JUNE 2017

CAPSTONE

RUSSIAN HYBRID WARFARE

BARBER, VICTORIA
KOCH, ANDREW
NEUBERGER, KAITLYN

CAPSTONE PROJECT PREPARED FOR
UNITED STATES SPECIAL OPERATIONS COMMAND

This report was written to satisfy part of the degree requirements for the Masters of Arts in Law and Diplomacy at the Fletcher School of Law and Diplomacy at Tufts University. The contents of this paper do not necessarily reflect the official policy of the U.S. Government, the Department of Defense, or any of its agencies.

This research was originally completed and presented in April 2016. During preparation for formal publication, some information was updated based on events, but there may be other, more recent events or information that is not wholly reflected in this report. However, the underlying analysis of Russian hybrid warfare and the historical studies remain consistent and relevant.

Table of Contents

Part I: Hybrid Warfare

Figures

Tables

Preface

In the fall of 2014, Joint Special Operations University (JSOU) began an initiative to circulate external research projects that are of interest to the enterprise. This report is a capstone research project undertaken by a small team of graduate students fulfilling their graduate research requirement in the International Security Studies Program at the Fletcher School of Law and Diplomacy at Tufts University. The culmination of their research, *Russian Hybrid Warfare*, was presented to senior leaders and staff representatives at United States Special Operations Command (USSOCOM) during April 2016. *Note:* For information on outreach efforts to external universities or access to other papers or projects, contact jsou_research@socom.mil and include "Outreach" in the subject line.

The purpose of the research project was to provide a comprehensive review of the emerging threat of hybrid warfare, with a particular focus on the use of hybrid tactics by Russia against those states that were part of the former Soviet Union and contain what Moscow describes as having "near-abroad" Russian populations. The objective of the study was to examine the extent to which hybrid warfare represents the future of interstate conflict and the ramifications of Russian hybrid warfare against these states for NATO, the U.S. government, and particularly USSOCOM. The students presented three historical cases and one fictional, but plausible, scenario, which will be of benefit to wargame events.

USSOCOM was not the students' first travel opportunity. Through Tufts University–sponsored travel, the team conducted their research and interviewed experts during visits to Special Operations Command, Europe (Stuttgart-Vaihingen, Germany), as well as Latvia, Estonia, and Lithuania during their semester-long effort. Admiral (retired) James Stavridis, the former Supreme Allied Commander - NATO Forces and now Dean of the Fletcher School, was a special advisor to the student group on hybrid warfare implications for NATO. Mr. Will Irwin, a JSOU Resident Senior Fellow and author, met the student research team during two in-progress review sessions and provided recommendations and guidance for their project. Dr. Richard Shultz, Director of the International Security Studies Program at the Fletcher School and a JSOU Senior Fellow, was the research team's mentor and accompanied the group for their briefing at USSOCOM.

In the pages that follow, the reader will find a thorough review of the threat of hybrid warfare paired with nine specific recommendations for Special Operations Forces (SOF) and USSOCOM.

Part I

Hybrid Warfare

Introduction

On 17 March 2014, the Crimean Parliament formally declared independence from the Ukraine and, in the same breath, asked to join the Russian Federation. This came just a day after a sizeable majority of Crimeans voted to leave Ukraine.[1] The same day as the Crimean Parliamentary decision, Russian Federation President Vladimir Putin signed a decree recognizing the independence of the Crimea and paving the way for the Russian Duma to vote on annexation in the following days.[2] Two days later, on 20 March 2014, the Russian Federation began the process of annexation for the Crimean Peninsula with a vote in the lower house of the Duma.[3] The annexation was finalized when Putin signed the order the following day.[4] The annexation capped off months of crisis in the Ukraine and scheming in the Kremlin, and marked the end of a major chapter in recent Russian activity in Ukraine. It also demonstrated to many the power of a 'new' type of warfare that incorporated both conventional military forces as well as irregular activities and non-violent means to reach a political goal. While this type of warfare has been referred to by many terms within the literature,[5] in order to describe it, we will use the phrase 'hybrid warfare.'

The purpose of this project is to provide an overview of the components of hybrid warfare, their use by the Russian Federation, and ways these components can be mitigated by actions taken by the United States Special Operations Command (USSOCOM) and the United States Government (USG) as a whole.

The first part of this project provides an overview of hybrid warfare. We will start with a discussion of what hybrid warfare is and whether or not it is new. We will follow this discussion with a review of its major components. For each one we will describe the component, provide principles around which it is used in warfare, and, finally, describe how the Russian Federation is using or has used that component in its current and recent operations in its near-abroad. We will follow this discussion with our proposed theoretical framework for understanding and combatting hybrid warfare and its techniques, based upon the Netwar theory, which we believe is the most effective way to understand the problem of hybrid warfare.

In the second part of this paper, we will review two cases of Russian use of hybrid warfare techniques as well as one case of hybrid warfare used by another international actor: China. In the first case, we will examine the Russian annexation of the Crimean Peninsula. In the second case, we will explore the 2007 cyber attack on Estonia. In the third case, we will look at the tactics and consequences of China's actions in the South China Sea. In each of these cases, we will provide background information, describe the components used by the aggressing actor, explain how these actions integrate into the Netwar theory, and describe the responses given by members of the international community to these aggressive actions. Finally, we will walk through a stylized case of our own creation. This case will look specifically at how the Russian Federation might use hybrid warfare against a North Atlantic Treaty Organization (NATO) member in the future.

Following the review of hybrid warfare, its component parts, and a discussion of four case studies, we will provide several recommendations for the European Union (EU), NATO, USG, and USSOCOM. These recommendations will focus on steps that these actors can and should take to effectively mitigate the effects of hybrid warfare techniques. These recommendations have been derived through academic research, phone conversations with academics and practitioners, and on-the-ground interviews with individuals and officials from the three Baltic republics—Estonia, Latvia, and Lithuania—as well as U.S. military personnel in Stuttgart, Germany.

What Is Hybrid Warfare?

