. Today the traditional poles of the state are challenged from regional and multinational organizations from above, from the side by NGOs, and from below from terrorists and militias.[131] The Ukraine Crisis was a product of this newly less stable world. According to Izhak, Russia utilized the weakness of this system to assert itself as a pole of influence.[132] The furthering of this multipolar or nonpolar world is an important part of the Russian foreign policy goals.

In early 2013 before the Ukraine crisis began, the head of the Russian General Staff published an article describing the new form of warfare that must be waged in the modern era. He described a warfare that includes a combination of non-military measures alongside utilizing protests led by the people. These weren’t tactics devised solely by Russia but in fact are the lessons learned from the “color revolutions” that diminished Russian influence in their former satellite states. Interestingly, nine months later these ideas would be put to the test in Ukraine.[133] In 2013 the crisis in Ukraine began with the protests that destabilized the country. The Euromaidan protests in Kiev were in the wake of this instability, and Russia embarked on an operation to retain its influence in the country by any means necessary. This campaign ended with the

[130] Richard N. Haas "The Age of Nonpolarity." Foreign Affairs. 2008. Accessed February 10, 2019. https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity.
[131] Oleksii Izhak. "The Threats and Challenges of a Multipolar World: A Ukraine Crisis Case Study." *Connections 15, no. 1* (2016): 32-44. http://www.jstor.org.offcampus.lib.washington.edu/stable/26326427.
[132] Ibid. 39.
[133] Valery Gerasimov. "The Value of Science Is Prediction. New Threats Demand Rethinking the Ways and Means of Conducting Warfare." Voenno-promyshlenniy Kurier, February 27, 2013. Accessed February 10, 2019. http://www.vpk-new.ru/articles/14632.

Russian annexation of the recognized Ukrainian territory of Crimea as well as the creation of another frozen conflict zone in the east of Ukraine. These territorial issues then effectively stopped Ukraine's bid for EU membership.[134]

2.2.2 The Role of Ethnicity

Ukraine has a unique history, especially regarding its relationship with Russia. Since the domination of independent Ukrainian states in the 14th c. the land of Ukraine has been partitioned and separated or under outside rule until 1991. This long absence of independence has led many in Russia not to see Ukraine as a separate state but as an important client state, much like Belarus. This extends into the shared history of Russia and Ukraine as well. Russia traces its origin to the Kievan Rus', who were Slavic peoples who lived from modern Ukraine to Finland. Both Russia and Belarus are named after the Rus', and Ukraine derives its name from its position in relation to the Rus' as Ukraine means borderland. This historical interconnectedness makes the disentanglement of identity extremely difficult, and more so for the Russophones living in Ukraine. The role of ethnicity cannot be disregarded in its role within hybrid warfare utilized by Russia. The Russian state utilized in 2014 an organized propaganda war for the hearts and minds of those in Crimea and eastern Ukraine. A combination of propaganda in the majorly Russian speaking areas dominated by Russian media alongside nongovernmental organizations created the conditions necessary for Russia to be able to fully influence the views of the people of these areas. It is important to note the extent that Russia went in demonizing the new Ukrainian government, painting it as a fascist junta or undemocratic Western puppet- the sort of vitriol only matched by Slobodan Milosevic, Saddam Hussein, or Kim Jong-un in the West.[135] With an intense opposition to the new government in place in the key areas, demonstrations broke out. In the examples of Ukraine, South Ossetia, and Abkhazia, Russia has used what they view as Russian population to justify its meddling in the affairs of sovereign states.

Zhurzhenko posits an important point on the strength of Ukrainian national identity, asserting that especially in the border regions of Ukraine, the national identity of

[134] Michael Ray. "Ukraine Crisis." Encyclopædia Britannica. May 26, 2017. Accessed February 01, 2019. https://www.britannica.com/topic/Ukraine-crisis.
[135] Oleksii Izhak. 36.

the state created in 1991 was not developed strongly enough.[136] She suggests that the weakness of the Ukrainian identity was the key to Russian influence in the area. In the post-Soviet time, the different political leaders walked a fine line between nationalist and pro-Russian/Soviet attitudes to placate two major camps of thought within Ukraine. After the Orange Revolution, President Victor Yushchenko framed Ukraine as a post-colonial nation, still under Russian political and cultural influences and aimed to free Ukraine of them.[137] This set the stage for the nationalist and pro-Soviet clashes over how to understand Ukraine's history, which formed a major part of the political conflicts going forward. This came to a head after the decision to postpone the signing of the EU-Ukraine Association Agreement, leading many pro-EU Ukrainians to protest seeing it as a victory for Russia that they aimed to distance themselves from. In the east and south, Russian media portrayed these events as an outpouring of Ukrainian nationalism and a pro-fascist putsch.[138] Russia set the groundwork for the events of 2014 almost immediately after the Orange Revolution which shocked the Kremlin out of its post-Soviet assurance of its absolute influence in the former Soviet space. This led to the adaptation of perceived Western tactics of the color revolutions, such as using grassroots youth organizations to organize hacking attacks or to damage state monuments.

Another prong against Ukraine came in the form of the ideology of *Russkiy mir*, or Russian World, that posits that Russian speakers and Orthodox Christians are part of a larger Russian diaspora and historically have much deeper ties than recent borders.[139] These ideas were sent into Ukraine through state sponsored sources and through soft power initiatives such as literature and TV series which exported the idea of Russian greatness to many Ukrainians. Another dimension to this soft power imitative to win over Ukraine was the appeal to conservative values regarding the family and sexuality, especially focusing on the idea of European sexual deviancy and the destruction of gender norms.[140] But after the Crimean Crisis overall perceptions

[136] Tatiana Zhurzhenko. "A Divided Nation? Reconsidering the Role of Identity Politics in the Ukraine Crisis." *Die Friedens-Warte 89, no. 1/2* (2014): 249-67. http://www.jstor.org.offcampus.lib.washington.edu/stable/24868495.
[137] Tatiana Zhurzhenko. 254.
[138] Ibid. 256.
[139] Ibid. 259.
[140] Ibid. 259.

between the countries have declined rapidly. As De Maio points out, the Russian media has painted the Ukrainians in an intensely negative light leading to a very hostile relationship.[141]

2.2.3 The Role of Religion

Russia has used the shared majority religion of Orthodox Christianity as a tool against Ukraine, as many Ukrainian churches were under the auspices of the Moscow Patriarchate. As of January 2019, the Ecumenical Patriarch granted the Orthodox Church of Ukraine Autocephaly, or ecclesiastical autonomy, formalizing the rift that began late 2018. This religious division is further proof of the growing divide between the historically close nations and will have major repercussions in the long term. As recently as January 31st of 2019 Putin has lambasted the Ukrainian government for interfering with the Orthodox Church and compared them to church persecutors of the past century.[142] The official Russian narrative of this split is that the Ukrainian church already had independence under the Russian Orthodox Church and the split is merely a political tool used by Poroshenko to boost his popularity before the upcoming election. As the spiritual center of Orthodox Christianity, the Ecumenical Patriarchate of Constantinople plays a major role in this conflict. According to their own published research on the history and ecumenical law, the Patriarchate has ruled that it had full authority over the status of the Ukrainian Orthodox Church.[143] This ruling set the groundwork for the granting of autocephaly to the Ukrainian Orthodox Church, essentially making it independent of Moscow and directly under the rule of the Ecumenical Patriarchate.[144] This move both united and separated the Orthodox community of Ukraine, as it unified previously split away churches that were formed outside of Moscow's Patriarchate and created a new split in its wake with the Ukrainian churches that wished to stay under the Moscow Patriarchate. This split creates new

[141] Giovanna De Maio. Report. Istituto Affari Internazionali (IAI), 2016. http://www.jstor.org.offcampus.lib.washington.edu/stable/resrep09810.
[142] Rfe/rl, Russian Service, and Rfe/rl. "Putin Blasts Kyiv For 'Blatant Interference' In Orthodox Church." RadioFreeEurope/RadioLiberty. January 31, 2019. Accessed February 01, 2019. https://www.rferl.org/a/putin-blasts-kyiv-for-blatant-interference-in-orthodox-church/29744338.html.
[143] "The Ecumenical Throne and the Church of Ukraine." The Ecumenical Patriarchate. September 18, 2018. Accessed February 11, 2019. https://www.patriarchate.org/theological-and-other-studies/-/asset_publisher/GovONi6kIiut/content/o-oikoumenikos-thronos-kai-e-ekklesia-tes-oukranias-omiloun-ta-keimena?_101_INSTANCE_GovONi6kIiut_languageId=en_US.
[144] Carlotta Gall. "Ukrainian Orthodox Christians Formally Break From Russia." The New York Times. January 06, 2019. Accessed February 11, 2019. https://www.nytimes.com/2019/01/06/world/europe/orthodox-church-ukraine-russia.html.

tensions within Ukrainian society. One could be viewed as a Russian supporter if you attend a Moscow church, or you could be seen as an opportunist or Western stooge if you go to a Kiev church. Another criticism coming from Russia is aimed at the Ecumenical Patriarchate, which the Russian Orthodox Church has broken relations with over the Ukrainian issue, concerning the inner politics of the Orthodox church. These issues stem from the alleged handover of all overseas churches in the Ukrainian name over to the Ecumenical Patriarchate, this claim is not corroborated in any reports but remains an important Russian narrative especially within Russian leaning Ukrainians. The Orthodox church worldwide is split on this issue, and it is clear that many do not want to recognize the autocephaly of the Orthodox Church of Ukraine as that would anger the Russian Church which is the largest and most influential church within Orthodoxy.

The influence of the Russian Church cannot be ignored in this matter, due to its massive size and importance, consisting of half of the entire population of Orthodox Christians in the world today. As the church does not conduct official records of church goers this number could be exaggerated to include everyone who considers themselves an Orthodox Christian in Russia, not just those who hold strictly religious beliefs. Even so, the Russian Church is still the most well-funded and physically large churches in the Orthodox faith, and its influence within the Orthodox world cannot be denied. This is a problem for the Ecumenical Patriarch and the Ukrainian Church as an ongoing disagreement within the church may have far reaching consequences for the Orthodox faith, even possibly leading to schism- which is something that every side claims to want to avoid at all costs.[145] As this complicated relationship is still unfolding, it is unclear where it may lead. The only thing that is certain is that a conclusion will not be reached in the near future. Recent events indicate this will not be a clear and effective path for Russian influence.

.

[145] Andrew Higgins. "As Ukraine and Russia Battle Over Orthodoxy, Schism Looms." The New York Times. December 31, 2018. Accessed February 11, 2019. https://www.nytimes.com/2018/12/31/world/europe/ukraine-russia-orthodox-church-schism.html.

Conclusions 2.2.4

The lessons of what happened in Ukraine with the stirring of unrest and assistance of rebel groups provides a stark check on the capability of NATO and the West. Although Ukraine was not and is still not a NATO member, it has been an extremely important partner in eastern Europe, joining the North Atlantic Cooperation Council in 1991 and the Partnership for Peace in 1994, as well as placing full membership in NATO as a domestically important foreign policy goal.[146] This significant cooperation between NATO and Ukraine signifies the important strategic importance Ukraine has, but also the willingness of Ukraine to commit to deepening the relations between the alliance and themselves. Alongside this, NATO has implemented significant programs to assist Ukraine before and especially after the crisis of 2013/14. These areas of cooperation include peace-support operations, military-to-military cooperation, defense technology, interoperability and industry, civil preparedness, science and environment, and public diplomacy.[147] An important piece to this cooperation is the Comprehensive Assistance Package, approved in 2016, it aims to help Ukraine strengthen its defenses by building stronger security structures.[148] All of these components are integral to NATO-Ukraine cooperation in the wake of the 2014 crisis which led to the annexation and breakaway territory which is unchanged to this day. These events were not taken lightly by NATO members, they condemned the annexation and the military intervention in the strongest terms by deeming them fully illegal and illegitimate actions within the international community.[149] As a result of the lack of NATO membership for Ukraine no wider spread conflict erupted, but internationally recognized territory had changed hands without the consent of both nations. Despite years of punishing sanctions from the international community to compel Russia to reverse its actions, it has not made any moves to change course. In fact, with the building of the Kerch Strait bridge and confrontation over Ukrainian access to the Sea of Azov, it can be argued the situation has only gotten worse. The implementation of martial law in the vulnerable provinces of Ukraine is November of

[146] "Relations with Ukraine." NATO. June 14, 2018. Accessed February 11, 2019. https://www.nato.int/cps/en/natolive/topics_37750.htm.
[147] "Relations with Ukraine." NATO.
[148] Ibid. NATO.
[149] Ibid. NATO.

2018 in response to the naval confrontation as well as the mass movement of Russian troops along Ukraine's border, alongside the President of Ukraine decreeing that attack from Russia could be imminent at the time, this situation is anything but settled.[150] With the increase of tensions that the Orthodox split has caused only has furthered the political and military tensions between the two countries.

As NATO moves forward, it needs to be conscious of what led to the current situation, being aware of the limits of partnership and how this may have hurt or aided the alliance. As Russia would most likely not want to confront the entire alliance, Ukraine being made a NATO member would have most likely avoided this situation entirely. But it has to be noted that a defined step by Ukraine towards the West through the EU was one of the catalysts that set Russia on the current path. But an earlier admission of Ukraine into NATO may have been too early for Russia to have been able to easily influence any pro-Russian Ukrainians to destabilize the country in any effective way. The lesson of Ukraine comes from NATO recognizing the importance of national ethnic minorities and religious sects and their role within hybrid warfare engaged by Russia. The ethnic Russian and Russophone majority populations in Crimea and eastern Ukraine were instrumental in the Russian annexation and intervention of these areas. The effectiveness of Russian propaganda in Russian over the Ukrainian narrative was instrumental during the pivotal period of the Euromaidan in Kiev. NATO can learn from the tactics used by Russia and take preventive action to prevent future conflict occurring.

Ukraine is an important case study in how hybrid warfare is being used today, especially in the context of ethnicity and religion. Although NATO does not have direct authority over these issues, its analyzers of global trends and threats can take into account these important cultural identifiers to identify regions that are susceptible to Russian influence. NATO can put resources towards greater understanding of Russian and Ukrainian perspectives to better understand why people in each individual nation may support a certain policy. This could take shape in working together with organizations with more experience with religious and ethic affairs such as the EU or

[150] Andrew Osborn. "Ukraine Introduces Martial Law Citing Threat of Russian Invasion." Reuters. November 27, 2018. Accessed February 11, 2019. https://www.reuters.com/article/us-ukraine-crisis-russia/ukraine-introduces-martial-law-citing-threat-of-russian-invasion-idUSKCN1NV0N1.

NGOs such as the U.S. Ukraine Foundation. A particular understanding of the Orthodox Church would also be beneficial to understand another layer of politics that is playing underneath the high politics that is given the most attention. The changing day-to-day status of the Ukrainian-Russian Orthodox Church split is a very important story to follow for NATO to fully comprehend the situation in Eastern Europe. Although NATO cannot take any concrete policy steps in the sphere of religion, this knowledge can be used to craft more informed and significant policy in the ever-shifting political landscape of the region. Through studying Russian tactics NATO can update how it operates and build resiliency against any future hybrid war.