While it could be argued that the use of hybrid warfare has been around for centuries, the phrase 'hybrid warfare' is a relatively new phenomenon. The phrase was first used by Frank Hoffman in a 2007 report commissioned by the Potomac Institute for Policy Studies, "Conflict in the 21st Century: The Rise of Hybrid Wars." In this report, Hoffman outlines the future of warfare and defines hybrid warfare/threats as:

> Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict. The effects can be gained at all levels of war.[6]

Hoffman then defines three principles of this new type of warfare. First, the warfare must be "omni-directional," meaning that "commanders observe a potential battlefield without mental preconditions or blind spots"[7] and that "[a]ll traditional domains, (ground, seas, air, and outer space) as well as politics, economics, culture, and moral factors are to be considered battlefields."[8] Second, hybrid warfare must have "synchrony," meaning that commanders should "link the disaggregated nature of multiple battlefields in different domains with consideration of the temporal dimension."[9] Finally, hybrid warfare must have "asymmetry." While Hoffman recognizes that asymmetry exists in almost every type of warfare, he also notes that in this new type of warfare, the "spectrum for overlooking the normal rules is much wider."[10]

Hoffman notes that celebrated Marine General Charles Krulak stated in 1996[11] that "[O]ur enemies will not allow us to fight the son of Desert Storm, but they will try to draw us into the stepchild of Chechnya."[12] With this statement, Hoffman supports his view that conventional wars are not the wars of the future. However, despite Krulak's assertion that the war in Chechnya was a precursor to the new era of war, Hoffman did not use Chechnya as an example of hybrid warfare. Instead Hoffman cites Lebanese Hezbollah's actions against Israel during the 2006 war in southern Lebanon as a prime example of this "new" type of warfare.[13] He states specifically that the summer 2006 war is "the clearest example of a modern hybrid challenger."[14] Hoffman goes on to state:

> The amorphous Hezbollah is representative of the rising hybrid threat. This battle in southern Lebanon reveals significant weaknesses in the posture of the Israeli defense force … Mixing an organized political movement with decentralized cells employing adaptive tactics in ungoverned zones, Hezbollah showed that it could inflict as well as take punishment. Its highly disciplined, well trained, distributed cells contested ground and wills against a modern conventional force using an admixture of guerrilla tactics and technology in densely packed urban centers.[15]

Hoffman also argues that this new type of warfare will fundamentally challenge the United States government and military. He writes:

> Hybrid Warfare presents a mode of conflict that severely challenges America's conventional military thinking. It targets the strategic cultural weaknesses of the American Way of Battle quite effectively. Its chief characteristics—convergence and combinations—occur in several modes. The convergence of various types of conflict will present us with a complex puzzle until the necessary adaptation occurs intellectually and institutionally.[16]

To simplify Hoffman's far ranging definition and to build upon his example of the 2006 war, we can think of hybrid warfare as a coordinated combination of regular and irregular tactics conducted by a state or non-state actor designed to accomplish a specific political goal. Throughout the remainder of this project we will use this simplified version of Hoffman's definition to describe hybrid warfare.

Is Hybrid Warfare New?

The question over whether or not hybrid warfare is new has continued to be a topic of conversation since Hoffman's piece introduced the new phrase. Hoffman spends several sections of his article explaining where other theories of new-generation warfare, such as compound warfare and fourth-generation warfare, somewhat explain his new conception of warfare, but not entirely.[17] Thus, he concedes that his conception is not completely new, but instead a combination of other new warfare theories. Since publishing this piece, Hoffman has further clarified his view on the novelty of hybrid warfare by stating clearly that he does not view hybrid warfare as new, just different.[18] Thus, the majority of voices claiming that hybrid warfare is new are coming from the media and some policy makers who either do not have the background or are playing into fears of a new type of warfare. Most academics and practitioners recognize that this is not a new form of warfare. In the following section, we focus on examples that show hybrid warfare is not a new concept. We will also provide an analysis and framework for why some believe that hybrid warfare is a new concept.

Hybrid Warfare Is Not New

Academics and most practitioners recognize that hybrid warfare is not a new concept. In fact, Lieutenant General Riho Terras, the Chief of Defense for the Estonian armed forces stated in no uncertain terms that "hybrid warfare is not anything new" during a meeting in Boston on 18 November 2015.[19] Likewise, in her article for the German Marshall Fund, leading Estonian defense thinker Merle Maigre writes a clear rebuke of the notion that hybrid warfare is new by specifically focusing on Russian activities over history. She writes:

> The concept of "hybrid warfare" goes back far beyond a decade, with military history including numerous examples of a combination of regular and irregular forms of warfare. The ancient Chinese philosopher Sun Tzu celebrated war as the art of cunning. In the 1920s, the Soviet military developed a concept of "masked warfare" (maskirovka), which included various active and passive measures designed to deceive the enemy and influence the opinion-making process in the West. The notorious Soviet intelligence official Pavel Sudoplatov, who served in

> the KGB for over 50 years, recalled how the Soviet intelligence's secretive Administration for Special Tasks was responsible for kidnapping, assassination, sabotage, and guerrilla warfare, and how it set up networks during World War II in the United States and Western Europe. The Soviet invasion in Afghanistan in 1979 began with hybrid tactics when 700 Soviet troops dressed in Afghan uniforms seized key military and administrative buildings in Kabul.[20]

It is not just Estonians writing and talking about the history of hybrid warfare. A NATO General Report on the topic of hybrid warfare stated: "Hybrid tactics as used by Russia are not inherently anything new for the Alliance. The Soviet Union often sought to manipulate domestic issues inside of NATO member states creating grey zones of ambiguity surrounding the degree of its involvement."[21] However, the NATO report goes on to say that the goals of the deployment of these techniques are different. It states: "A key difference, however, between Soviet and today's Russia's use of hybrid tactics is that, while the Soviets used them primarily to soften their opponents, President Putin seems to be using them as a means of achieving his objectives of a politically restructured Europe."[22]

There are also scholars from the United States who point out very clearly and strongly that hybrid warfare is not new. In a piece for the Wilson Center's Kennan Institute, Michael Kofman and Matthew Rojansky wrote:

> The first part of the misconception around "hybrid war" is the term itself. Despite sounding new and in vogue, its analytical utility is limited. The "hybrid" aspect of the term simply denotes a combination of previously defined types of warfare, whether conventional, irregular, political or information. Even those who have put forward such a definition must admit that the combination of war across domains is not new, but in fact is as old as warfare itself. It is helpful to think beyond the contemporary definitions of war we have become accustomed to, but the term is inherently imprecise, and does not describe a new form of warfare.[23]

Kofman and Rojansky go on to say:

> From the Russian perspective, an approach to war that combines different types of power projection also is not itself reflective of any newly devised strategy. Rather, it is an illustration or acknowledgement by Russia of a growing trend in how wars are fought, whoever may be fighting them. Modern wars, simply put, are waged through a combination of many elements of national power. In Washington, this conventional wisdom has long been characterized by the beltway catchphrase of "using all the tools in the toolkit," or the more recent mantra of using "smart power." The "hybrid" concept is well established in modern Western military discourse today, while the problem set it seeks to define is not novel, but rather has been cited frequently under concepts of "unconventional" warfare and "political" warfare.[24]

It is not just the Russians who have used hybrid warfare techniques in the past. As Alex Deep writes in his article for the *Small Wars Journal*:

> This blending has historic examples in the American Revolution with George Washington's Continental Army and robust militia forces; the Napoleonic Wars where British regulars challenged French control of major Spanish cities, while Spanish guerrillas attacked their lines of communication; and the Arab Revolt where the British Army combined conventional operations in Palestine with irregular forces under British operational control.[25]

The sections of text above show the extent to which this topic of "new-ness" has been debated, discussed, and been found wanting. From our research, academics and practitioners clearly share this belief, but many also make the point that while the concept might not be new, some of the techniques and enabling technology are different and must be addressed.[26] Because of the potency of the combination of multiple elements of national power and new enabling technology, we believe that the use of hybrid warfare is a significant threat to America and its allies. Thus, the threat needs to be addressed through a variety of mechanisms. We believe that the pieces for a successful defense are already in our arsenal, but we must deploy them effectively. These mechanisms and pieces will be discussed in detail in future sections of this project.

Despite the indication that hybrid warfare is not a new technique, there is a clear strain of thinking and activism from practitioners, policy makers, and the media who advocate that this is a new phenomenon and should be treated as such. In the following section, we will provide an analytical framework which helps explain why so many view hybrid warfare as a new phenomenon.

Why Do Some Believe That Hybrid Warfare Is New?

As the previous section indicates, despite clear evidence that hybrid warfare is not a new phenomenon, many still believe that it is and are acting on this belief. Professor Daniel Drezner of The Fletcher School of Law and Diplomacy at Tufts University created a three-point framework to explain why so many believe hybrid warfare is new.[27]

First, Drezner shows that conventional military warfare has fallen off significantly from its high water mark during the 1900s. Thus, despite there actually being very few examples of hybrid warfare, relative to interstate military conflict, the increase in hybrid warfare looks astronomical.[28] In fact, Drezner points out that this excitement over a "massive" increase in a "new" type of war has happened before. He cites the 1990s and the thinking that civil wars and internal wars were increasing at a rapid pace. However, if we look at the data, we see that while there was an increase in civil wars and internal wars during this period, this increase was magnified by the significant decrease in the number of interstate wars (see Figure 1).[29] Thus, one element that is driving the view that hybrid warfare is a new phenomenon is that, relative to our traditional conception of warfare (i.e., interstate war), there has been a significant increase in hybrid wars.

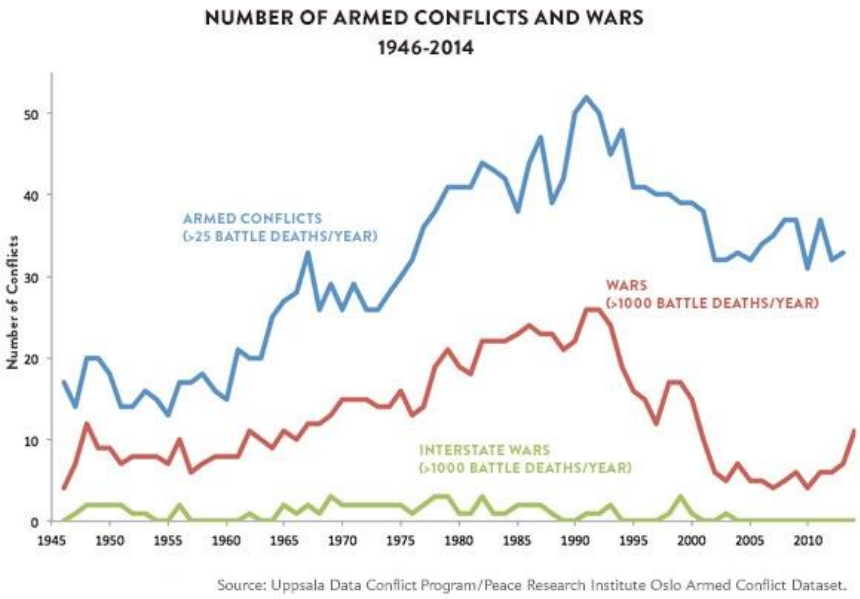

Figure 1: Graph showing the rise of internal wars and armed conflicts and fall of interstate conflicts from the mid-20th to the early 21st centuries[30]

Second, Drezner talks about the increase in technology and its impact on warfare.[31] The interconnectedness that technology has facilitated throughout the world has given actors the ability to use hybrid warfare tactics and remain covert. Attribution was much easier when tank columns were rolling over borders, but this new ability to remain covert through technology has made attribution much harder. The blindness that hybrid techniques using technology create, establishes a feeling of novelty for policy makers and commentators.

Finally, Drezner identifies one of the biggest sticking points: regulation of hybrid warfare and its component parts is nearly impossible.[32] As a society built on the idea of rule of law, the Westphalian system of sovereignty, and the Geneva Conventions that govern warfare, we look to norms to provide some type of regulation during conflicts. But, as Drezner points out, in order to regulate this sort of warfare, one would have to regulate lying, because deceit is at the heart of most, if not all, hybrid warfare actions. Because of this problem, there would be no way to monitor or enforce any regulations if they were created.[33]

Components of Hybrid Warfare

Keeping the simplified definition of hybrid warfare in mind, we will now define and describe the key components or 'nodes' of hybrid warfare. Because of the nature of hybrid warfare and its inherent flexibility, we would be remiss in saying that we have covered everything; however, these sections should provide an overview of the most important components of the hybrid warfare strategy. These sections will also provide information on how the Russian government is currently using or has used these components to accomplish political goals in its near-abroad.

Covert Action: The Overarching Component

When people think of covert action, some immediately jump to spies making a 'dead-drop' on a foggy bridge in the old Soviet Union, while others think of a special operations forces (SOF) team launching a raid to capture or kill a foreign target. By pure popularity, perhaps the most famous purveyor of covert action is the fictional character James Bond from Ian Fleming's novels and the movies based on them. Regardless of the lens through which someone views covert action, the importance of covert action to state interaction throughout history cannot be understated. Covert action has been taking place among countries and non-state actors for centuries. Nations have risen and fallen, in part, through actions taken in secret. It is this impact that makes covert action, and its various components, an integral part of hybrid warfare strategy. It is these covert actions that, in many cases, are combined with or lead to broader military, political, and diplomatic actions in support of a governmental goal. While much of the literature discussed below focuses on Western—specifically American—conceptions of covert action, the similarities in how countries think about covert action allows for parallels to be drawn regarding definitions, purposes, and principles of covert action programs.