2.3 Bosnia and Herzegovina: The Next Ukraine?

Sarah Nichols (Editor)

2.3.1 Introduction

The history of Bosnia and Herzegovina (BiH)[151] is fraught with ethnic and religious antagonisms. While there is debate on the origin of these tensions, there is no doubt that people seeking power exploit this history for their own gain. To begin, it is important to understand the groups within the country. The term "Bosnians" refers to the citizens of Bosnia, regardless of their ethnic identity. Therefore, references to "Bosnians," "the Bosnian national military," or "Bosnian leaders" apply to BiH citizens. In a similar vein, while "Croatians" or "Serbians" are citizens of their respective countries, they can come from a multitude of ethnic backgrounds. A "Serb" or "Croat" on the other hand refer to one's ethnicity. Hence, there can be Croatian Serbs, Serbian Bosniaks, and many other combinations. Within Bosnia there are three main ethnic groups: Bosniaks, Croats, and Serbs. While all three groups are united by their Slavic roots, it is their differences that receive the most attention. Their religions further identify these groups: Bosniaks are mostly Muslim, Croats mostly Catholic, and Serbs mostly Orthodox Christian.

Further complicating matters is the disjointed structure of Bosnia and its government. This is a result of the Dayton Peace Accords and while the Accords did end the Bosnian War (1992-1995), it impeded the function of the country and solidified ethnic divisions. Two autonomous entities divide the country: the Serb-dominated Republika Srpska and the Bosniak-Croat-dominated Federation. Such segregation continues into the government, as Bosnia is led by an ineffective tripartite presidency with a Bosniak, Croat, and Serb president. These factors make Bosnia a vulnerable target for hybrid attacks. Malevolent actors can use these existing differences to generate distrust, animosity, and chaos in the country.

While military conflict has not broken out in Bosnia since the 1990s, it is important for NATO to continue to monitor the situation. As Secretary-General Jens

[151] Also referred to as "BiH" and "Bosnia."

Stoltenberg pointed out, “in the long run prevention is much better than intervention.[152]” Prevention of conflict is key in Bosnia as the country possesses many of the same risks as Ukraine including a separatist movement, growing ethnic nationalism, and rising paramilitarism. The following report will look at why Russia is interested in BiH, how it exerts its influence in the region, and how and why NATO should respond.

2.3.2 Russia’s Interests in Bosnia and Herzegovina

Although the former Yugoslav states did not participate in the Warsaw Pact, Russia still considers the region a part of its near abroad. In the earlier part of the century, Russia had limited interests in Bosnia and Herzegovina. However, with the most recent additions of Montenegro and North Macedonia[153] into NATO, Russia is especially keen to keep the remaining Balkan states out of the alliance’s reach. In 2014, when asked about the status of Bosnia, Montenegro, and Macedonia, Russian Foreign Minister Sergey Lavrov commented, “with regards to the expansion of NATO, I see it as a mistake, even a provocation in a way".[154] NATO officials should take heed of Lavrov’s use of the word *provocation* as it implies that the Alliance is “poking the bear.” As a result of the perceived Western threat, Russian influence in the Western Balkans has continued to grow as NATO adds more members. There have already been instances of Russian-backed chaos in the region. For example, the 2016 coup in the Montenegrin parliament was supported by the Kremlin, who wanted to stall the country’s accession.[155] Russia has also been accused of trying to sabotage the Macedonian name change referendum to keep the country out of NATO.[156] Having failed at stopping the accession of Montenegro and Macedonia, Russia will be looking to double down its efforts in Bosnia.

Unlike Serbia, which has vocally denounced joining NATO, Bosnian leaders have been keen to join the Alliance. In December 2018, Bosnia drew closer to this goal after

[152] Jens Stoltenberg, “Speech by NATO Secretary General at the Graduate Institute Geneva,” *NATO* March 3, 2017. https://www.nato.int/cps/en/natohq/opinions_141898.htm
[153] Hereafter referred to as Macedonia.
[154] Daria Sito-Sucic, "NATO's Planned Balkan Expansion a 'provocation': Russia's Lavrov." Reuters, September 29, 2014. https://www.reuters.com/article/us-nato-balkans-russia-idUSKCN0HO11W20140929.
[155] Reuf Bajrović, Vesko Garčević and Richard Kraemer, “Hanging By A Thread: Russia’s Strategy Of Destabilization In Montenegro,” Foreign Policy Research Institute, 2018, https://www.fpri.org/wp-content/uploads/2018/07/kraemer-rfp5.pdf.
[156] Nick Squires. “Russia 'Orchestrating Covert Campaign to Wreck Macedonia Name Change Vote' .” The Telegraph, Telegraph Media Group, 27 Sept. 2018, www.telegraph.co.uk/news/2018/09/27/russia-orchestrating-covert-campaign-wreck-macedonia-name-change/.

NATO activated Bosnia's Membership Action Plan (MAP), which brings the country closer to NATO membership. Consequently, Russia is strengthening its presence in Bosnia while persuading the country to stay out of the Alliance. Vladimir Putin, Lavrov, and a Russian envoy to BiH have all denounced the activation of Bosnia's MAP.[157] Both Lavrov and Putin have made several trips to Bosnia in the past year to reaffirm Russia's relationship with the country. In particular, the Kremlin is leaning hard onto its Bosnian Serb Orthodox brothers which provides a gateway into exerting control. Russian influence is strongest in Republika Srpska (RS), the autonomous Serb-dominated entity within BiH. Not only do Serbs share religious and cultural ties to Russia but Republika Srpska has molded itself into a pro-Russian entity. As Milorad Dodik has pointed out, the RS flag is simply the Russian flag upside down.[158]

Republika Srpska has cemented its relationship with Russia politically, militarily, and economically. The leading Serb party, SNSD, is Russian-leaning and Russia benefits from their anti-NATO sentiment. Particularly in RS, the animosity towards NATO is strong. In October 2017, the National Assembly of Republika Srpska approved a resolution which affirmed the entity's wish not to join NATO.[159] The Bosniak Vice President of RS expressed concern over the resolution stating, "The declaration is more dangerous than it seems. It underlined how Bosnian Serb leaders are acting at the instructions of a foreign power that wants to destabilize the Balkans in order to strengthen its foothold in Europe."[160]

In return for their loyalty, Russia supports RS leaders that promote anti-Western sentiments. The most prominent politician to receive such support is Milorad Dodik. The leader of SNSD, Dodik was President of Republika Srpska before being elected to the national tripartite presidency in October 2018. Lavrov and Putin have frequently met

[157] Cristina Maza. "Vladimir Putin Travels to the Balkans to Push against NATO Membership, Slams U.S. Interference." *Newsweek*, 17 Jan. 2019, www.newsweek.com/russia-vladimir-putin-travels-balkans-push-against-nato-membership-slams-us-1294734.; Eline Schaart. "Lavrov: Russia Keeps Door Open for Talks with US to Save INF Treaty." *POLITICO*, 16 Jan. 2019, www.politico.eu/article/nuclear-sergei-lavrov-russia-keeps-door-open-for-talks-with-united-states-to-save-inf-treaty; "Russia against Dragging Bosnia and Herzegovina into NATO, Says Russian UN Envoy." TASS., 6 Nov. 2018. http://tass.com/world/1029532.

[158] "Meeting with President Of Republika Srpska Entity Of Bosnia And Herzegovina Milorad Dodik." President Of Russia. September 30, 2018.
http://en.kremlin.ru/events/president/news/58662

[159] "At the 22nd Regular Session, the Resolution on the Protection of the Constitutional Order and the Proclamation of Military Neutrality Was Adopted." NSRS, 18 Oct. 2017, www.narodnaskupstinars.net/?q=en/news/22nd-regular-session-resolution-protection-constitutional-order-and-proclamation-military-neutrality-was-adopted.

[160] "Resolution Against NATO Membership By Bosnian Serbs." Bosnia & Herzegovina, www.oscebih.org/resolution-against-nato-membership-by-bosnian-serbs.

with Dodik, who in turn has used his Russian friends to secure support from Bosnian Serbs. Dodik's ties with Russia are strong- he received an accolade from the Russian Orthodox Church, watched a Formula One race in Sochi with Putin, and was promised $625 million in Russian loans.[161] No other politician in BiH has received the same warm embrace as Dodik has from Russia, and as long as he plays the Kremlin's game such rewards will continue. Since Dodik's election to the Bosnian Presidency, he has become armed with increased influence making him an even more powerful ally for the Kremlin. Possibly more alarming is the build-up of paramilitary forces in Republika Srpska supported by the Kremlin. Dodik has consistently stated his desire for Republika Srpska to secede from BiH, and the addition of paramilitary forces makes this option plausible. Such a situation is disturbingly similar to that in Crimea where "little green men" helped take over.

One way RS has been building up its paramilitaries is through the police. While Republika Srpska does not have its own military force, it does have an autonomous police force. The government of RS has purchased over 4000 assault rifles within the past two years and three-quarters of its police force can be armed with such rifles.[162] Within the past two years, Republika Srpska has purchased more than 10 times the amount of assault weapons compared to Bosnia's national police.[163] There is little need for a civilian police force to possess such weapons. RS police officers also receive training from Russian intelligence officers and have sent RS officers off to Moscow for additional training.[164] The rise in such professional militarism is alarming and presents a security issue to minorities in RS and BiH as a whole.

There is also militarization of Bosnian Serbs outside of the police force. These paramilitary groups take the form of clubs, gangs, and NGOs. One such example is the growing presence of the Night Wolves, a Russian biker gang also known as "Putin's

[161] "Rent Receives Award in Moscow " B92.net. 12 March 2014 https://www.b92.net/eng/news/region.php?yyyy=2014&mm=03&dd=12&nav_id=89607; "First, the Race of Formula 1, and Then Talks about Politics: Dodik Met with Putin in Sochi." Telegraf RS, 01 October 2018. https://www.telegraf.rs/english/2995608-first-the-race-of-formula-1-and-then-talks-about-politics-dodik-met-with-putin-in-sochi.; Andrew Higgins. "Concern over Why Bikers Linked to Putin Slipped into Balkan City." The Seattle Times. March 31, 2018. S Presidhttps://www.seattletimes.com/nation-world/concern-over-why-bikers-linked-to-putin-slipped-into-balkan-city/.

[162] Reuf Bajrovic, Richard Kraemer, and Emir Suljagic, "Bosnia on the Russian Chopping Block: The Potential for Violence and Steps to Prevent It." Foreign Policy Research Institute. March 2018 https://www.fpri.org/article/2018/03/bosnia-russian-chopping-block-potential-violence-steps-prevent/.

[163] Vera Mironova and Bogdan Zawadewicz. "Putin Is Building a Bosnian Paramilitary Force." Foreign Policy. August 08, 2018. https://foreignpolicy.com/2018/08/08/putin-is-building-a-bosnian-paramilitary-force/.

[164] Ibid.

Angels." In the spring of 2018, the Kremlin spent $40,000 to fund a Balkan tour of the Night Wolves. Their official justification was to celebrate the Orthodox identity of Russians, Serbs, and other Slavs.[165] However, many bystanders believed the Night Wolves had ulterior motives. The gang is infamous for its 2014 involvement in Crimea where some of the members fought in pro-Russian forces and helped set the stage for a Russian invasion.[166] Officials in Bosnia and abroad feared the Night Wolves were in the region for a similar reason. Their activities were largely secretive - although locals noted they tended to fraternize with "hot-headed nationalists."[167] A separate arm of the Night Wolves made up of Bosnian Serbs has been growing in RS. It is feared that the growing presence of the biker gang is a guise under which Serb nationalists can gather. Another new paramilitary group is the youth group "Serbian Honor." While the group claims to promote humanitarian and environmental issues, their actions paint a very different picture. The young Serbs involved in the group have received military training, attended anti-Western protests, and idolized Serbian war criminals.[168] Dodik has relied on Serbian Honor to act as his security force, along with the militarized police. The build-up of these paramilitary groups is especially frightening considering the role of similar groups during the Bosnian War. For example, the gang Arkan's Tigers became infamous for caring out Slobodan Milosevic's nationalist policies. Such groups are also more difficult to monitor as their budgets, inventory, and objectives are not made public.

Russia has also been able to use Bosnia's media against itself. Journalism in BiH lacks transparency and freedom of the press. In Republika Srpska especially, news outlets are at the mercy of the RS government. Board members are changed out with each election cycle as new leading parties take the helm of the RS government.[169] Those that portray the RS position in good light receive generous funding, those that are too critical are shut down. This has resulted in a media that fuels ethnic polarization[170]. With limited funding available and low pay offerings for journalists, Bosnian media cannot compete with Russia news agencies, resulting in a major decline

[165] Andrew Higgins, "Concern Over Why Bikers."
[166] Ibid.
[167] Ibid.
[168] Reuf Bajrovic,, "Bosnia on the Russian Chopping Block."
[169] Milorad Milojević, Azra Memišević, and Bruce Clezy. "Media Landscape in Republika Srpska: Polarization and Financial Dependence." Balkan Diskurs. May 31, 2018. https://balkandiskurs.com/en/2018/05/25/media-landscape-republika-srpska/.
[170]Zselyke Csaky, "As Elections Near, Bosnia's Fractured Media May Do More Harm Than Good." Balkan Insight, 12 Oct. 2018, balkaninsight.com/2018/09/06/as-elections-near-bosnia-s-fractured-media-may-do-more-harm-than-good-09-05-2018/.

in local media. Pro-Russian outlets such as *Russia Today* and *Sputnik Srbija* are able to dominate the newsscape due to their user-friendly websites, stunning graphics, and quality writing. Dodik himself has been pushing for more Russian media in Bosnia which would almost certainly help spread his nationalistic messages.[171] The spread of disinformation is also rampant, with suspicious fake websites popping up constantly. As one journalist states, Bosnia has "an entire 'fake' media emerging [in the country]. Namely, temporary Internet portals are being established with the motive to publish fabricated and unconfirmed information."[172] These fake news sites fail to publish identifying information such as names of journalists, contact information, or ownership information. While there is no way to confirm these fake news sites are linked to Russia, one thing is certain: their release of nationalist propaganda increases tensions in Bosnia.

Finally, the parallels between Crimea and Republika Srpska are plentiful. Dodik has called for the secession of Republika Srpska several times over the years.[173] Unlike Crimea, the entity will not be absorbed by Russia directly. Instead, Dodik is seeking either the RS's reunification with Serbia or independence for RS itself. Such an event would be disastrous for regional stability in the Western Balkans and threatens to reignite a war on par with that in the 1990s. Stoking internal border disputes is also a surefire way to keep Bosnia out of NATO and the EU- something Russia has learned during its exploits in Georgia and Ukraine.

2.3.3 NATO's Interests in Bosnia and Herzegovina

NATO has a long-standing history in BiH. Beginning in the 1990s, the Alliance helped bring an end to Slobodan Milosevic's ethnic cleansing campaign and secure sovereignty for the new country. Their mission was further extended after the signing of the Dayton Peace Accords, which approved a NATO peacekeeping force called the Implementation Force (IFOR). IFOR later evolved into the smaller Stabilization Force

[171] "RS President Wants Russian Media Reach Increased in Bosnia." *N1 BA*, 25 May 2018, ba.n1info.com/English/NEWS/a262683/RS-President-wants-Russian-media-reach-increased-in-Bosnia.html.
[172] Milorad Milojević, "Media Landscape"
[173] "Milorad Dodik: Serb Nationalist Wins Bosnia Presidency Seat." BBC News. October 08, 2018. https://www.bbc.com/news/world-europe-45774872.