Definition of Covert Action

While the United States and other countries use covert action in a variety of ways, there is a common definition that encompasses the spirit of these actions. This definition is provided by the USG in section 503(e) of the National Security Act of 1947. The Act defines covert action as: "[a]n activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[34] Simply replace the phrase "United States Government" with the government of any nation and you would find something similar in their approach to these activities. The key statement in the definition is: "the role of [insert country here] will not be apparent or acknowledged publicly."[35] Covert action must be secret to be effective. The USG maintains the idea that an activity must have 'plausible deniability' for it to maintain its secrecy and ensure the effective implementation of the action.[36] This concept has become harder to ensure with the advent of improved communications technology and a more decentralized press. Because of these changes, even if countries go to great lengths to ensure secrecy and plausible deniability, they and their leadership must be aware that these programs do become public,[37] thus the policymakers should have a clear purpose and follow distinct principles to ensure that these programs are worth the potential risk to reputation and resources.

Purpose of Covert Action

The definition of covert action from the U.S. National Security Act tells us that the activities must be in some way secret, but it only provides a loose statement of purpose: "to influence political, economic or military conditions abroad."[38] In his book *Dirty Tricks or Trump Cards*, Roy Godson provides more color when he outlines his three purposes of covert action: "(1) To influence the internal balance of power in a country or in a transstate group, such as an ethnic alliance or an international criminal cartel; (2) To influence the climate of opinion in them; and (3) To induce specific actions unrelated to the internal power balance or climate of opinion."[39] A huge variety of activities fall under the definition of covert action. These activities could range from support to a foreign government during elections, to providing material support to a political group, to

implementing coups and conducting assassinations, and these are just some of the actions that fall within the covert action domain. However, the majority of covert actions can be divided into three categories, which we'll discuss in much more detail in the following sections: (1) political action; (2) military operations; and (3) information operations (IO). While these three categories encompass many activities designated as covert actions, we must understand that many, if not all, components of hybrid warfare can have covert aspects to them. Before discussing the other components, we must first review the principles of covert action.

Principles of Covert Action

The secret nature of covert action and the wide variety of activities that fall underneath the definition make specific principles hard to establish. However, Godson does outline some basic principles to be followed when utilizing covert action. Godson writes: "Covert action is a policy tool, not a substitute for policy."[40] A government must have a concrete policy goal in mind before employing covert action. These actions tend to be less effective, harder to implement, and generally counterproductive when the goal established by the policy makers is ambiguous or constantly changing.[41] Additionally, covert action cannot be seen by government actors as a magic bullet that can solve the problems of a failing foreign policy. Instead, Godson writes that any clandestine activity "must be coordinated with and supported usually by diplomatic, military, and/or economic measures."[42] While there are situations where the use of covert action alone can have the necessary effect on a situation, more often than not, covert action must be used along with other activities to create a mass effect that achieves the goal.

Policymakers cannot just make covert action happen by establishing a policy and telling the relevant agency or organization to act; instead, they must put the right leaders and operators in place to effectively capitalize on opportunities.[43] For these leaders and operators to be effective they must be creative in their thinking, they must coordinate with policymakers, and they must be willing to be self-reflective on the results of any program.[44] However, creativity does not make up for a lack of knowledge of the region or the subject area of the target.[45] These pieces of knowledge are critical for any operator attempting to formulate and execute a covert action program.

Additionally, timing is a crucial aspect of covert action programs. Godson writes "Launching a covert program too early can be disastrous, while doing so after a crisis has developed—and after the adversary has prepared its defenses—can be equally futile."[46] Because there is a sweet spot for covert action programs, policymakers must be discerning about when they deploy these programs. Finally, Godson writes: "Covert action is far more effective as a preemptive measure."[47] Thus, the success of a covert program is not just reliant on policymakers establishing a concrete set of policy goals. Instead, covert action requires the right people to be in the right place at the right time.

The Overarching Component

We consider covert action to be the overarching component. As stated above, covert actions fall mainly into three categories: (1) political action; (2) military operations; and (3) IO. However, covert activities can be found in all of the components that we describe below. Additionally, overall, hybrid warfare relies on deception, which many times necessitates covert action to complete.

Political Action

Political action is a type of covert action aimed at influencing political leaders or the political situation in other states. There are a variety of different ways that actors in the international system have used political action to influence the political situation in countries of their adversaries and allies. Two of these methods are described below.

Support to Politically Influential Groups

One method of influencing the political situation in other states is by covertly supporting, through financial or other means, actors like opposition groups or political allies in those countries. With the dramatic increase of politically influential groups in the modern era, this political action tactic has become even more important.[48] These groups include political parties, nongovernmental organizations, the media, businesses, labor unions, religious organizations, ethnic groups, and professional associations.[49]

Perhaps the most famous case of political action through the support of politically influential groups was the American support to the non-communist Christian Democrat party during the 1948 Italian elections. There was a fear in the United States that the Italian communist party would win the 1948 elections and would bring the country under Soviet influence.[50] In order to prevent this from occurring, the Central Intelligence Agency (CIA) directly funded the Christian Democrats and provided expert advice to Christian Democrats and other anti-communist party politicians.[51] F. Mark Wyatt, who was a CIA officer in Rome at the time, said later in an interview, "We had bags of money that we delivered to selected politicians, to defray their political expenses, their campaign expenses, for posters, for pamphlets."[52] In all, the CIA provided millions of dollars to the anti-communist parties during the 1948 campaign in Italy.[53] While the overall amount may not have reached the $8 to $10 million per month range that the Soviet Union provided to communist parties,[54] the CIA's support had a huge impact on the Christian Democrats and eventually led to their comfortable victory in the election.

As the United States did in Italy, a government can provide a combination of hard currency and advice[55] through covert political action in order to support and influence groups. These groups are then more likely to move toward the goals of the country deploying the political action.