(SFOR) before being dissolved in 2004.[174] NATO still has a presence in BiH through NATO Headquarters Sarajevo (NHQSa) which aids in defense reform.[175] However, the security mission has since been handed over to the European Union's EUFOR under Operation Althea. In doing so, it has required NATO to increase their cooperation with other international institutions within BiH. In cases of emergency, KFOR also has a mandate to respond to emergency security issues in BiH if need be. In continuing its ties to NATO, Bosnia joined the Partnership for Peace program in 2006. Most recently, the activation of Bosnia's MAP encourages hope that accession is in its future. Although Bosnia is not a member state, it is located near several NATO members such as Croatia and Montenegro, as well as soon-to-be North Macedonia. Should a conflict in Bosnia break out the security of these members is at stake. As exemplified in the 1990s, instability in the Western Balkans can quickly spread and it would not be unprecedented for members such as Croatia and Turkey to be drawn into another war. As Secretary-General Jens Stoltenberg has said, "the best way of avoiding new conflicts, new tensions is [...] to continue to work with NATO on strengthening the partnership between NATO and Bosnia Herzegovina.[176]"

2.3.4 Current NATO Efforts and Moving Forward

NATO's current mission in BiH is to "project stability" in the country.[177] As mentioned above, NATO is present in BiH in several different areas. Most notably is NHQSa, which mainly focuses on defense reform now that the International Criminal Tribunal for Yugoslavia is over. The institution also helps Bosnia maintain its PfP commitments and provides guidance on achieving its MAP guidelines. However, NHQSa does not appear to be well funded and its objectives are relatively narrow in scope. The mission of NHQSa falls short of NATO's mission to "project stability" in Bosnia. While defense reform in BiH is certainly a priority, building stability in Bosnia requires increased investment.. Other international institutions, such as the EU and

[174] "15 years ago, Dayton Peace Accords: a milestone for NATO and the Balkans." *NATO Review*. December 14, 2010 https://www.nato.int/cps/en/natolive/news_69290.htm
[175] https://jfcnaples.nato.int/hqsarajevo
[176] Nato. "Joint Press Conference with NATO Secretary General Jens Stoltenberg and the Chairman of the Tri-Presidency of Bosnia and Herzegovina, Mladen Ivanić." NATO. 02 Feb. 2017 https://www.nato.int/cps/ie/natohq/opinions_140549.htm?selectedLocale=en.
[177] Ruben Díaz-Plaja. "Projecting Stability: an agenda for action." *NATO Review Magazine*. March 13, 2018. https://www.nato.int/docu/review/2018/also-in-2018/projecting-stability-an-agenda-for-action-nato-partners/en/index.htm

OSCE, help fill those gaps. NATO cannot achieve its mission in Bosnia without cooperating with and complementing these institutions. Yet communication and cooperation among the organizations is not always efficient. In February 2018, the director of the EU Command Element identified two areas in which the EU and NATO have conflicting interests: communicating the breakdown of law and order in Bosnia and training the Bosnian military.[178] EUFOR and NATO must work together to address these challenges. One option would be to host a joint NATO-EU council in the region in which the two organizations can communicate on a daily basis. Meetings between EUFOR and NHQSa should meet weekly in which the two organizations can share developments, craft joint military training initiatives, and other such ventures to ensure confidence and cooperation. Finally, the two organizations should share in monitoring paramilitary buildup in Republika Srpska and commit to intelligence sharing between the organizations. Another way to expand NHQSa's potential would be to consolidate with KFOR in Kosovo, putting the two structures under one joint headquarters. By doing so, communication and resources can be easily shared between the two missions providing them more leeway to achieve goals of reform and stability.

Along with NATO-led institutions such as NHQSa, Bosnia also partners with NATO on many initiatives. The BiH government runs the Peace Support Operations Training Centre (PSOTC) which trains Bosnian military, NATO and UN members, and NATO partners on peace support operations.[179] BiH also voluntarily participates in NATO's Building Integrity program, which helps increase transparency in their defense sector and provides training to the Bosnian military. The PSOTC and BI program provide multiple beneficial trainings for Bosnian military and civilian personnel. However, there is no training focused on de-escalating ethnic tensions. Since NATO does not operate the PSOTC, it would be unable to force the center to run trainings focused on ethnic conflicts. However, NATO could design and suggest the implementation of such course and certify the course under the NATO name. By doing so, NATO can ensure that Bosnian military personnel are ready to help de-escalate conflicts within the Bosnian national military.

[178] Mark Patton, " NATO and EU cooperation marks Bosnia and Herzegovina trip." JFC Naples. Feb. 22, 2019. https://jfcnaples.nato.int/newsroom/news/2018/nato-and-eu-cooperation-marks-bosnia-and-herzegovina-trip
[179]http://www.mod.gov.ba/OS_BIH/struktura/Komanda_za_podrsku/KOiD/PSOTC/Default.aspx?template_id=193&pageIndex=1

2.3.5 Conclusion

The security of Bosnia and Herzegovina is inextricably tied to the security of NATO. Such a fact is as true now as it was in the 1990s. Any outbreak of violence within BiH threatens to draw in NATO members and create rifts in the Alliance. At the same time, the case of Bosnia gives NATO a chance to prevent another Crimean conflict. By monitoring the rise of nationalist leaders, the build-up of paramilitarism, and the spread of disinformation, NATO can quickly mitigate a problem before it gets out of control. These issues can be solved in a number of ways. Cooperating closely with EUFOR to monitor developments, providing improved training for Bosnian military and civilian personnel, and consolidating resources throughout the Western Balkans will help ensure stability in Bosnia and help it fulfil its MAP.

Conclusion

As hybrid warfare continues to evolve and the threats from Russia diversify, it is important for NATO to be aware of the threats that lie just outside member states' borders. To avoid Russia's creeping influence, which has shown its willingness to break international norms to keep, NATO must understand how Russia uses soft power to influence key nations outside the Alliance. The soft power Russia employs, namely religion or ethnic identity, are some of the most powerful tools as the differences created by these identities are very difficult to affect. Kosovo, Ukraine, and Bosnia and Herzegovina are three important case studies that the Alliance can learn from that involve the use of soft power. By consolidating NATO's efforts in the Western Balkans, the Alliance can more easily respond to any crises and simplify complicated international structures. Working more closely with Ukraine can help reverse the gains made by Russia in the country and slowly work Ukraine into the European defense structure. By identifying problem areas early, NATO can work with these countries which already have significant cooperation with the Alliance to help bolster resilience and integrity for the peace and security of Europe.

Religion and Ethnicity Policy Recommendations

- Moderately increase KFOR troops in Kosovo to enhance mission capability.
- Improve intelligence gathering and information sharing with NATO Partner countries, including cultural and religious analysis.
- Develop a clear Membership Action Plan for Ukraine that establishes achievable goals.
- Enhance cooperation between the EU and NATO in Bosnia
- Consolidate NHQSa with KFOR under one Headquarters and Command structure for the Western Balkans.
- Expand trainings initiatives at the Peace Support Training Centre and within the Building Integrity Program.

3. NATO/EU COOPERATION

Introduction

New threats from Russia have led to the need for increased cooperation between NATO and the EU in response to hybrid threats. This chapter will evaluate the joint efforts between these two organizations to improve readiness against hybrid threats and enhance strategic communications and resilience against Russia. NATO and the EU have increased cooperative efforts in building resilience and deterrence throughout their member states, specifically in the Baltics. Disinformation campaigns, cyber-attacks, and military buildup on Russian borders are just a few of the many threats that near-abroad countries like Lithuania, Latvia, Estonia face. As a new member of NATO, the Republic of North Macedonia faces threats of Russian influence which could contribute to further destabilization in the Balkans. With increased challenges of Russian influence in methods of communication, NATO must strengthen its own strategic communications while working more closely with the European Union. Both organizations must work internally and cooperatively to counter Russian efforts to undermine the West and create divisions within society. In a world with increasing and complex malign influences, it is imperative to look toward the future and how NATO and EU security can remain strong amidst a changing global atmosphere.

3.1 Resilience and Deterrence Building in the Baltics

Sofija Raisys

3.1.1 Introduction

In recent years, the security of countries surrounding Russia's borders have come under scrutiny with risk of potential conventional warfare and hybrid threats. Hybrid threats present a complex challenge worldwide, but particularly threaten vulnerable states in Eastern Europe. NATO and the European Union have many member states that border Russia, which prompts the need for a coordinated response from both organizations in creating stronger communication systems and building resilience to prepare the region. Cyber-attacks, ethnic tensions, and Kremlin backed disinformation campaigns have plagued all three Baltic countries in recent years, coupled with the looming threat of a possible Russian invasion of the territories. Disinformation and cyber-attacks are the most pertinent threats to Lithuania today, and the country has implemented counter measures to respond to the hybrid threats.[180] NATO and the EU have each established action plans specifically in the Baltics and have created joint measures to increase resilience and deterrence to combat Russia's growing hybrid threats.

This section will establish the risk of Russia's hybrid threat capabilities as seen by Lithuania and evaluate the individual and cooperative measures of the EU and NATO throughout the Baltics to combat these threats. When assessing the threats that the Baltics face from Russia, NATO must focus on Russia's intentions and the tools they could use to carry out conventional and hybrid threats. NATO has increased deterrence and resilience building efforts in the Baltics in recent years, which will be evaluated in this section and compared to the established threat against the Baltics. For the purpose of this paper, deterrence will be defined as "the threat of force in order to discourage an opponent from taking an unwelcome action. This can be achieved through the threat of retaliation (deterrence by punishment) or by denying the

[180] State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018), 4-6.

opponent's war aims (deterrence by denial)".[181] Looking forward, NATO must enhance its cooperation with the EU to strengthen communication and preparedness in the Baltics with the increasing risk of hybrid threats from Russia.

3.1.2 Threats from Russia

After the Russian annexation of Crimea in 2014, the Baltic countries were considered at risk as former Soviet Republics near Russia. In the "Annual Assessment of Threats to National Security," the State Department of Lithuania asserts that the main threat against Lithuania's security is Russia's aggressive actions along with their motives to change the global balance of power and establish spheres of influence in the Baltics.[182] Surveys conducted in Lithuania in 2012 and 2014 show the change in perception of Lithuanian security and the growing concern around the security of the state amidst threats from Russia.[183] In a 2012 study[184], 18 percent of Lithuanian citizens said that they felt the biggest threat to their country was Russia, while 60.1 percent perceived no military threat to their independence. By 2014, another study[185] showed that public opinion had shifted, with 54.1 percent of the population concerned about the security of the country. However, in the years since the annexation of Crimea, general feelings of security have gradually returned to Lithuanian citizens as years have passed without further public movement from Russia.[186] Latvian national security policy [187] focuses on bilateral and multilateral cooperation as well as participation in international organizations to counter emerging hybrid threats from Russia. Estonia's 2018 National Security Report[188] states that while the largest threat to the Baltics comes from Russia, there is very low probability of Russian military aggression due to Article 5 of the

[181] Michael Ruhle. "Deterrence: What it Can and Cannot Do" NATO Review Magazine. https://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/en/index.htm
[182] State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018), 4-5.
[183] Ingrida Geciene-Janulione, "The Consequences of Perceived (In)Security and Possible Coping Strategies of Lithuanian People in the Context of External Military Threats", *Journal on Baltic Security*. 2018, 6.
[184] Mindaugas Jackevičius, Eglė Samoškaitė. "Apklausa: Realių Grėsmių Lietuvai Nėra, O Jei Bus – Mus Apgins NATO?" *DELFI*. 2012. https://www.delfi.lt/news/daily/lithuania/apklausa-realiu-gresmiu-lietuvai-nera-o-jei-bus-mus-apgins-nato.d?id=60063003.
[185] Egle Samoskaite, "Rusijos Grėsmė Privertė Suprasti Nemalonią Tiesą". *DELFI*. 2015 https://www.delfi.lt/news/daily/lithuania/rusijos-gresme-priverte-suprasti-nemalonia-tiesa.d?id=66883848.
[186] Ingrida Geciene-Janulione, The Consequences of Perceived (In)Security and Possible Coping Strategies of Lithuanian People in the Context of External Military Threats. *Journal on Baltic Security*. 2018, 8-9.
[187] Ministry of Foreign Affairs of the Republic of Latvia. "Directions of Security Policy". 2016. *Mfa.Gov.Lv*. https://www.mfa.gov.lv/en/policy/security-policy/directions-of-security-policy.
[188] Estonian Foreign Intelligence Service, "International Security And Estonia 2018", Estonian Foreign Intelligence Service, 2018, 2-3

Washington Treaty. All three threat assessments present differing concerns on the national security of the individual states in the Baltics, all due to differing history, relationships and global perceptions of Russia influenced by current events.

As former Soviet bloc states with large ethnic Russian populations today, there is a great amount of shared history between Russia and the Baltic States. Russia manipulates history to use to its own political advantage, often victimizing ethnic Russians living in the Baltics and justifying their occupation of Estonia, Latvia and Lithuania for the latter half of the 20th century. A publication from the NATO Strategic Communications Center for Excellence [189] states that Russia's "falsification of history" is commonly used as a tool of confrontation on a global scale. The same publication states that the Russians living abroad are the mechanisms through which Russia promotes its own historical narratives, with history used as one of the front lines in the information war in building national identity and self-esteem. With the independence of the Baltic states in 1991, Russians living in the three countries found themselves outside of their home country in newly recognized independent republics. The history of Russian control over the Baltics under the Soviet Union coupled with an ethnic Russian population in all three countries is used as justification by Russia to protect their citizenry abroad. These actions include military interference and internal interference through less defined hybrid threats. The following section will focus on the hybrid threats from Russia as defined by Lithuanian National Security Policy.

3.1.3 Case Study: Lithuania

This section will highlight Russian hybrid threat capabilities cited from the "Lithuanian National Threat Assessment" as well as NATO documents. The Baltic countries are at potential risk of Russian military and hybrid threats, and each country perceives its risk level differently. Lithuania is an important case because of its proximity to Kaliningrad and Belarus but is often overlooked because of the country's small ethnic Russian population. As mentioned in the above section, Lithuania's State Department claims that there is a threat from Russia due to its aggressive actions and motives to

[189] NATO Strategic Communications Centre of Excellence. "Russia's Footprint In The Nordic - Baltic Information Environment". Riga, 2018, NATO Strategic Communications Centre of Excellence. 44.

expand its spheres of influence worldwide. The report also states that the Enhanced Forward Presence by NATO as well as increased military capability deployed by the alliance have decreased the threat of a Russian military invasion. With presidential elections coming up in May of 2019, Lithuania is now in a vulnerable state and at heightened risk of hybrid attacks from Russia.

In a report on national threat assessment, [190] the Security Department of Lithuania stated that in 2017, Russian propagandists began to focus on campaigns in Lithuania, traveling to the country on tourist visas to fuel anti-Western sentiment through social media and information warfare. Journalists would prepare propaganda aimed at Russian audiences in Lithuania to increase negative attitudes towards the internal and foreign policy of Lithuania, while also organizing defamation campaigns against Lithuanian politicians who opposed Kremlin policies.[191] Many of the ethnic Russians living in Lithuania only follow Kremlin backed news sources, which has little opposition since there are very few independent Russian news sources.[192] Through Kremlin backed news sources, these journalists also sought to create conflict between Polish and Lithuanian citizens based off their shared history.