Influence and Infiltration of Established Regimes

While normal diplomacy involves influencing and cajoling political leaders, these activities are done in the open with known actors. Covert actors can also play a part in influencing regimes. There are three specific political action mechanisms that governments have used to influence established regimes. First, there are some situations where a covert actor can provide valuable advice and influence the decision of a political actor. [56] In these situations, the covert actor is known to the political actor as a member of another government, but is seen as a confidant and advisor.[57] Second, a country could place an unacknowledged covert actor into the employment of the target head of state or other leader to influence decisions without the political actor's knowledge.[58] Finally, a country could focus on befriending or acquiring as an asset a target country national who is well positioned to influence policy decisions.[59] This can be done when that person is in office or early on in her or his career. All of these methods would have direct effects on the political situation in a target country.

The topic of influencing and infiltrating has a variety of sub-components. An example of how a known covert actor can serve as a valuable asset to a foreign government comes from William Colby, who would become director of the CIA. He wrote in his memoir that he, a CIA officer, and not the U.S. ambassador was called in to mediate deadly factional struggles in South Vietnam in the 1950s and 1960s.[60] Additionally, the Soviet Union was somewhat successful in its efforts to acquire assets in U.S. and British policy positions during the Cold War. Specifically, the Soviet Union was able to establish as assets Harry Dexter White and Alger Hiss in the U.S., as well as Guy Burgess and Donald Maclean in the United Kingdom.[61] These examples of political action through covert actors is essential to understanding the overall ability of countries to influence policies from afar.

Russian Use

Political action has been used for centuries by successive Russian regimes to affect the political situation in their near-abroad as well as in other states around the world. For example, according to Godson, the Soviet Union was particularly adept at identifying young future leaders from different countries, educating them in the Soviet Union, and then continuing a relationship with these leaders as they moved up the ranks.[62] A good example of this creation of long-term relationships is the Soviet relationship with Hafez al-Assad of Syria. The man who eventually came to power in a coup was trained by the Soviet Air Force in the Soviet Union.[63] He later relied on the Soviet Union for his domestic and international achievements.[64]

Current Russian use of political action is focused on providing support to leaders and groups inside of near-abroad countries and using influence to affect the actions of other states. While there are likely cases of covert infiltration and influence occurring throughout the near-abroad, these cases have not currently come to light and will likely remain hidden for years to come. Thus, this section will focus on some of the many cases of recent Russian use of political action in the form of support for influence. Ukraine provides two of the best examples.

Russian influence in the political structure of the Ukraine goes back centuries, however since the fall of the Soviet Union, the Ukrainian state had been moving toward Europe and away from Russia.[65] This culminated in the Orange Revolution of 2004, which brought the pro-Western Viktor Yushchenko to power.[66] In 2010, the pro-Russian Viktor Yanukovych[67] came to power with the support of the Russian regime.[68] This began a significant shift of Ukraine back to the Russian sphere of influence.[69] By 2013, the Russian regime and the Yanukovych government had become even closer. In November 2013, the Russian regime's influence over the government of Yanukovych reached a breaking point for the population when the government rejected an economic deal with the EU.[70] Yanukovych instead decided to sign a Russian economic package, reportedly after heavy lobbying by Putin and other Russian actors. This lobbying included threats to reduce support to the regime.[71] This launched months of protests that eventually brought down the Yanukovych government. With the government gone, the Russians lost the ability for to directly influence the Ukrainian government, thus they turned to other groups.

Since the fall of Yanukovych, the Russian government has clearly supported pro-Russian groups, both in the Donbass and in Kiev, against the government. They have sponsored them with financial and non-lethal aid,[72] as well as with political and technical advice,[73] in order to influence the future of the eastern part of Ukraine and the Ukrainian government in Kiev. In the U.S., we have heard a lot about the Russian soldiers, equipment, and other supplies that flowed over the border to the Eastern Ukrainian separatists. While this support was important for cementing

Russian influence within the rebel organization, the political and technical advice that the Russian regime supplied was equally important. This ensured that the rebels focused on the political goals of Russia as they were pursuing their own goals. An example of the political influence that the Russian regime has had over the rebels happened during the Minsk peace negotiations in 2015. During these negotiations, President Putin represented the interests of the Eastern Ukrainian separatists. When an acceptable agreement from the Russian perspective was reached, Putin reportedly put pressure on the rebel leadership to accept the agreement despite calls from more hardline rebels to reject the accord.[74] Without the political actions taken by the Russian regime to support the rebels, likely the Russian influence would not have been significant enough to force the agreement on the rebels.

It is important to reiterate, Russia's use of political action in the Ukraine is likely much more expansive then the two examples described in this section, but as with most components discussed in this project, it will be difficult to determine the full level of activities for decades due to the covert nature of the majority of these political actions.

Cyber Action

As society becomes increasingly reliant on technology, the use of cyber warfare tactics or cyber action has become more and more common. Not only is cyber action being employed increasingly frequently by states, but also the deftness with which these tactics are employed is reaching new levels. The impact of these actions is becoming increasingly concerning.

Definition of Cyber Action

Cyber attacks take many forms and can target a wide range of vulnerabilities within states. These actions can be categorized as targeting three different areas: confidentiality, availability of data, and integrity.[75]

Cyber actions surrounding the acquisition of confidential information are some of the most common types of attacks. Intended to gain access to sensitive government information or individuals' personally identifiable information, there have been many examples of these sorts of attacks in the recent past, including the U.S. Office of Personnel Management data breach[76] and the 2013 theft of the F-35 design data from government contractor Lockheed Martin.[77] Both of these attacks, while distinctly different in nature, represent a significant threat to Americans and our national interest.

The issue of data availability is most closely linked to distributed denial of service (DDoS) campaigns, which compromise users' ability to access sites and information. DDoS attacks "attempt to exhaust the victim's resources. These resources can be network bandwidth, computing power, or operating system data structures."[78] By overwhelming the system, attackers are able to shut down sites ranging from banks, to official government sources, to news outlets. The 2007 attack on Estonia's cyber capabilities is a clear example of this sort of action. Described in further detail in the case study section of this report, this attack rendered Estonian government sites inaccessible for several weeks and disrupted communication, banking, and other crucial functions in the country.[79]

Integrity of data and information is critical to the functioning of systems. Attacks against the integrity of a system seek to alter the data that governs a system, changing its function or

allowing the attacker to access critical information about the way the system functions. These attacks compromise a system's integrity and leave it vulnerable to manipulation. This breach of a system's integrity can often be difficult to detect and can be ongoing during what appears to be normal system operations. The Stuxnet virus found in Iran is an example of this type of attack geared toward infecting an industrial control system and manipulating the data therein.[80] While this virus was specifically targeted to affect system operations and damage an Iranian nuclear facility's capacity, it is conceivable that future attacks against system integrity could be targeted to threaten more substantial infrastructure elements and even human life.[81]

Purpose and Threat of Cyber Action

Cyber warfare can be used for numerous different reasons, including the collection of intelligence and the disruption of activities. All of these intents, however, come back to a central desire to disrupt a nation's normal operations and compromise both their systems and their information. This impact, particularly when well targeted, can have a substantial effect on highly technology-dependent countries, shutting down banking systems and stymieing the government's ability to function and respond to the attack.