Russian Intelligence and Security Services (RISS)[193] poses the greatest threat to Lithuanian intelligence, with RISS secret information collection fueling the support for Russia's information, security, and foreign policy against the country. Although Lithuania sustains cyber-attacks on critical infrastructure from many non-state hacker groups, the main threat to Lithuania's cyber security is attacks from Russia. Much of the threat comes from RISS related activities [194] that unleash malicious programs concentrated on infiltrating military, economic, and political information from Lithuania and other NATO member states. In 2018, the Ministry of National Defense became the only government institution in Lithuania responsible for cyber security.[195] This represents the severity of the cyber threat against Lithuania and the country's efforts to centralize coordinated response efforts and increase defense. Increased information warfare and cyber attacks

[190] State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018), 5.
[191] State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018) 5, 26.
[192] Alexandra Wiktorek Sarlo. 2019. "Fighting Disinformation In The Baltic States - Foreign Policy Research Institute". *Foreign Policy Research Institute*. https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.
[193] State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018), 25-27.
[194] Ibid, 25-17.
[195] Ministry of National Defense of the Republic of Lithuania, Lithuanian Defense System: Facts and Trends. 2018. Vilnius. Lithuanian Defense Ministry, 19.

from Russia have created the need for Lithuania to begin to find alternative, non-military methods to combat these attacks.

Russia does not have the conventional power to advance a military conflict against NATO or the Baltics in the coming years, however their focus on regime changes in vulnerable states or countries holding elections will remain high. Russian actors will aim to antagonize the Lithuanian government and society with cyber-attacks and disinformation campaigns with the intent of undermining trust in NATO and democracy. Although Lithuania may not currently be highly vulnerable to existing threats, it must continue to advance resilience and deterrence building efforts. In order to implement resilience within society and counter future disinformation campaigns, media literacy has been introduced into Lithuanian national curriculum.[196] This curriculum helps teach students the methods used to detect fake news and gives tools to evaluate news sources and their accuracy. Media literacy will continue to help build resilience in the coming years as technology and methods of news distribution continue to evolve.

Lithuania continues to increase its military presence throughout the country and provides resources to many international organizations that assist with its defense. With NATO's Enhanced Forward Presence[197], Lithuania provides accommodations for soldiers, force and fire protection, transportation assistance and coordination, as well as access to training facilities. General public support for NATO and its missions within Lithuania have remained high, with 81 percent of those surveyed[198] having support for the presence of NATO troops in Lithuania and 83 percent supporting NATO membership. Lithuania has pledged to increase its defense spending to 2.5 percent of its Gross Domestic Product by 2030 to ensure that long term defense needs are met.[199] The government also vowed to continue updating the national security strategy in response to hybrid threats and to strengthen the monitoring and prevention of possible threats.[200] Russia will continue to develop its military and hybrid capabilities in the face

[196] European Schoolnet. 2017. "Lithuania: Country Report On ICT In Education". European Schoolnet. http://www.eun.org/documents/411753/839549/Country+Report+Lithuania+2017.pdf/dd707697-196e-4c33-ba03-254f3698ea23.
[197] Ministry of National Defense of the Republic of Lithuania, Lithuanian Defense System: Facts and Trends. 2018. Vilnius. Lithuanian Defense Ministry, 11.
[198] Ibid, 16.
[199] Ministry of National Defense of the Republic of Lithuania. Agreement on Lithuanian Defense Policy Guidelines. 2018. Vilnius. Lithuanian Defense Ministry.
[200] Ibid.

of an increased NATO and EU presence in the Baltics, and Lithuania must continue to build up resilience measures within its communities and military to continue to deter Russia from aggressive actions.

3.1.4 NATO and the EU in the Baltics: What Needs to be Done

As EU and NATO member countries, the Baltics have a plethora of allies and resources at their disposal. Although NATO's Article 5 might dissuade Russia from a military invasion, hybrid threats are much more complicated to predict and combat. Multinational NATO battalions currently stationed in the Baltics are enough to deter Russia from invading but also small enough not to provoke a military response[201]. This section will look at the efforts that NATO and the EU implement individually in the Baltics in response to hybrid threats as well as the joint efforts between the two groups. In our current global climate, NATO faces diverse and complex security issues originating from military, cyber, terrorist, and hybrid attacks. Russia's military build-up close to NATO borders has forced NATO to enact deterrence and defense measures to respond and prepare for any imminent attacks to member states. Collective defense and deterrence remain a core element of NATO's overall strategy in protecting allies and preventing conflict within and outside of the alliance[202]. The Readiness Action Plan (RAP) began after the 2014 Wales Summit and was the first reinforcement of collective defense since the end of the Cold War. The RAP provides reassurance to Eastern European members by increasing military activity and implementing assurance and adaptation measures to increase readiness in response to security challenges.[203] This plan helps assist the Baltic countries in building up their own military capability and enables them to respond to attacks as they may arise. Assurance measures include land, sea, and air activities to deter potential security threats, such as Russia. As part of NATO's deterrence plan, the Enhanced Forward Presence was established at the 2016 Warsaw Summit and has stationed 4 battle groups in the Baltic Countries and Poland. The forces operate on a rotating and voluntary basis, meaning they are not permanent

[201] "How The Baltic States Resist Russia". 2019. *The Economist*. https://www.economist.com/europe/2019/02/02/how-the-baltic-states-resist-russia.
[202]"Deterrence And Defence", *NATO, 2018*. https://www.nato.int/cps/en/natohq/topics_133127.htm.
[203] NATO. "NATO's Readiness Action Plan" NATO Factsheet. 2016. www.nato.int/factsheets

armies, and provide defense in line with international commitments. This is a constant reminder of Article 5 and a large reinforcement of collective defense.[204] Battlegroups are led by the United Kingdom, Canada, Germany, and the United States with contributions from smaller NATO countries and local defense forces. Across the Baltics and Poland, there is a total of roughly 4,547 troops stationed under NATO's Enhanced Forward Presence.[205] NATO Air policing also ensures the integrity of allied airspace and gives airspace security to the Baltic countries who do not have necessary air capabilities to maintain their own security.[206] Through NATO's efforts there is an increased military presence throughout the Baltics which sends a clear message to Russia on the collective willingness of allied members to respond to any aggressive actions. NATO's current stance on responding to hybrid threats is as follows: to be prepared, to deter hybrid threats, and to defend allies against any attack.[207] Continued information gathering and analysis are imperative in detecting and assessing threats to NATO member states. The increased military presence in the Baltics coupled with cooperative Strategic Communication and Cyber Centers in Latvia and Estonia help provide research, training, and exercises to prepare and defend against hybrid threats. The 2016 declaration of cyber defense as a core task of NATO's collective defense highlights the increasing awareness of the harm that cyber-attacks have the potential to release within vulnerable countries.[208] Military deterrence through programs like Enhanced Forward Presence and RAP have taken up many resources in NATO, and with looming hybrid threats the organization must widen their focus to building resilience in communities.

Awareness, resilience, and response are the three key points of the EU's response to hybrid threats.[209] The creation of the European Center for Excellence for Countering Hybrid Threats in Helsinki has allowed the EU to continue research and analysis of hybrid threats while also developing counter measures. Responding to and discrediting disinformation online while also preventing interference in elections are top

[204] NATO, "Boosting NATO's presence in the East and Southeast" NATO Topics.
[205] NATO, "NATO's Enhanced Forward Presence", NATO Factsheet. 2018. www.nato.int/factsheets
[206] "Allied Air Command | NATO Air Policing". 2019. *Ac.Nato.Int*. https://ac.nato.int/page5931922/-nato-air-policing.
[207] "NATO'S Response To Hybrid Threats". 2018. *NATO*. https://www.nato.int/cps/en/natohq/topics_156338.htm.
[208] NATO. "NATO Cyber Defense" 2019. NATO Factsheets. www.nato.int/factsheets
[209] European Union. "A Europe that Protects: Countering Hybrid Threats" 2018. EU Factsheet. https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en

priorities for the EU. Building resilience within communities while providing reliable media is a key factor in countering disinformation campaigns and their influence on populations. The EU Action Plan against Disinformation [210] aims to strengthen bonds between member states and the EU in order to effectively address disinformation campaigns and threats within the EU. The European Union and its member states have identified disinformation as a threat to European Democracy, and through the action plan the members improve detection, cooperation, and awareness while creating resilience and mobilizing the private sector.[211] This allows members within the European Union to communicate their concerns over disinformation campaigns, such as those in the Baltics, while using the tools and resources within the EU to combat the campaigns.

With a changing security dynamic throughout Europe, the European Union has initiated the Permanent Structured Cooperation on security and defense (PESCO). This program aims to increase the effectiveness of EU member states in addressing and combating security issues and increasing cooperation within the organization.[212] By using a treaty-based framework, PESCO jointly develops defense capabilities among participating countries in order to improve the EU's role in ensuring the security of its member countries.[213] All three Baltic states participate in the efforts of PESCO, and in 2017 Lithuania proposed an initiative that would strengthen European cooperation in cyber defense by creating response units to cyber-attacks.[214] This creates a more nationalized response to cyber-attacks as they increasingly threaten vulnerable countries such as the Baltics. Lithuania has taken a leadership role in EU cooperation on cyber defense, with other nations observing and participating in their preparation exercises.

As threats continue to emerge, there has been an increasing need for cooperation between the European Union and NATO. The Joint Declaration on EU-

[210] European Union. "Action Plan Against Disinformation" 2018. EU Factsheet https://eeas.europa.eu/headquarters/headquarters-homepage/54831/action-plan-against-disinformation_en
[211] European Union. "Action Plan Against Disinformation" 2018. EU Factsheet https://eeas.europa.eu/headquarters/headquarters-homepage/54831/action-plan-against-disinformation_en
[212] The European Union External Action. 2018. "Permanent Structured Cooperation - PESCO". Brussels: The European Union
[213] Ibid.
[214] "Lithuanian Contribution To Implementation Of The Common (European) Security And Defence Policy | Lithuania's Security Policy | Lithuania In The Region And The World | Foreign Policy | Ministry Of Foreign Affairs". 2018. *Urm.Lt*. https://www.urm.lt/default/en/foreign-policy/lithuania-in-the-region-and-the-world/lithuanias-security-policy/-lithuanian-contribution-to-implementation-of-the-european-security-and-defence-policy.

NATO cooperation was made between the two organizations to highlight their efforts in maritime cooperation, hybrid threats, and security of member states.[215] As a result of this declaration, NATO and the EU have increased burden sharing responsibilities and have heightened their commitments for security and defense. The 2018 Brussels Summit Declaration [216] reiterated the importance of EU and NATO cooperation in the face of shared security interests and reinforced their strategic partnership with the aims of transparency, openness, and respect. This continued the efforts between both organizations to create dialogue and awareness of their cooperation in maintaining European security and Russian deterrence. A 2018 factsheet [217] on NATO and EU relations states that the two organizations have developed closer cooperation on cyber defense as well as protection against hybrid threats through maritime security and enhanced cooperation between partner countries. NATO and the EU hold annual political assessments on security issues throughout Europe and its surrounding states, and recent aggressions by Russia have led to increased communication between both organizations to ensure complementary reactions.[218] The European Center for Excellence on Countering Hybrid Threats has been influential in helping establish cooperation between NATO and the EU by allowing them to cooperate on research, analysis, training, and exercises against hybrid threats. This cooperation between both organizations is a positive recognition of the heightened security and defense needed in response to hybrid threats from Russia. Communication and cooperation between the EU and NATO moving forward is necessary to combat existing hybrid threats, as each organization has valuable resources that are more powerful together.

3.1.5 Conclusion

NATO and the EU have implemented many independent security initiatives within their organizations to protect the Baltics. Independently, the Baltic countries have used different risk analyses of the threats from Russia and the steps they must take to protect themselves. However, as EU and NATO members, the Baltic countries all benefit from

[215] NATO. 2018. “Joint Declaration on EU-NATO Cooperation”. https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en
[216] NATO. 2018. "Brussels Summit Declaration". https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21.
[217] NATO. “NATO – EU Relations” 2018. NATO Factsheets. www.nato.int/factsheets
[218] NATO. “NATO – EU Relations” 2018. NATO Factsheets. www.nato.int/factsheets

increased deterrence and resiliency building efforts by both organizations. In a global order where Russia has proved to be untrustworthy and extremely unpredictable with conventional and hybrid threat methods, preparedness is key. With 22 member states in common, the EU and NATO must communicate and operate on the ground together in the Baltic states to increase their readiness against potential threats. This should include joint military exercises and operations between both countries as well as increased cooperation in resilience and deterrence building efforts. Each Baltic country views the threat of Russia's military and hybrid capabilities differently, and NATO must work to establish the unique threat levels for each country while ensuring that all three countries are properly prepared for the threats they face. This includes preparedness in cyber security, energy security, disinformation, and military realms as they each play a different role in each of the Baltics. In addition to continued military presence in Lithuania, creating resilience within local communities to combat disinformation campaigns is vital. The continuation of media literacy programs is essential in teaching citizens how to spot inaccurate news and Kremlin backed sources. Without programs like Enhanced Forward Presence, the Baltics would be at greater risk for military aggression from Russia, and NATO and the EU must cooperate to make a coordinated and effective response to protect their allies. Both organizations, as well as the Baltic States, must consider the true intentions of Russia and its zero-sum game and prepare accordingly.

3.2 Collaborative Efforts to Strengthen Strategic Communications Against Hybrid Threats from Russia

Sara Bak

3.2.1 Introduction

In order to effectively build resilience and integrity against Russian hybrid threats, NATO must consider other methods of hybrid warfare including strategic communications. In general terms, strategic communications could be loosely defined as the strategic utilization of communication mechanisms to achieve specific objectives, such as advancing political agendas, spreading propaganda, or fostering public support. As Russia continues to challenge the Western narrative through means of strategic communications, it is imperative for NATO to strengthen its own strategic communications while countering that of Russia. NATO defines its strategic communication as "the coordinated and appropriate use of NATO communications activities and capabilities… in support of Alliance policies, operations and activities, and in order to advance NATO's aims".[219] Meanwhile, Russia does not use the term "strategic communications" nor does it have an equivalent term, as it is difficult to fully encapsulate the nature of Russian information campaigns in a few, succinct words. However, for the sake of clarity, the term "information war[220]" is similar enough to describe Russia's strategic communications. This refers to the ability to "undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a State in order to destabilize society and the government; and force a State to make decisions in the interests of their opponents".[221]

Russia's information campaigns are increasingly problematic since Russian narratives, propaganda, and disinformation intend to undermine the current efforts, cohesion, and trust among NATO members. By tailoring and strategically distributing different information to the Russian and foreign public, the Russian government is able

[219] "FAQ," STRATCOMCOE, Accessed January 29, 2019, https://www.stratcomcoe.org/faq.
[220] Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," Defence Strategic Communications 1, no. 1 (2015): 12, Accessed February 20, 2019.
[221] Ibid.

to achieve its goals for each target. Through strategic communications, Russia can inflict great damage overseas while solidifying its own image and credibility within its borders. Targeting the minds of people can arguably be more dangerous than utilizing other methods of hybrid warfare since people can easily spread a vast amount of false information via media, internet, and other networks with a simple click of a button. This section will focus on Russia's strategic communication in the mainstream media, NATO's current efforts to build up resilience and defense in the strategic communications sphere, and the European Union's efforts as well. After analyzing these components, policy recommendations will be provided.