The threat of a massive cyber attack in the future is contested, with some arguing that the fear is overblown,[82] while others feel that a looming "cyber Pearl Harbor"[83] could have a major impact on the United States.[84] According to a poll conducted by the Pew Internet & American Life Project regarding the situation in the U.S., 60 percent of technology experts interviewed believe that by 2025 "a major cyber attack [will] have caused widespread harm to [the] nation's security and capacity to defend itself and its people."[85] While it is impossible to know how the future of cyber action will unfold, it is certainly important to consider this element in concert with the other hybrid tactics employed by states to fully assess future threats.

Debate Over Cyber Action's Place in War

At the NATO Summit in Wales in September 2014, the question of the gravity of cyber action was confronted as the summit representatives attempted to assess if cyber warfare could be devastating enough to merit the invoking of NATO Article 5, also known as the collective defense clause.[86] These large-scale cyber attacks have never led to a formal declaration of war. Without this, institutions like NATO are unable to respond.

To address the gap, the Wales Summit Declaration affirmed that cyber threats could often be as crippling as traditional threats and that there is a role for NATO in responding to these actions. It stated: "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence."[87] However, the level of attack necessary to reach the threshold of magnitude required to invoke the collective defense provision in Article 5 was not clearly defined at this meeting. This lack of definition left the question of the use of cyber action and the response from the international community murky. This debate, which was largely born out of the April 2007 DDoS cyber attack in Estonia, is far from over and the feasibility of invoking Article 5 to respond to cyber action remains debatable.

Russian Uses of Cyber Action

The Russian government's ability to make use of sophisticated cyber tactics poses a serious threat to NATO nations. While the Russians have denied any involvement in the 2007 Estonia attack, this case study stands as a clear example that cyber action must be taken seriously as an element of any hybrid warfare that could be waged in the future. Beyond DDoS-style attacks and campaigns geared toward espionage and compromising sensitive information, the Russian government has taken cyber action to another level with a whole agency focused on trolling the Internet and disrupting information flows.[88] Additionally, Russia has devoted a significant amount of government resources to cyber action and views these tactics as a critical part of their long-term vision for Russian strategy.[89] Russia's cooperation with China on cyber issues is also concerning for NATO countries.[90]

This particular hybrid tactic is critical to the future of Russian pressure on the Baltic States. The reliance of the Baltic States on technology makes them especially vulnerable to this threat and efforts to build cyber resilience are ongoing.[91] Increasing allies' ability to provide support in responding to a cyber attack and better understanding NATO's role in these situations is critical to countering this threat.

Information Operations

On 1 February 1942, the words "We bring you voices from America" were spoken in German over a radio broadcast into Nazi Germany.[92] This broadcast, spoken by William Harlan Hale, was made just 56 days after the United States entered WWII and marked the establishment of the Voice of America (VOA)[93]. Throughout WWII and the Cold War, VOA served as the information channel for the USG into Nazi occupied Western Europe and communist dominated Eastern Europe. The establishment and use of VOA during these periods of conflict represents the use of propaganda by the U.S. against its enemies. This form of propaganda, designed to influence an opponent, is just one form of a broader component of hybrid warfare called IO.

IO[94] takes a variety of forms depending on the user and the audience. The RAND Corporation defines IO as including "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[95] RAND's definition points to two sides of the IO arena, which are important to understanding the overall utility of this hybrid warfare component: (1) the collection of information, and (2) the dissemination of information. In the discussion below we will focus on the second part of RAND's definition: the dissemination of information. However, that is not to say that the collection of tactical information is in any way less important within a hybrid campaign. Rather, it is a tactic that has been in use consistently in war making, as evidenced by the myriad of intelligence services in operation throughout the world, and is often assumed to be present. As such, we will focus on the less institutionalized aspect of IO. For a discussion of the collection or restriction of information through technical means, please see the cyber action section above.

Dissemination of Information for Deception and Influence, or Propaganda

In order to understand this component of hybrid warfare, we must first define dissemination of information for deception/influence, also known as propaganda[96]. Harold Lasswell[97] states: "Propaganda in the broadest sense is the technique of influencing human action by manipulation

of representations. These representations may take spoken, written, pictorial or musical form."[98] We can then supplement Lasswell with Mark Lowenthal's definition of the uses of propaganda. He states that propaganda "can be used to support individuals or groups friendly to one's own side or to undermine one's opponents. It can also be used to create false rumors of political unrest, economic shortages, or direct attacks on individuals…."[99] These definitions combined touch on the goal of propaganda. To simplify, the goal of propaganda is to, through some medium, influence another individual, society, or government to believe a desired 'truth' or act in a way that accomplishes the political goals of the propagandist.

Propaganda is disseminated in a variety of fashions and can be directed either overtly or covertly by the acting country against the target country. Overt propaganda are items we see every day: official government announcements, television and radio broadcasts, popular culture, music, print advertisements, the Internet, cultural centers,[100] and official information centers[101] based in the target country.[102] The key distinguishing characteristic of these pieces of propaganda is that there is some formal recognition that these are official messages from one country to another.