3.2.2 Russian Methods and Tactics

Russia's utilization of strategic communications as a method of hybrid warfare is not a recent phenomenon. Since the Cold War, Russia has continued to create anti-West propaganda in hopes to reassert its power and to dismantle the West's soft power, specifically its credibility.[222] Through this usage of propaganda, Russia "[pours] the elixir of life into one's own masses and poison into the enemy's, and by using [positive] propaganda as an antidote, [Russia] should save [its own people] from the enemy's poison".[223] This, along with convincing European audiences that NATO and the EU are neglecting legitimate threats from the south by directing their attention on imagined threats from Russia, are the objectives of their strategic communications. [224]

Considering Russia's unilateral position against the Western world, pro-Russian and anti-West propaganda can be easy to spread within Russia. As for overseas, Russia has implemented Internet troll campaigns to distribute false or controversial information and create further division between groups of people.[225] At the Internet Research Agency in St. Petersburg, Russians were hired by the government to post pro-Kremlin propaganda under fake identities on social media.[226] These trolls aim "to publish and disseminate commissioned articles, to establish fake accounts on social

[222] Antonio Missiroli et al., Strategic Communications - East and South, report, 25.
[223] Ofer Fridman, "The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse.," Defence Strategic Communications 2, no. 1 (2017): 67, accessed January 27, 2019, doi:10.30966/2018.riga.2.3.
[224] Antonio Missiroli et al., Strategic Communications - East and South, report, 14.
[225] Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," 13.
[226] Adrian Chen, "The Agency," New York Times, accessed February 27, 2019, http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0

networks so as to distribute commissioned information, as well as to disseminate spam and persecute opponents on the Internet".[227] The more frightening fact is that these Russian trolls can post anonymously and without attribution, thus avoiding accountability and responsibility. Its intentional aims to demonize the West and undermine democracy have, unfortunately, been more successful than not. Alarmingly, Russia's persistence in pursuing anti-West propaganda has not deteriorated over time. It continues to produce propaganda and succeeds in creating noise.

Recently, there were two separate Russian disinformation attempts against Germany and Lithuania that seized the attention of German Chancellor Angela Merkel and NATO Secretary-General Jens Stoltenberg. Germany's role in the Ukraine crisis, Merkel's push for sanctions against Russia, and her leadership in Europe made Germany a main target for Russia's disinformation campaign.[228] In the German case, it was falsely reported that a 13-year-old Russian-German girl was sexually assaulted by migrants. No one could have predicted the aftermath - demonstrations involving neo-Nazi groups, public statements presented by both Russian Foreign Minister Sergey Lavrov and German Chancellor Angela Merkel, and the false information distributed through social media and right-wing groups.[229] A similar case occurred in Lithuania where German soldiers (stationed there as a part of NATO's new battle group) were falsely accused of sexually assaulting a teenage girl.[230] The Lithuanian authorities were swift to discredit these accusations and Secretary General Stoltenberg commended their quick efforts to reveal the truth.[231] Despite the immediate dismissal in this one incident, it is still concerning to see how quickly these disinformation campaigns spread to the public and captured the attention of nation leaders as well. These two incidents are only a small piece of the countless amounts of anti-West propaganda that aims to create noise, distract the public, and taint NATO's reputation.

Ironically, the oversaturation of disinformation distributed by the Russian media has proven to occasionally backfire and be counter-productive. The overwhelming

[227] Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," 13.
[228] Stefan Meister, "The "Lisa Case": Germany as a Target of Russian Disinformation," NATO Review Magazine, accessed February 6, 2019, https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.
[229] Ibid.
[230] Teri Schultz, "Why the 'fake Rape' Story against German NATO Forces Fell Flat in Lithuania," DW, February 23, 2017, accessed February 6, 2019, https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870.
[231] NATO, "Doorstep Statement," news release, February/March, 2017, NATO, accessed February 1, 2019, https://www.nato.int/cps/en/natohq/opinions_141621.htm.

amount of news given to the public has caused confusion among the people since news reports can be contradictory. Russian news outlets also spread lies such as the denial of any Russian armed forces in southern and eastern Ukraine.[232] This contradicts Putin's own propaganda that proclaims Russia's responsibility to save Crimea and Ukraine.[233] For other incidents, several news stations and the government would offer contradicting facts to the same story; this is detrimental to their credibility and trust.

Even so, the number of Russians who hold negative perceptions of the West is startlingly high. The Levada Center, located in Moscow, has conducted several public opinion surveys regarding the West in recent years. In October 2015, 82% of respondents said that the West is hostile towards Russia and 44% accused the West of waging an information war.[234] In 2014, 4% of respondents believed that by tightening the sanctions against Russia, the West was trying to "stop the war, destruction, and people's deaths in Eastern Ukraine" but merely a year later, 71% of respondents believed that the West was instead aiming to "weaken and humiliate Russia".[235] The drastic rise within a year is a testament to the influence Russian propaganda has over the public.

Some may argue that the Western media could eliminate and discredit Russian propaganda by simply fact-checking but it is not that straight-forward. It is extremely important to navigate this carefully since the Russians may try to manipulate any opposing narrative or create their own to generate more propaganda. Since Russia's general public holds distrust towards the West, they are unlikely to believe the West's claims that Russian news is false. Even President Vladimir Putin openly stated "Today, NATO seems to be making a show of its anti-Russian stance… as we face a growing barrage of information attacks unleashed against Russia by some of our so-called partners, we need to make even greater efforts in this direction" at a Russian Federation meeting in 2016.[236] By portraying NATO as a malicious and two-faced actor who seeks

[232] "60 минут по горячим следам (вечерний выпуск в 18:50) от 14.01.19," YouTube video, 58:33, "60 минут," January 14, 2019, https://www.youtube.com/watch?v=lK-UntXwq7Y.
[233] Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," 17.
[234] Fridman, "The Russian Perspective on Information Warfare", 79.
[235] Ibid.
[236] "Meeting of Russian Federation Ambassadors and Permanent Envoys," news release, June 30, 2016, President of Russia, accessed February 7, 2019, http://en.kremlin.ru/events/president/news/52298.

to sabotage Russia, Putin is able to unite Russians with a shared distrust of NATO and the West.

3.2.3 The NATO Response

Due to the rise in information warfare, NATO is facing a greater and more urgent need to defend its member-states and the West from Russian strategic communication threats. NATO has been implementing more transparency, public awareness, and information regarding its own strategic communications methods and research.[237] It is critical for NATO to be transparent with the public so that it can gain more credibility and trust. Though anti-West propaganda has already influenced some audiences, NATO cannot afford to ever stop producing its journals and reports; it must continue to counter disinformation attempts by providing its own facts and data. This will boost public faith and morale, which would then enable NATO to carry out its plans with more ease.
To foster resilience and readiness in response to strategic communications threats, the NATO Strategic Communications Centre of Excellence (NATO StratCom COE or StratCom COE) was established in January 2014 by a group of like-minded nations.[238] It's important to note that not all NATO members are participants of StratCom COE – the current member states are Estonia, Germany, Italy, Latvia, Lithuania, Poland, Netherlands, Canada, France, United Kingdom, Finland, and Sweden – and that the last two countries are not members of NATO.[239] The StratCom COE holds a significant role of NATO's efforts in achieving its political and military objectives. Its mission is "to provide a tangible contribution to the strategic communications capabilities of NATO, NATO allies, and NATO partners"; these capabilities encompass "Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations and Psychological Operations".[240] NATO partners are the international organizations and countries in different structures, such as the "Partners Around the Globe", United Nations, EU, and Euro-Atlantic Partnership Council.[241] Since NATO operates as an organization that

[237] NATO's strategic communications is "the coordinated and appropriate use of NATO communications activities and capabilities - Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations and Psychological Operations, as appropriate - in support of Alliance policies, operations and activities, and in order to advance NATO's aims"
[238] "About Us." STRATCOMCOE, accessed January 29, 2019, https://www.stratcomcoe.org/about-us.
[239] Ibid.
[240] Ibid.
[241] "Partners," NATO, November 11, 2015, accessed January 29, 2019, https://www.nato.int/cps/en/natohq/51288.htm.

values consensus and only has 10 members participating in StratCom COE, the center is not a part of the NATO Command Structure. Nonetheless, it still serves to contribute to all of NATO as needed.

NATO StratCom COE has proven itself to be a promising and valuable asset to NATO's strategic communications objectives. It provides "comprehensive analyses, timely advice and practical support to the Alliance, designs programs to advance doctrine development, conducts research and experimentation to find practical solutions to existing challenges".[242] This past year, its main activities included the annual conference "The Riga StratCom Dialogue", the "Defence Strategic Communications" academic journal, several reports analyzing social media, and participation in various efforts.[243] StratCom COE also aims to promote awareness of and build support for NATO's policies, efforts and activities.[244] With more successful activities and well-researched published journals regarding strategic communications, NATO is able to gain more public support for its activities.

A defining component of StratCom COE is the annual Riga StratCom Dialogue. This is a groundbreaking conference where the top strategic communications experts from 40 different countries' government sectors, militaries, academia, and private sectors gather to discuss the most pressing strategic communications topics.[245] Its establishment is very recent, as it will host its fourth annual conference this upcoming June. Without this Dialogue, StratCom COE would not be as impressive and influential as it is today. With that said, it is not without flaws. The lines between spheres such as public affairs and public diplomacy, and information operations and psychological operations are blurred. It is difficult to definitively distinguish the components from one another since there are several overlaps. While public diplomacy is the "civilian communications and outreach efforts... responsible for promoting awareness of... NATO's policies...", public affairs is the "civilian engagement through the media to

[242] "FAQ," STRATCOMCOE.
[243] "About Us," STRATCOMCOE.
[244] "About Strategic Communications," STRATCOMCOE, accessed January 28, 2019, https://www.stratcomcoe.org/about-strategic-communications/
[245] "The Riga StratCom Dialogue 2018." STRATCOMCOE. Accessed February 21, 2019. https://www.stratcomcoe.org/riga-stratcom-dialogue-2018

inform the public of NATO policies...".[246] Too much overlap can dilute the effectiveness and vision of StratCom COE.

3.2.4 The EU Response

NATO considers the European Union (EU) to be a unique and essential partner and has already collaborated with the EU on various issues of strategic communications since 2001.[247] In 2016, the President of the European Council, President of the European Commission, and the Secretary General of NATO signed a joint declaration that outlines EU-NATO goals for their strategic partnership – one goal being "countering hybrid threats".[248] In 2017, the EU held the official inauguration of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).[249] Though it is a hub of the EU, it has proven to be a successful neutral facilitator to foster cooperation between the EU and NATO.

The functions of the European Center of Excellence for Countering Hybrid Threats are as follows: be a *platform* for nations to come together to share best practices, build capability, test new ideas and exercise defense against hybrid threats; be a *neutral facilitator* between the EU and NATO through strategic discussions and exercises; and to lead the conversation on countering hybrid through research and sharing of best practices.[250] The Center has already been effective in strengthening EU-NATO cooperation in the area of hybrid threats - both organizations have participated in the Center's activities, workshops, seminars, and exercises to foster greater understanding of hybrid threats.[251] In NATO's progress report of 2016-2017, it was reported that NATO and the EU discussed further cooperation in the East, the South, and the Western Balkans.[252] It was also noted that the strategic communications

[246] Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," 136-137.
[247] "Relations with the European Union," NATO, July 18, 2018, accessed January 29, 2019, https://www.nato.int/cps/en/natohq/topics_49217.htm#.
[248] EU-NATO Cooperation, report, accessed January 29, 2019, https://eeas.europa.eu/sites/eeas/files/eu_nato_factsheet_05-03-2018_en.pdf.
[249] "EU And NATO Welcome Hybrid CoE," STRATCOMCOE, October 4, 2017, accessed January 31, 2019, https://www.stratcomcoe.org/eu-and-nato-welcome-hybrid-coe.
[250] "What Is Hybrid CoE?" Hybrid CoE, accessed January 29, 2019, https://www.hybridcoe.fi/what-is-hybridcoe/.
[251] Ibid.
[252] *Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*., report, June 8, 2018, accessed January 29, 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf.

counterparts engage with each other often but the specifics of those engagements were not disclosed.

Within the Hybrid CoE are two active Communities of Interest (COI) – "Hybrid Influence" and "Vulnerabilities and Resilience".[253] COIs are integral to Hybrid CoE since they "allow the space for multinational and multidisciplinary sharing of best practice, experience and expertise so that member states and institutions can better understand, defend against and respond to Hybrid threats".[254] The Hybrid Influence COI focuses on how state and non-state actors conduct hybrid campaigns, and how hostile actors use their influences to destabilize other nations while the Vulnerabilities and Resilience COI focuses on detecting member states' vulnerabilities and fostering resilience.[255] Participation in these communities is open to all EU member states and NATO allies. These COIs are instrumental in strengthening and propelling Hybrid CoE forward to effectively fulfill its functions.

The EU also has the Strategic Communications Division (StratComms) which works to promote key EU policies to all audiences, provide professional support to the High Representative in all public diplomatic activities, and develop communication strategies.[256] In essence, StratComms offers communications guidance to the EU. Hybrid CoE and StratComms are both valuable and necessary, since they allow a platform in which nations can come together to discuss hybrid warfare and offer guidance to the EU on communicating effectively to the public. However, it is noteworthy that their core functions are different to those of NATO.

3.2.5 Comparative Analysis of Hybrid CoE and Stratcom COE

Although StratCom was created to specifically lead the EU's strategic communications efforts, the Hybrid CoE is more established and relevant to the study of strategic communications as a tool of hybrid warfare. Hybrid CoE's scope is wider than solely communication guidance; it encompasses the study of information warfare and offers spaces where participants may be better equipped to aid their respective

[253] "Communities of Interest," Hybrid CoE, accessed January 29, 2019, https://www.hybridcoe.fi/communities-of-interest/
[254] Ibid.
[255] Ibid.
[256] "Strategic Communications," European Union External Action, accessed January 29, 2019, https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en

organizations. It would be more productive to look more closely into Hybrid CoE when comparing EU's capabilities to NATO.

Though Hybrid CoE and StratCom COE both hold workshops, seminars, and activities to build better understanding and research of Russia's strategic communications, the former is distinguished by its role as a platform for inclusive discussion. The latter could be considered as NATO's version and blend of StratComms and Hybrid CoE's functions and capabilities.

These two centers also publish several journals and reports on their websites at a monthly rate, which are available to the public. StratCom COE also provides valuable information and reports via Twitter. With free and easily accessible information through the Internet, the public are able to keep up with recent news and educate themselves of disinformation attempts, NATO/EU updates, and other reports. The work and progress that these two centers have put out are already promising; though they are separate, they cover a substantial amount of the strategic communications realm.

3.2.6 Conclusion

NATO has achieved substantial progress in strengthening its strategic communications strategies, but it has the capabilities and resources to widen its reach. Both NATO and EU possess sophisticated and powerful centers of excellence that have provided tremendous assistance, expertise, and activities related to strategic communications. As of right now, NATO StratCom COE and the EU's Hybrid CoE have no past or current joint efforts. NATO members have been invited to participate in Hybrid Coe's events and vice versa, but the two centers have never held an official joint event before. These two organizations have been independently successful, therefore future collaboration may yield very promising results. Increased EU-NATO cooperation is essential in building integrity and resiliency against strategic communications hybrid threats from Russia.