In direct contrast is covert propaganda. Lowenthal describes covert propaganda as "information, ideas, and symbolic actions whose sponsor remains unknown."[103] Within the covert propaganda genre there are "black" actions, which are completely hidden,[104] and "gray"[105] actions that are sent out using a "thin veil" of cover but can be denied by the issuing country.[106] Because of its secrecy, covert propaganda is most often used when a country is attempting to spread untruths or disinformation to its adversary.[107]

Throughout history, propaganda has been a successful tool in warfare. During times of war, propaganda has been used to influence populations against their governments and spread disinformation to governments and militaries. However, there is an important caveat to its effectiveness. As Godson states: "The effectiveness of disinformation often depends more on the predisposition of the intended recipients than on the quality of the disinformation or the vehicles used to disseminate it. People will believe what they want to."[108]

There are many examples of the use of information and propaganda to affect adversaries during the conflicts in the Middle East over the last fifteen years. For example, during the summer 2006 conflict between Israel and Hezbollah, Hezbollah and its leader Hassan Nasrallah used the media to show the devastation in southern Lebanon and the actions of the Israeli military.[109] According to Marvin Kalb, Hezbollah "projected a very special narrative for the world beyond its kin—a narrative that depicted a selfless movement touched by God and blessed by a religious fervor and determination to resist the enemy, the infidel, and ultimately achieve a 'divine victory,' no matter the cost in life and treasure."[110] This concerted effort to use media against the Israeli military and government is a clear use of IO. While Hezbollah also ran traditional propaganda, their use of the media to inadvertently champion their cause helped perpetuate the dual image that the Israelis were in the wrong for launching the attack and that Hezbollah was triumphant in the end.[111]

Electronic Operations

Another aspect of IO that is worth noting is the sub-component of electronic warfare. These operations involve the use of the magnetic spectrum to disrupt the operations of an adversary.[112] This can take three main forms: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA is the most direct form of electronic warfare, dealing primarily with

using "electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability."[113] While EP involves securing one's forces against such an attack and ES operations attempt to discern both intentional and unintentional sources of electromagnetic energy that could disrupt one's own operations.[114] In short, electronic warfare can be used both offensively and defensively.

Russia's Recent Use of IO

The use of information as a tool of war by Russia goes back centuries. During the Cold War, the Soviet Union used both open and covert propaganda to try to achieve their goals. In recent years, the Russian regime has utilized similar tactics to influence the political and cultural situations in their near-abroad.

For example, following years of unease over the Republic of Kyrgyzstan's lease of the Manas Air Base to NATO forces operating in Afghanistan, in 2010, the Russian regime began a concerted IO against the Kyrgyz government.[115] The Russian government had been particularly angered over Kyrgyz president Kurmanbek Bakiyev's effort to play Russia and the U.S. off against each other. The Russian government had agreed to provide the Kyrgyz government with $450 million in aid, but there was a tacit agreement that this aid was contingent on the Kyrgyz closing Manas.[116] Instead, Bakiyev changed the name of Manas to a 'transit center' and brokered a renewed deal with the U.S.[117] As Bakiyev signed the deal with the U.S., the Russian government began hosting a variety of Kyrgyz opposition leadership in Moscow.[118] The signing of the agreement triggered the beginning of an aggressive IO against the Kyrgyz government.

In March 2010, Russian media and local opposition media outlets released reports accusing the president of corruption.[119] When the government shut down the websites it was not just press-freedom NGOs that protested, but also the Russian Foreign Ministry.[120] The reporting prompted widespread protests against the government on 7 April 2010. It took only 24 hours for the government to fall and a new government to take over.[121] While the new government had members who were close to both Russia and the U.S., the change in government did provide a positive change for Russian interests in Kyrgyzstan.[122]

While the concerted IO against the Kyrgz government by the Russian Federation is a great example, we have seen an even more recent effort by the Russian regime. The IO launched in Crimea and eastern Ukraine was on a much larger level then what was seen in Kyrgyzstan. In fact, the then–NATO Supreme Allied Commander, Europe, U.S. General Phillip Breedlove, stated that the Ukraine operation was "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[123] In part two of this report, we will discuss the case of Crimea and delve deeper into the use of IO by the Russian Federation as they sought to annex the peninsula.

Military Operations

Military operations as a title for this component is a misnomer but a necessary one. Many, if not all, of the components described above and below involve the military in some ways, but this section seeks to address the military's involvement in its traditional form: the conduct or facilitation of kinetic actions against an opponent. Of the components, military operations are

likely the most diverse. Governments as well as non-state actors can deploy a variety of different military capabilities to accomplish their goals. Because of this ability, military operations, specifically covert ones, should be seen as an integral part of hybrid warfare.

Conventional Force

Perhaps the most important form of military operations is conventional force. Conventional forces (CF) are defined by the U.S. Joint Chiefs of Staff as: "[t]hose forces capable of conducting operations using nonnuclear weapons."[124] To expand this definition, we should include non-SOF applications, as well. In short, conventional force is the normal application of force utilizing ground, naval, and air assets in a coordinated fashion to accomplish battlefield goals. However, in hybrid warfare, CF serve two purposes. First, they can be part of a military engagement with the enemy in coordination with other components of hybrid warfare. Second, they can serve a performatory role. By this we mean, CF can be used to signal to an actor or an actor's population a certain message. When directed at another actor, it may indicate a deterrence, denial, or compellence strategy. When directed at an actor's population, it may send the message that the country is behind that population or that the government of the target actor is not protecting them adequately.

For example, the Persian Gulf War in the early 1990s showed the power and limits of conventional force, in a performatory role, as a deterrent and compellence tool. The deployment of U.S. and Coalition CF to the Saudi Arabia–Iraq border in Operation Desert Shield attempted to deter Saddam Hussein from attacking Saudi Arabia. It was successful in deterring any further movement south by Saddam's forces, but it failed in its other writ, which was to compel Saddam to withdraw his forces from Kuwait. An actual use of force was required to accomplish that task.

Overall, while CF are seen as less important as wars have evolved, this type of military operation is still a vital component of hybrid warfare because of both its kinetic and performatory role in military actions.

Special Operations Forces

SOF are the complement force to CF. SOF are defined by the U.S. Joint Chiefs of Staff as:

> Those Active and Reserve Component forces of the Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations.[125]

SOF can be used in a variety of ways. To simplify, their activities can be separated into special operations and paramilitary operations. Lowenthal especially makes it clear, in his seminal work on intelligence, that paramilitary and special operations should be separated from each other.[126]

Special Operations

Special operations utilize uniformed SOF personnel to conduct kinetic activities against an enemy actor. The U.S. military defines special operations as:

> Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk .[127]

As indicated in the definition, special operations are focused on using force, not facilitating the use of force. An excellent recent example is the use of uniformed Navy SEALs during the raid to capture or kill Osama bin Laden in Pakistan. These soldiers were not sent to provide advice and assistance to local forces attempting to kill bin Laden, but instead were sent to engage the target directly. This tactic obviously has both limitations and great risks, as evidenced by the disastrous Operation Eagle Claw,[128] authorized by President Jimmy Carter to save the U.S. embassy hostages in Iran. Thus, special operations with uniformed personnel or personnel that could be identified as a country national are an important but limited component of hybrid warfare.