3.3 NATO Resilience and Article 3, The Case of Macedonia

Naomi Faletti

3.3.1 Introduction

Hybrid threats from Russia present a serious challenge to the transatlantic relationship. It is essential for NATO and the EU to enhance cooperation and resiliency to resist and deter Russian hybrid warfare threats. The Republic of North Macedonia (hereafter referred to as Macedonia) is a necessary ally in deterrence efforts against Russian aggression in the Balkans. Macedonia is awaiting ratification of the accession protocol, signed on February 6th, 2019. Full NATO membership will help stabilize the country and its neighboring states. Macedonia is not a member of the EU, but following Macedonia's name change, the EU has reopened possibilities for its membership after approval from all member states. The decision of Macedonia to join NATO is essential for stabilizing the country, bringing democracy to the region and improving resiliency and integrity against Russia's hybrid threats in the Balkans.[257]

3.3.2 Case Study: The Republic of North Macedonia

On January 27, 2019, the Greek ratification of Macedonia's name change to the Republic of North Macedonia was a momentous occasion for both countries. This name change was necessary for the Republic of North Macedonia as this was a prerequisite for NATO membership. The dispute over the name change arose when the breakup of Yugoslavia took place nearly 26 years ago between Macedonia and Greece. This region was part of an ancient kingdom that was led by Alexander the Great and the name "Macedonia" is critical to the national identity of Greece and Macedonia.[258]

Russia has been taking advantage of disputes between Greece and Macedonia to regain influence in the Balkans since the division of Yugoslavia. The Balkan elites also took advantage of the exacerbated situation created by Russia, in turn delaying internal reforms in Macedonia. These factors also delayed Macedonia's accession process into

[257] Joyce P. Kaufman. NATO and the Former Yugoslavia: Crisis, Conflict, and the Atlantic Alliance. Rowman & Littlefield, 2002.
[258] Joanna Kakissis. 2018. "For Two Countries, The Dispute Over Macedonia's Name Is Rooted In National Identity." npr. February 4, 2018. https://knpr.org/npr/2018-02/two-countries-dispute-over-macedonias-name-rooted-national-identity.

NATO.[259] However, Western powers in the region emphasized NATO and EU engagement which hindered Russia's motives in extending its spheres of influence, thus provoking Russian aggression.[260]

Washington detected Russia's attempts to spread disinformation and to meddle with voting preceding Macedonia's 'name-change' referendum.[261] U.S. Defense Secretary Jim Mattis delivered the U.S. intelligence findings of disinformation attempts with the Macedonian government during his visit in September 2018. Putin has used destabilization campaigns, backed by the Kremlin's financial support, to damage democratic norms and distract the underdeveloped infrastructures in the Western Balkans region.[262] Macedonia's recent ratification process and Putin's attempt to influence this is an example of a small nation's vulnerability against Russia. It is also a threat to democracy and NATO–EU relations where shared values and cooperation are fundamentally crucial [263] to member states' stability. Russia's alleged tampering in the Macedonian referendum,[264] demonstrates the strategy, knowledge of the targeted nation and other methods used by Russia to exert its malign influence.[265]

Russia's attempt to destabilize countries like Macedonia as a result of its internal vulnerabilities is problematic. This action also affects other peripheral states through disinformation campaigns. This phenomenon is essential to understand as it shows its disregard for international norms and democracy. During the vote of Macedonia's name change, there was evidence of Russia's involvement in attempting to influence the outcome of the referendum. Through the destabilization campaign, Russia was openly working to restore its former Soviet spheres of influence. [266] NATO is an attractive

[259] Jeffrey Mankoff. 2017. "How to Fix the Western Balkans." Foreign Affairs. July 7, 2017. https://www.foreignaffairs.com/articles/southeastern-europe/2017-07-07/how-fix-western-balkans.
[260] Anastasakis, Othon. 2017. "Russia, South East Europe and the 'Geopolitics of Opportunism'." Clingendael Spectator 4 – 2017 (Vol.71) – Item 7 of 11. 2017. https://spectator.clingendael.org/pub/2017/4/russias-involvement/.
[261] Indrees Ali. 2018. "Russia's Been Meddling with a US Ally in Europe, and Mattis Isn't Happy." Business insider. September 17, 2018. https://www.businessinsider.com/russias-been-meddling-with-us-ally-macedonia-and-mattis-isnt-happy-2018-9?IR=T.
[262] Matthias Bieri. 2015. "The Western Balkans Between Europe and Russia No. 170." CSS Analyses in Security Policy. CSS. March 2015. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse170-EN.pdf.
[263] "The Future of the Transatlantic Alliance." 2019. NATO. January 19, 2019. https://www.nato.int/cps/en/natohq/opinions_162650.htm?selectedLocale=en.
[264] "Russia's Been Meddling with a US Ally in Europe, and Mattis Isn't Happy." April 17, 2018. Accessed February 13, 2019. https://www.businessinsider.com/russias-been-meddling-with-us-ally-macedonia-and-mattis-isnt-happy-2018-9?IR=T
[265] Jeff Seldin. 2018. "Russia Influence Operations Taking Aim at US Military." VOV. November 2, 2018. https://www.voanews.com/a/russia-influence-operations-taking-aim-at-us-military/4640751.html?fbclid=IwAR0pRrpCxrrCpsj79Nt3DknTy5xLIL3JAJNHQi-dCHpNDnhg50GLNp_wVNo.
[266] James Kitfield. 2018. "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti." Breaking Defense. October 1, 2018. https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter-russians-gen-scaparrotti/.

"club"[267] for small nations like North Macedonia in preserving its sovereignty and territorial integrity.

NATO's position to reiterate its open door policy and protect the smaller states [268] illustrates a unified stance regarding NATO's engagement with small but geographically important states to resist and deter Russian aggression. [269] This political message is one of strong solidarity and unity, aimed at deterring any potential adversary from future aggression. Once the EU ends the accession freeze on Macedonia, its membership process will resume. This process will provide a mutually beneficial relationship aimed at uniting NATO and EU common goals regarding Macedonia's development. This shift will also threaten Russia's influence as NATO's development into the Balkans affects Moscow's goal in recapturing former spheres of influence.[270] Macedonia's participation in NATO and possible EU membership is a blow to Russia, as it "struggles to cling to its power in the Balkans, the site of Europe's bloodiest conflicts since the end of World War II".[271]

Since 1995, Macedonia has been a part of NATO's Partnership for Peace (PfP) providing valuable support to NATO-led operations in Afghanistan and Kosovo.[272] In Feb 2001, NATO aided Macedonia when conflict broke out between Albanian insurgents and security forces in western Macedonia.[273] Macedonia's vulnerability continues as it provides an easy Russian target in the process of establishing democracy and infrastructure. Macedonia is lagging in several areas that are essential for economic growth and development following decades of conflict.[274]

---

[267] Steven Erlanger and Erick Gladstone. 2019. "Https://Www.nytimes.com/2019/02/06/World/Europe/North-Macedonia-Nato-Russia.html." New York Times. February 6, 2019. https://www.nytimes.com/2019/02/06/world/europe/north-macedonia-nato-russia.html.
[268] "Joint Press Point with NATO Secretary General Jens Stoltenberg and Foreign Minister Nikola Dimitrov." 2019. NATO. February 6, 2019. https://www.nato.int/cps/en/natohq/opinions_163080.htm?selectedLocale=en.
[269] Crosby, Alan. 2019. "Now That NATO Door Is Open, North Macedonia Gets To Show That It Belongs." RadioFreeEuropeRadioLiberty. February 7, 2019. https://www.rferl.org/a/macedonia-nato-russia-influence-greece-name-change/29757662.html.
[270] "Relations with the Republic of North Macedonia." n.d. NATO. Accessed February 15, 2019. https://www.nato.int/cps/en/natohq/topics_48830.htm.
[271] Chris Strohm. 2018. "U.S. Says It Will Alert Public to Foreign Influence Operations." Cyber security . Bloomberg. July 20, 2018. https://www.bloomberg.com/news/articles/2018-07-19/rosenstein-cites-growing-cyber-threat-against-u-s-elections.
[272] "Relations with the Republic of North Macedonia." n.d. NATO. Accessed February 15, 2019. https://www.nato.int/cps/en/natohq/topics_48830.htm.
[273] Ibid.
[274] "Macedonia." n.d. U.S. Department of State. Accessed February 20, 2019. https://www.state.gov/j/inl/regions/europeasia/219024.htm.

Thus, the international order must help the state resolve issues resulting from the lack of infrastructure and resources.[275] The vulnerability of Macedonia remains constant especially in today's complex and multidimensional environment, especially in the Balkan region. It is now necessary to reinforce further efficiency of NATO and the EU's role in assisting Macedonia's stable transition toward increased democracy and sovereignty.[276]

Additionally, the EU has been an active supporter of Macedonia's economic development by establishing "Stabilization and Association Agreements" (SAAs) in 2004.[277] SAA is a bilateral free trade agreement (FTA) to help promote Macedonia's economic development and assist political stabilization in other participating nations in the region. These programs will create a long-term association between the EU and the Western Balkans. Macedonia has received the Instrument for Pre-Accession Assistance (IPA) from EU for its "transition and institution building, cross-border cooperation, regional development, human resources, and rural development".[278]

3.3.3 Conclusion

Macedonia's geopolitical position is essential in maintaining European and Balkan security.[279] Macedonia's active participation in European affairs and NATO membership plays a significant role in future stability efforts. Russia's goal is to create instability and distract the rule of law[280] in the Balkans and it will likely continue in Macedonia. Thus, Russia is expected to continue using its resources to undermine democracy creating a continued threat.

Russia's behavior is becoming progressively unpredictable and aggressive following the annexation of Crimea in 2014. Putin's desire to expand its spheres of influence

[275] Yoan Stanev. 2018. "Macedonia Seeks Funding for Regional Infrastructure Projects." EMERGINGEUROPE The Gateway to the Region. July 14, 2018.
[276] Ivica Gjorgjevski.. 2018. "Marshall Center – Republic of Macedonia at the Fourth 'European Week – Days of Europe' 2018." Marshall Center-Republic of Macedonia Alumni Association. May 23, 2018. https://mcrm.org.mk/en/2018/05/23/marshall-center-republic-of-macedonia-at-the-fourth-european-week-days-of-europe-2018/.
[277] "Western Balkans." n.d. European Commission. Accessed February 19, 2019. http://ec.europa.eu/trade/policy/countries-and-regions/regions/western-balkans/.
[278] "Instrument for Pre-Accession Assistance (IPA)." n.d. European Commission. Accessed February 19, 2019. https://ec.europa.eu/regional_policy/en/funding/ipa/.
[279] Sotirovic, Vladislav B. 2019. "The Geopolitics Of South-East Europe And Importance Of The Regional Geostrategic Position (I)." OrientalReview.Org. February 20, 2019. https://orientalreview.org/2019/02/20/the-geopolitics-of-south-east-europe-and-importance-of-the-regional-geostrategic-position-i/.
[280] "Opening Remarks." 2019. NATO. February 6, 2019. https://www.nato.int/cps/en/natohq/opinions_163075.htm?selectedLocale=en. Rule of Law

encompasses military and ideological ambitions. General. Curtis Scaparrotti (NATO Supreme Allied Commander) claims Russia will continue to break international law and norms to further its own position and motives.[281] Just like the disinformation campaign Russia used in the Macedonia referendum, unconventional hybrid warfare tactics are less costly compared to armed military measures.

In the NATO–Russia Founding Act of 1997, Russia pledged to not threaten or use force against NATO members and partners. Although this is the case, Russia continues to utilize aggressive hybrid tactics to further its motives.[282] Macedonia's case study demonstrates Russian activities, and the use of force and shows the potential weakness and strengths of NATO–EU cooperation to deter Russian influence in a region. The newly structured EU-NATO strategic partnership announced on July 8, 2018[283] will also enhance collaboration in response to hybrid threats, cyber security, and defense as well as joint exercises and operations in the future. Acceptance of democratic ideologies, assistance in infrastructure development and structural financial stability programs, and resource sharing in Macedonia could help extend the common NATO–EU agenda of peace and democracy in the region.[284]

The next step is to ensure efficient NATO–EU cooperation without duplicating efforts. [285] Close coordination will not only increase efficiency while cutting costs but also create a path for joint success. It is highly probable that, like Macedonia, other NATO and EU members and potential member states will also face Russia's malicious influence in the future.[286] Estonia, Latvia, and Lithuania are good examples of the benefit that NATO and EU membership can provide. Here, individual and national initiatives paired with organizational membership leads to stronger resilience, while they continued to be under Russian focus and attempted influence. Therefore NATO–EU cooperation with well-established and reciprocal efforts to deter risks needs to be addressed regularly.

---

[281] Ibid.
[282] "Relations with Russia." 2019. NATO. February 4, 2019. https://www.nato.int/cps/en/natolive/topics_50090.htm.
[283] "EU-NATO Cooperation - Factsheet." 2018. EU-NATO cooperation Factsheet. November 22, 2018. https://eeas.europa.eu/headquarters/headquarters-homepage_en/28286/EU-NATO cooperation - Factsheet.
[284] Ibid.
[285] "Relations with the European Union." 2019. NATO. February 15, 2019. https://www.nato.int/cps/en/natohq/topics_49217.htm?selectedLocale=en.
[286] Mankoff, Jeffrey. 2017. "How to Fix the Western Balkans." Foreign Affairs. July 7, 2017. https://www.foreignaffairs.com/articles/southeastern-europe/2017-07-07/how-fix-western-balkans.

Finally, Russia will likely focus on Bosnia who has expressed a desire to cement its potential membership. NATO should set up vigorous programs with EU organizations to ensure reciprocal efforts to deter Russia in the heart of Western Europe. Enhanced information and resource sharing programs are integral to create comprehensive frameworks to deter future Russian threats. There have been current activities for broader cooperation with Macedonia "focused in particular on cyber defense, counter-terrorism, defense against chemical, biological, radiological and nuclear agents, and environmental security".[287] These sharing efforts between NATO and Macedonia are valuable guidelines for future targets to deter Russian influence, especially for those vulnerable States in the Balkans yet to become NATO and EU members.

[287] "Joint Press Point with NATO Secretary General Jens Stoltenberg and Foreign Minister Nikola Dimitrov." 2019. NATO. February 6, 2019. https://www.nato.int/cps/en/natohq/opinions_163080.htm?selectedLocale=en.

Conclusion

NATO and EU efforts in response to hybrid threats need to go beyond their independent organization's efforts. Both organizations lead independent defense efforts and strategic communication centers but must enhance their deterrence and readiness in response to hybrid threats. The European Union and NATO have both agreed to enhance their cooperation in security of their member states as they face growing security concerns and have reaffirmed their commitment to increased dialogue. In the Baltic region, NATO leads several military defense efforts to deter Russia from invading, while the European Union has implemented PESCO to increase cooperative defense capabilities. In response to Russia's hybrid warfare aggressions, NATO and the EU must enhance their cooperation in resilience and deterrence building in the Baltics. This includes coordinating joint exercises to create a military presence to deter Russia's advances while also increasing communication and resilience building in response to disinformation campaigns. All three Baltic states must be equipped and prepared to face any potential threats from Russia with the help of their allies. Considering both NATO and EU have centers of excellence which focus on hybrid threats and strategic communications, it would be beneficial for both organizations if they collaborated on workshops, conferences, or research. Increasing joint communication efforts between NATO Stratcom COE and the EU Hybrid CoE is key in strengthening overall strategic communications. The newly announced membership of the Republic of North Macedonia is a unique situation to NATO due to its strategic location in the Balkans and influence in stabilization of the area. Because of its size and unstable government, the process of democratization can be hindered by Russia and its efforts to expand its spheres of influence. NATO and the EU should cooperate to establish an effective system to assist new member states in their successful transition into democracy and European integration.

NATO/EU Policy Recommendations

- Enhance cooperation of the EU and NATO in military exercises and communications to increase resilience and deter possible threats from Russia.
- Continue NATO Enhanced Forward Presence in the Baltics to maintain a strong deterrence posture.
- Improve threat analysis and risk assessment in the Baltics to ensure that each country is properly equipped to face its own security challenges.
- Encourage civilian resilience in response to Russian disinformation campaigns through media literacy.
- Implement and encourage more independent Russian and Baltic news sources to counter the increasing disinformation campaign attempts from Russia
- Establish joint efforts and formal communication links between NATO Stratcom COE and the EU's Hybrid CoE to strengthen the overall common strategic communications.
- Clearly define the mision of NATO StratCom COE and work to improve its strategic vision.
- Improve coordination of efforts between NATO and the EU to integrate Macedonia into European institutions.
- Improve information and resource sharing programs between NATO and the EU to deter future Russian threats.

Sources

“About." NIS. Accessed February 10, 2019. https://www.nis.eu/en/about-us/our-business/energy.

"About Us." STRATCOMCOE. Accessed January 29, 2019. https://www.stratcomcoe.org/about- us.

“About Strategic Communications.” STRATCOMCOE. Accessed January 28, 2019. https://www.stratcomcoe.org/about-strategic-communications/

“Advanced Persistent Threat Groups.” FireEye. Accessed February 01, 2019. https://www.fireeye.com/current-threats/apt-groups.html

Ali, Indrees. 2018. “Russia's Been Meddling with a US Ally in Europe, and Mattis Isn't Happy.” Business insider. September 17, 2018. https://www.businessinsider.com/russias-been-meddling-with-us-ally-macedonia-and-mattis-isnt-happy-2018-9?IR=T.

"Allied Air Command | NATO Air Policing". 2019. *Ac.Nato.Int*. https://ac.nato.int/page5931922/-nato-air-policing.

Alperovitch, Dmitri. “Bears in the Midst: Intrusion into the Democratic National Committee.” CrowdStrike. October 08, 2018. Accessed February 03, 2019 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Anastasakis, Othon. 2017. “Russia, South East Europe and the ‘Geopolitics of Opportunism’.” Clingendael Spectator 4 – 2017 (Vol.71) – Item 7 of 11. 2017. https://spectator.clingendael.org/pub/2017/4/russias-involvement/.

“At the 22nd Regular Session, the Resolution on the Protection of the Constitutional Order and the Proclamation of Military Neutrality Was Adopted.” NSRS, 18 Oct. 2017, www.narodnaskupstinars.net/?q=en/news/22nd-regular-session-resolution protection-constitutional-order-and-proclamation-military-neutrality-was-adopted.

Bajrović, Reuf, Vesko Garčević, and Richard Kraemer. Hanging By A Thread: Russia’s Strategy Of Destabilization In Montenegro. Foreign Policy Research Institute, 2018. https://www.fpri.org/wp-content/uploads/2018/07/kraemer-rfp5.pdf.

Bajrovic, Reuf; Richard Kraemer; and Emir Suljagic, "Bosnia on the Russian Chopping Block: The Potential for Violence and Steps to Prevent It." Foreign Policy Research Institute. March 2018 https://www.fpri.org/article/2018/03/bosnia russian-chopping-block-potential-violence-steps-prevent/.

Bieri, Matthias. 2015. “The Western Balkans Between Europe and Russia No. 170.” CSS Analyses in Security Policy. CSS. March 2015. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse170-EN.pdf.

Black, J. L. "Russia and NATO Expansion Eastward: Red-Lining the Baltic States." International Journal 54, no. 2 (1999): 249-66. doi:10.2307/40203375.

"Brussels Summit Declaration." NATO Official Text. July 11 12, 2018. Accessed July 02, 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-sumitdeclaration-eng.pdf.

Bump, Philip. “Here's the Public Evidence That Supports the Idea That Russia Interfered in the 2016 Election.” The Washington Post. July 06, 2017. Accessed February 02, 2019. https://www.washingtonpost.com/news/politics/wp/2017/07/06/heres-the-public-evidence-that-supports-the-idea-that-russia-interfered-in-the-2016-election/?utm_term=.3da6736cdc92.

Chen, Adrian. “The Agency,” New York Times. Accessed February 27, 2019. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0

"COMMISSION STAFF WORKING DOCUMENT: SERBIA 2007 PROGRESS REPORT." COMMISSION OF THE EUROPEAN COMMUNITIES SEC(2007), no. 1435 (November 6, 2007). https://ec.europa.eu/neighbourhoodenlargement/sites/near/files/pdf/key_documents/2007/nov/serbia_progress_reports_en.pf

“Commission." EEAS - European External Action Service. November 02, 2019. Accessed February 11, 2019. https://eeas.europa.eu/delegations/kosovo_en/1387/Kosovo and the EU.

“Communities of Interest.” Hybrid CoE. Accessed January 29, 2019. https://www.hybridcoe.fi/communities-of-interest/

"Congratulations for All Citizens of Both Countries for the Peace, Progress and Development That the Ratified Prespa Agreement Brings." Government of Republic of Macedonia. January 25, 2019. Accessed February 08, 2019. https://www.vlada.mk/node/16550?ln=en-gb.

Cooper, Helene, and Eric Schmitt. "U.S. Spycraft and Stealthy Diplomacy Expose Russian Subversion in a Key Balkans Vote." The New York Times. October 09, 2018. Accessed February 02, 2019. https://www.nytimes.com/2018/10/09/us/politics/russiamacedoniagreece.html?module=inline.

Crosby, Alan. 2019. “Now That NATO Door Is Open, North Macedonia Gets To Show That It Belongs.” RadioFreeEuropeRadioLiberty. February 7, 2019. https://www.rferl.org/a/macedonia-nato-russia-influence-greece-name change/29757662.html.

CrowdStrike Editorial Team. “Who Is Cozy Bear (APT29)?” CrowdStrike. June 07, 2018. Accessed February 10, 2019. https://www.crowdstrike.com/blog/who-is-cozy-bear/

"Cyber Defence." NATO. July 16, 2018. Accessed February 02, 2019. https://www.nato.int/cps/en/natohq/topics_78170.htm.

De Maio, Giovanna. Report. Istituto Affari Internazionali (IAI), 2016. http://www.jstor.org.offcampus.lib.washington.edu/stable/resrep09810.

Definition “BRUSSELS SUMMIT DECLARATION .” 2018. NATO . July 11, 2018. https://www.nato.int/nato.

Dempsey, Judy. "Russia's Gazprom Takes Control of Serbian Oil Monopoly." The New York Times. January 23, 2008. Accessed February 10, 2019. https://www.nytimes.com/2008/01/23/world/europe/23serbia.html.

"Deterrence And Defence". 2018. *NATO*. https://www.nato.int/cps/en/natohq/topics_133127.htm.

Erlanger, Steven, and Rick Gladstone. 2019. "With North Macedonia'S Inclusion, NATO Gets A Boost That Sends A Message". *Nytimes.Com*. https://www.nytimes.com/2019/02/06/world/europe/north-macedonia-nato russia.html?rref=collection%2Ftimestopic%2FMacedonia.

Estonian Foreign Intelligence Service. 2018. "International Security And Estonia 2018". Estonian Foreign Intelligence Service.

"EU-NATO Cooperation - Factsheet." 2018. EU-NATO cooperation Factsheet. November 22, 2018. https://eeas.europa.eu/headquarters/headquarters-homepage_en/28286/EU-NATO cooperation - Factsheet.

"EU And NATO Welcome Hybrid CoE." STRATCOMCOE. October 4, 2017. Accessed January 31, 2019. https://www.stratcomcoe.org/eu-and-nato-welcome-hybrid-coe.

European Schoolnet. 2017. "Lithuania: Country Report On ICT In Education". European Schoolnet. http://www.eun.org/documents/411753/839549/Country+Report+Lithuania+201 pdf/dd707697-196e-4c33-ba03-254f3698ea23.

European Union. "Action Plan Against Disinformation" 2018. EU Factsheet https://eeas.europa.eu/headquarters/headquarters-homepage/54831/action-plan-against-disinformtion_en

European Union. "A Europe that Protects: Countering Hybrid Threats" 2018. EU Factsheet. https://eeas.europa.eu/topics/economic-relations-connectivity innovation/46393/europe-protects-countering-hybrid-threats_en

European Union External Action. 2018. "Permanent Structured Cooperation - PESCO". Brussels: The European Union

"FAQ." STRATCOMCOE. Accessed January 29, 2019. https://www.stratcomcoe.org/faq.

"First, the Race of Formula 1, and Then Talks about Politics: Dodik Met with Putin in Sochi."

Telegraf RS, 01 October 2018.

Fridman, Ofer. "The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse." Defence Strategic Communications 2, no. 1 (2017): 61-86. Accessed January 27, 2019. doi:10.30966/2018.riga.2.3.

Galeotti, Mark. “Putin's Hydra: Inside Russia's Intelligence Services.” European Council on Foreign Relations. May 11, 2016. Accessed February 10, 2019. https://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intellige ce_services.

Gall, Carlotta. "Ukrainian Orthodox Christians Formally Break From Russia." The New York Times. January 06, 2019. Accessed February 11, 2019. https://www.nytimes.com/2019/01/06/world/europe/orthodox-church-ukraine russia.html.

Geciene-Janulione, Ingrida. “The Consequences of Perceived (In)Security and Possible Coping Strategies of Lithuanian People in the Context of External Military Threats”. Journal on Baltic Security. 2018.

Gerasimov, Valery. "The Value of Science Is Prediction. New Threats Demand Rethinking the Ways and Means of Conducting Warfare." Voenno-promyshlenniy Kurier, February 27, 2013. Accessed February 10, 2019. http://www.vpk-new.ru/articles/14632.

Gjorgjevski, Ivica. 2018. “Marshall Center – Republic of Macedonia at the Fourth ‘European Week – Days of Europe’ 2018.” Marshall Center-Republic of Macedonia Alumni Association. May 23, 2018. https://mcrm.org.mk/en/2018/05/23/marshall-center-republic-of-macedonia-at the-fourth-european-week-days-of-europe-2018/.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."Wired. December 07, 2018. Accessed February 11, 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed the-world/.

"Guiding Principles of the Contact Group for a Settlement of the Status of Kosovo." Kosovo Contact Group. Guiding principles of the Contact Group for a settlement

of the status of Kosovo.

Haass, Richard N. "The Age of Nonpolarity | Foreign Affairs." Foreign Affairs. 2008. Accessed February 10, 2019. https://www.foreignaffairs.com/articles/united states/2008-05-03/age-nonpolarity.

Higgins, Andrew. "As Ukraine and Russia Battle Over Orthodoxy, Schism Looms." The New York Times. December 31, 2018. Accessed February 11, 2019. https://www.nytimes.com/2018/12/31/world/europe/ukraine-russia-orthodox church schism.html.

Higgins, Andrew. "Concern over Why Bikers Linked to Putin Slipped into Balkan City." The Seattle Times. March 31, 2018. https://www.seattletimes.com/nationworld/concern-over-why-bikers-linked-to-putin-slipped-into-balkan-city/.

"How The Baltic States Resist Russia". 2019. *The Economist*. https://www.economist.com/europe/2019/02/02/how-the-baltic-states-resist-russia.

ICS.SANS. “Analysis of the Cyber Attack on the Ukrainian Power Grid”. March 18, 2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

“Instrument for Pre-Accession Assistance (IPA).” n.d. European Commission. Accessed February 19, 2019. https://ec.europa.eu/regional_policy/en/funding/ipa/.

Izhak, Oleksii. "The Threats and Challenges of a Multipolar World: A Ukraine Crisis Case Study." Connections 15, no. 1 (2016): 32-44. http://www.jstor.org.offcampus.lib.washington.edu/stable/26326427.

Jackevičius, Mindaugas and Samoškaitė, Eglė. 2012. "Apklausa: Realių Grėsmių Lietuvai Nėra, O Jei Bus – Mus Apgins NATO?". *DELFI*. https://www.delfi.lt/news/daily/lithuania/apklausa realiu-gresmiu-lietuvai nera-o-jeibus-mus-apgins-nato.d?id=60063003.

“Joint Press Point with NATO Secretary General Jens Stoltenberg and Foreign Minister Nikola Dimitrov.” 2019. NATO. February 6, 2019. https://www.nato.int/cps/en/natohq/opinions_163080.htm?selectedLocale=en.

Joubert, Vincent. “Five years after Estonia’s cyber attacks: lessons learned for NATO?” Published by: NATO Defense College (May. 1, 2012)

Kakissis, Joanna. "For Two Countries, The Dispute Over Macedonia's Name Is Rooted In National Identity." Npr. February 04, 2019. Accessed February 09, 2019 https://www.npr.org/sections/parallels/2018/02/04/582506402/for-two-countries the-disputeover-macedonias-name-is-rooted-innationalidentit?t=1549699601598.

Kaufman, Joyce P. NATO and the Former Yugoslavia: Crisis, Conflict, and the Atlantic Alliance. Rowman & Littlefield, 2002.

Kitfield, James. "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti." Breaking Defense. October 02, 2018. Accessed February 10, 2019. https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter russians-gen-scaparrotti/.

Kosovo* and the EU - EEAS - European External Action Service – European Commission." EEAS - European External Action Service. November 02, 2019. Accessed February 11, 2019. https://eeas.europa.eu/delegations/kosovo_en/1387/Kosovo and the EU.

L., Ronald. "Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." Homeland Security Digital Library. March 01, 2016. Accessed February 18, 2019.

"Lithuanian Contribution To Implementation Of The Common (European) Security And Defence Policy ". 2018. https://www.urm.lt/default/en/foreign-policy/lithuania-in-the-region-andthe-world/lithuanias-security-policy/-lithuanian-contribution-to-implementation of-the-european-security-and-defence-policy.

“Macedonia.” n.d. U.S. Department of State. Accessed February 20, 2019. https://www.state.gov/j/inl/regions/europeasia/219024.htm.

Mankoff, Jeffrey. 2017. “How to Fix the Western Balkans.” Foreign Affairs. July 7, 2017. https://www.foreignaffairs.com/articles/southeastern-europe/2017-07-07/how-fix-wester-balkans.

Maza, Cristina. “Vladimir Putin Travels to the Balkans to Push against NATO Membership, Slams U.S. Interference.” Newsweek, 17 Jan. 2019, www.newsweek.com/russia-vladimir-putin-travels-balkans-push-against-nato membership-slams-us-1294734.

Meeting with President Of Republika Srpska Entity Of Bosnia And Herzegovina Milorad Dodik. President Of Russia. September 30, 2018. http://en.kremlin.ru/events/president/news/58662

"Meeting of Russian Federation Ambassadors and Permanent Envoys." News release, June 30, 2016. President of Russia. Accessed February 7, 2019. http://en.kremlin.ru/events/president/news/52298.

Meister, Stefan. "The "Lisa Case": Germany as a Target of Russian Disinformation." *NATOReview Magazine*. Accessed February 6, 2019. https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target russian-disinformation/EN/index.htm.

Milojević, Milorad, Azra Memišević, and Bruce Clezy. "Media Landscape in Republika Srpska: Polarization and Financial Dependence." Balkan Diskurs. May 31, 2018. https://balkandiskurs.com/en/2018/05/25/media-landscape-republika-srpska/.

Ministry of National Defense of the Republic of Lithuania. “Agreement on Lithuanian Defense Policy Guidelines”. 2018. Vilnius. Lithuanian Defense Ministry.

Ministry of National Defense of the Republic of Lithuania, “Lithuanian Defense System: Facts and Trends”. 2018. Vilnius. Lithuanian Defense Ministry.

Mironova, Vera, and Bogdan Zawadewicz. "Putin Is Building a Bosnian Paramilitary Force." Foreign Policy. August 08, 2018. https://foreignpolicy.com/2018/08/08/putin-is-building-a-bosnian-paramilitary force/.

Missiroli, Antonio, Jan Joel Andersson, Florence Gaub, Nicu Popescu, and John Joseph Wilkins. *Strategic Communications - East and South.* Report. July 29, 2016. https://www.iss.europa.eu/content/strategic-communications-–-east-and-south.

NATO, “Boosting NATO’s presence in the East and Southeast” NATO Topics.

NATO. "Brussels Summit Declaration". 2018. https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21.

NATO. "Doorstep Statement." News release, February/March, 2017. NATO. Accessed February, 2019. https://www.nato.int/cps/en/natohq/opinions_141621.htm.

NATO. 2018. “Joint Declaration on EU-NATO Cooperation”. https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en

Nato. "Joint Press Conference with NATO Secretary General Jens Stoltenberg and the Chairman of the Tri-Presidency of Bosnia and Herzegovina, Mladen Ivanić." NATO. 02 Feb. 2017 https://www.nato.int/cps/ie/natohq/opinions_140549.htm?selectedLocale=en.

NATO, “NATO’s Enhanced Forward Presence”, NATO Factsheet. 2018. www.nato.int/factsheets

NATO. “NATO – EU Relations” 2018. NATO Factsheets. www.nato.int/factsheets

NATO. “NATO Cyber Defense” 2019. NATO Factsheets. www.nato.int/factsheets

NATO. NATO-Russia Relations: The Facts. September 07, 2018. Accessed February 02, 2019. https://www.nato.int/cps/en/natolive/topics_111767.htm.

NATO. “NATO’s Readiness Action Plan” NATO Factsheet. 2016. www.nato.int/factsheets

Nato. "NATO's Role in Kosovo." NATO. Accessed February 10,2019. https://www.nato.int/cps/en/natolive/topics_48818.htm.

Nato. "Statement by the NATO Secretary General on the Adoption of the Laws on the Transition of the Kosovo Security Force." NATO. Accessed February 11, 2019. https://www.nato.int/cps/en/natohq/news_161631.htm?selectedLocale=en.

Nato. "The Situation in and around Kosovo - Statement Issued at the Extraordinary Ministerial Meeting of the North Atlantic Council..." NATO. Accessed February

10, 2019.
https://www.nato.int/cps/en/natohq/official_texts_27435.htm?selectedLocale=en

“NATO." The New York Times. December 14, 2018. Accessed February 11, 2019.
https://www.nytimes.com/2018/12/14/world/europe/kosovo-army-serbia nato.html.

NATO. "Resilience and Article 3." Resilience and Article 3. June 25, 2018. Accessed February 02, 2019.
https://www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=en.

NATO Strategic Communications Centre of Excellence. "Russia's Footprint In The Nordic- Baltic Information Environment". 2016. Riga. NATO Strategic Communications Centre of Excellence.

"NATO’S Response To Hybrid Threats". 2018. *NATO*.
https://www.nato.int/cps/en/natohq/topics_156338.htm.

"NATO-Russia Relations: The Background." NATO. April 2018. Accessed February 26, 2019.
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_04/20180426_180 NATO-Russia_en.pdf.

"New Wave of Cyberattacks against Ukrainian Power Industry." WeLive Security. January 21, 2016. Accessed February 11, 2019.
https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power industry/.

New York Times. January 23, 2008. Accessed February 10, 2019.
https://www.nytimes.com/2008/01/23/world/europe/23serbia.html.

Newman, Lily Hay. “Hacker Lexicon: what is the attribution problem?” Wired. June 03, 2017. Accessed February 02, 2019.
https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

NOPETYA TECHNICAL ANALYSIS LogRhythm Labs. July 2017.
https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical analysis-logrhythm-labs-threat-intelligence-report.pdf

O'Flaherty, Kate. "Midterm Election Hacking -- Who Is Fancy Bear?" Forbes. August 23, 2018. Accessed February 08, 2019. https://www.forbes.com/sites/kateoflahertyuk/2018/08/23/midterm-election hacking-who-is-fancy-bear/#18da2cdd2325.

“Opening Remarks.” 2019. NATO. February 6, 2019. https://www.nato.int/cps/en/natohq/opinions_163075.htm?selectedLocale=en.

"Osborn, Andrew. ""Ukraine Introduces Martial Law Citing Threat of Russian Invasion."" Reuters. November 27, 2018. Accessed February 11, 2019. https://www.reuters.com/article/us-ukraine-crisis-russia/ukraine-introduces martial-law-citing-threat-of-russian-invasion-idUSKCN1NV0N1.

"Partners." NATO. November 11, 2015. Accessed January 29, 2019. https://www.nato.int/cps/en/natohq/51288.htm.

Pio. "About EULEX." EULEX Report to the UN - EULEX Kosovo. Accessed February 11, 2019. https://www.eulex-kosovo.eu/?page=2,60.

Ramani, Samuel. "Why Serbia Is Strengthening Its Alliance with Russia." The Huffington Post. February 12, 2017. Accessed February 11, 2019. https://www.huffingtonpost.com/samuel-ramani/why-russia-is-tightening _b_9218306.html.

Ray, Michael. "Ukraine Crisis." Encyclopædia Britannica. May 26, 2017. Accessed February 01, 2019. https://www.britannica.com/topic/Ukraine-crisis.

Relations with the European Union.” 2019. NATO. February 15, 2019. https://www.nato.int/cps/en/natohq/topics_49217.htm?selectedLocale=en.

“Relations with the Republic of North Macedonia.” n.d. NATO. Accessed February 15, 2019. https://www.nato.int/cps/en/natohq/topics_48830.htm.

“Relations with Russia.” 2019. NATO . February 4, 2019. https://www.nato.int/cps/en/natolive/topics_50090.htm.

"Relations with Ukraine." NATO. June 14, 2018. Accessed February 11, 2019. https://www.nato.int/cps/en/natolive/topics_37750.htm.

“Resolution Against NATO Membership By Bosnian Serbs.” Bosnia & Herzegovina, www.oscebih.org/resolution-against-nato-membership-by-bosnian-serbs.

Rfe/rl, Russian Service, and Rfe/rl. "Putin Blasts Kyiv For 'Blatant Interference' In Orthodox Church." RadioFreeEurope/RadioLiberty. January 31, 2019. Accessed February 01, 2019. https://www.rferl.org/a/putin-blasts-kyiv-for-blatant-interference-in-orthodox-church/29744338.html.

RL, RFL. "Denmark, Sweden, Switzerland Give $14 Million To UN Aid For Eastern Ukraine." Radio Free Europe Radio Library. February 09, 2019. Accessed February 10, 2019.https://www.rferl.org/a/denmark-sweden-switzerland-give-14 million-to-un-aid-for-eastrnukraine/29760738.html.

“RS President Receives Award in Moscow "" B92.net. 12 March 2014 https://www.b92.net/eng/news/region.php?yyyy=2014&mm=03&dd=12&nav_id=9607

“RS President Wants Russian Media Reach Increased in Bosnia.” N1 BA, 25 May 2018, ba.n1info.com/English/NEWS/a262683/RS-President-wants-Russian-media reach-increased-in-Bosnia.html.

"Russia against Dragging Bosnia and Herzegovina into NATO, Says Russian UN Envoy." TASS., 6 Nov. 2018. http://tass.com/world/1029532.

"Russia's Been Meddling with a US Ally in Europe, and Mattis Isn't Happy." April 17, 2018. Accessed February 13, 2019. https://www.businessinsider.com/russias-been-meddling-with-us-ally-macedonia-and-mattis-isnt-happy-2018-9?IR=T

Russian Economic Footprint in Serbia Policy Brief No. 72." Center for the Study of Democracy 72 (2018). doi:10.6027/anp2018-832.

“Russia, Ukraine, and the Orthodox Church,” Council on Foreign Relations, 30-Oct 2018. Accessed February 26, 2019. https://www.cfr.org/conference-calls/russia-ukraine-and-orthodox-church.

Ruhle, Michael. “Deterrence: What it Can and Cannot Do” NATO Review Magazine. https://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia military/en/index.html

Samoskaite, Egle. 2015. "Rusijos Grėsmė Privertė Suprasti Nemalonią Tiesą". *DELFI*. https://www.delfi.lt/news/daily/lithuania/rusijos-gresme-priverte-suprasti nemalonia-tiesa.d?id=66883848.

Schultz, Teri. "Why the 'fake Rape' Story against German NATO Forces Fell Flat in Lithuania." *DW*, February 23, 2017. Accessed February 6, 2019. https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell flat-in lithuania/a-37694870.

Seldin, Jeff. 2018. “Russia Influence Operations Taking Aim at US Military.” VOV. November 2, 2018. https://www.voanews.com/a/russia-influence-operations-taking-aim-at-us military/4640751.html?fbclid=IwAR0pRrpCxrrCpsj79Nt3DknTy5xLlL3JAJNHQi-dCHpNDnhg50GLNp_wVNo.

"Serbia Caught between Two Chairs? Does Serbia Want to Be Part of the Russian Sphere of Influence or Join the European Union?" Heinrich Böll Stiftung Serbia, Montenegro, Kosovo. Accessed February 11, 2019. https://rs.boell.org/en/2014/12/10/serbia-caught-between-two-chairs-does-serbia want-be-part-russian-sphere-influence-or.

Schaart, Eline. “Lavrov: Russia Keeps Door Open for Talks with US to Save INF Treaty.” POLITICO, 16 Jan. 2019, www.politico.eu/article/nuclear-sergei-lavrov russia-keeps-door-open-for-talks-with-united-states-to-save-inf-treaty/.

Schneier, Bruce. “Why Proving Source of a Cyberattack Is so Damn Difficult.” CNN. January 06, 2017. Accessed February 01, 2019 https://edition.cnn.com/2017/01/05/opinions/proving-source-of-dnc-hacks difficult-opinion-schneier/index.html.

Seals, Tara. "APT29 Re-Emerges After 2 Years with Widespread Espionage Campaign." The First Stop for Security News. November 20, 2018. Accessed February 10, 2019. https://threatpost.com/apt29-re-emerges-after-2-years-with-widespread-espionage-campaign/139246/.

Sito-Sucic, Daria. “NATO's Planned Balkan Expansion a 'Provocation': Russia's Lavrov.” Reuters, Thomson Reuters, 29 Sept. 2014, www.reuters.com/article/us-nato-balkans-russia-idUSKCN0HO11W20140929.

Skroupa, Christopher P. “No Bit Sherlock—The Role of Forensics In Tracing The DNC Hack.” Forbes. Accessed February 2, 2019. https://www.crai.com/sites/default/files/publications/FORBES_The-role-of forensics-in-tracing-the-DNC-Hack.pdf

Sotirovic, Vladislav B. 2019. “The Geopolitics Of South-East Europe And Importance Of The Regional Geostrategic Position (I).” OrientalReview.Org. February 20, 2019. https://orientalreview.org/2019/02/20/the-geopolitics-of-south-east-europe-and importance-of-the-regional-geostrategic-position-i/.

Squires, Nick. “Russia 'Orchestrating Covert Campaign to Wreck Macedonia Name Change Vote' .” The Telegraph, Telegraph Media Group, 27 Sept. 2018, www.telegraph.co.uk/news/2018/09/27/russia-orchestrating-covert-campaign wreck-macedonia-name-change/.

Stanev, Yoan. 2018. “Macedonia Seeks Funding for Regional Infrastructure Projects.” EMERGINGEUROPE The Gateway to the Region. July 14, 2018. https://emergingeurope.com/news/macedonia-seeks-funding-for-regional-infrastructure-projects/.

State Security Department of the Republic of Lithuania, National Threat Assessment 2018, (Vilnius, 2018)

Stokel-Walker, Chris. “Hunting the DNC Hackers: How Crowdstrike Found Proof Russia Hacked the Democrats.” Wired. September 28, 2017. Accessed February 02, 2019. https://www.wired.co.uk/article/dnc-hack-proof-russia-democrats.

Strohm, Chris. "U.S. Says It Will Alert Public to Foreign Influence Operations." Bloomberg. July 20, 2018. Accessed February 05, 2019. https://www.bloombergquint.com/business/australia-bank-ceos-face-day-of-reckoningforyears-of-scandals.

Studzińska, Zofia. "How Russia, Step by Step, Wants to Regain an Imperial Role in the Global and European Security System." Connections 14, no. 4 (2015): 21-42. http://www.jstor.org/stable/26326416.

Surk, Barbara. "Kosovo Parliament Votes to Create an Army, Defying Serbia and NATO." The New York Times. December 14, 2018. Accessed February 11, 2019. https://www.nytimes.com/2018/12/14/world/europe/kosovo-army-serbia nato.html.

Taylor, Adam. "To Understand Crimea, Take a Look Back at Its Complicated History." The Washington Post. February 27, 2014. Accessed February 11, 2019. https://www.washingtonpost.com/news/worldviews/wp/2014/02/27/to-understand-crimea-take-a-look-back-at-its-complicated-history/?utm_term=.88d37cb08f2b.

Taylor, Adam. "That Time Ukraine Tried to Join NATO - and NATO Said No." The Washington Post. September 04, 2014. Accessed February 11, 2019. https://www.washingtonpost.com/news/worldviews/wp/2014/09/04/that-time-ukraine-tried-to-join-nato-and-nato-said-no/?utm_term=.f3696fc6133f.

Telegraf.rs. "From KLA, over the Kosovo Protection Corps, Kosovo Security Force, and Then to "army": Development of Terrorism on Kosovo." Telegraf – Najnovije Vesti. December 14, 2018. Accessed February 11, 2019. https://www.telegraf.rs/english/3015810-from-kla-over-the-kosovo-protection corps-kosovo-security-force-and-then-to-army-development-of-terrorism-on kosovo.

“The Ecumenical Throne and the Church of Ukraine." The Ecumenical Patriarchate. September 18, 2018. Accessed February 11, 2019.

“The Future of the Transatlantic Alliance.” 2019. NATO. January 19, 2019. https://www.nato.int/cps/en/natohq/opinions_162650.htm?selectedLocale=en.

“The Riga StratCom Dialogue 2018.” STRATCOMCOE. Accessed February 21, 2019. https://www.stratcomcoe.org/riga-stratcom-dialogue-2018

Thomas, Timothy. "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations." Defence Strategic Communications 1, no. 1 (2015)

Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December

2017. Report. June 8, 2018. Accessed January 29, 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_18008-3rd Joint-progress-report-EU-NATO-eng.pdf.

“Western Balkans.” n.d. European Commission. Accessed February 19, 2019. http://ec.europa.eu/trade/policy/countries-and-regions/regions/western-balkans/.

"Who We Are." Accessed February 10, 2019. https://www.osce.org/whatistheosce.

"What Is Hybrid CoE?" Hybrid CoE. Accessed January 29, 2019. https://www.hybridcoe.fi/whatis-hybridcoe/.

“Why Is Kosovo so Important for Serbs.” Accessed February 13, 2019. http://www.ptt.rs/korisnici/i/v/ivstar/quickhistory.htm.

Wiktorek Sarlo, Alexandra. 2019. "Fighting Disinformation In The Baltic States – Foreign Policy Research Institute". Foreign Policy Research Institute. https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.

Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'." Wired. June 04, 2017. Accessed February 11, 2019. https://www.wired.com/2013/03/stuxnet-act-of-force/.

Zhurzhenko, Tatiana. "A Divided Nation? Reconsidering the Role of Identity Politics in the Ukraine Crisis." Die Friedens-Warte 89, no. 1/2 (2014): 249-67. http://www.jstor.org.offcampus.lib.washington.edu/stable/24868495.