Paramilitary Operations or Unconventional Warfare

Paramilitary operations or unconventional warfare is in contrast to special operations because, according to Lowenthal, "They do not involve the use of a state's own military personnel in combatant units, which technically would be an act of war."[129] Instead, Lowenthal defines paramilitary operations as "involving the equipping and training of large armed groups for a direct assault on one's enemies."[130] The U.S. military uses the phrase 'unconventional warfare' when describing this component. The military defines it as: "Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[131] In short, paramilitary operations, or unconventional warfare, are focused on providing assistance to other forces, like resistance movements, in order to accomplish a political goal. This assistance in the form of advice, financing, weaponry, and other items is provided by covert agents or military personnel out of uniform. Because of this covert nature, paramilitary operations or unconventional warfare serve an obvious value as a hybrid warfare technique.

A good example of the successful use of paramilitary operations or unconventional warfare is the U.S. action in Afghanistan in the 1980s.[132] The U.S. was able to provide assistance in the form of advice, financing, and weaponry to the Mujahedeen, who were fighting a guerilla war against the Soviet Union in Afghanistan. The U.S. was successful in helping the Mujahedeen defeat the Soviets and eventually drive them from the country.

Blending Special and Paramilitary Operations

In recent years, we have seen a more distinct blending of special and paramilitary operations. While there are examples of the Soviet Union using its own pilots against the U.S. and its United Nations (UN) allies during the Korean War,[133] generally the use of uniformed personnel in situations where war was not declared was risky to the point of foolhardy, especially during the Cold War. However, as conflict shifted toward non-state actors, we have seen forces usually used for paramilitary assistance operations, being pushed into combat roles and vice versa. For example, the CIA paramilitary forces and Department of Defense (DOD) SOF, which operated in Afghanistan in the immediate aftermath of the 9/11 attacks, provided military assistance and advice, and actually participated with local forces in combat operations against the Taliban.[134]

Terrorism

The final use of military operations we will discuss is terrorism. Terrorism is connected to the definitions of both special and paramilitary operations, but remains a separate component of hybrid warfare because of its unique nature. Terrorism is defined by the U.S., in 18 U.S.C. § 2331, as:

> [V]iolent acts or acts dangerous to human life that violate federal or state law; [and] Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping….[135]

Terrorism is conducted covertly by either states, state proxies, or non-state actors to achieve a particular political goal. When that goal is not well defined, like other forms of covert action, the act of terrorism tends to produce few results.[136] For our purposes we will focus on the use of terrorism by states and state proxies. Overall, because of terrorism's covert nature and ability to create spectacular political results for one actor against another, it is an incredibly important part of the overall hybrid warfare strategy.

From the siege of Caffa[137] in 1346 to the assassination of Archduke Ferdinand in 1914, there are centuries of examples of terrorism being used by states or state proxies. A more recent example of terrorism's use as a political tool for a state or state proxy is the heavy use of terrorism against American targets in Lebanon during the 1980s. Iran, through its proxies, Islamic Jihad and Lebanese Hezbollah, targeted Americans in Lebanon with the ultimate goal of eliminating the American presence in the country.[138] This culminated with the 1983 bombings of the U.S. Marine barracks and the U.S. embassy, both in Beirut.[139] This terrorist attack accomplished its goal, causing the United States to withdraw from Lebanon.[140]

Russian Use of Military Operations in Hybrid Warfare

Russia has been a military power since the founding of the Grand Duchy of Moscow in the mid-1500s. During the Napoleonic Wars, the Russian military—and the Russian winter—successfully repelled Napoleon and his massive force. In WWII, the Russian military fought a hard campaign to throw back Hitler's advancing force. Without the Soviet force, Berlin would likely not have fallen and unconditional surrender would not have been achieved. These, and many other examples, show the proud Russian tradition in the military arts.

In recent years, despite Russia's poor economic situation,[141] its military remains a potent force with both CF and SOF. While its CF have always been well trained and led, there has been a new focus on SOF in recent years. In this section, we will focus on two examples of Russian use of military operations. We will not have examples of the use of SOF or paramilitary operations because those topics will be discussed at length in part two of this project.

Russia has used conventional force as both an actual tool of force as well as a performatory tool in recent years. As an example of the actual use of force, during the Russo-Georgian War of 2008 over the breakaway states in the northwest of Georgia, the Russian military used CF as part of a broader hybrid strategy to invade, destroy much of the Georgian military, and occupy the breakaway provinces. More recently, Russia has used snap military exercises to send a message to NATO and its neighbors about their military readiness and ability to launch a surprise attack.[142] We will discuss the conventional aspect of hybrid warfare during our case study discussions.

Finally, Russia and its proxies have used terror as a weapon in their hybrid warfare strategy. On 17 July 2014, pro-Russia rebels in eastern Ukraine shot down Malaysia Airlines Flight MH17 while it was flying over rebel controlled areas.[143] The missile used was a Russian-made Buk missile that was supplied to the rebels by the Russian regime.[144] While the order to shoot down the

airplane likely did not come from the Kremlin itself, this use of terror was clearly targeted toward the West.

Naval Power

Military strategic theorists have long debated the centrality of naval prowess in the growth and expansion of great powers. Alfred Thayer Mahan, a Naval officer, historian, and president of the Naval War College in the late 1880s, notably argued that a great navy is necessary for a major power.[145] As time has progressed, naval power has developed and expanded its scope, moving beyond Mahan's vision of a traditional navy to include many new uses for sea power, including hybrid warfare.

Definition of Naval Power in Hybrid Warfare

Although a traditional element of conventional military power, naval power can serve a unique purpose in hybrid warfare. With naval power, states are able to employ naval tactics to project power, increase strategic positioning, deter enemy action, and compromise sea-based systems. By developing naval capabilities and making use of these tools in unconventional ways, a hybrid approach to war expands the traditional notions of naval power beyond their conventional bounds.

Purpose of Naval Power in Hybrid Warfare

Unlike traditional offensive and defensive uses of naval power employed in conventional warfare, naval power in hybrid warfare seeks to shape naval strategy around goals other than combat. Through the use of ships and submarines, states can collect valuable intelligence and information. For example, in recent months there have been significant concerns regarding the highly vulnerable nature of deep-sea fiber-optic cables. These concerns stem from Russian use of naval assets in non-conventional ways that threaten to disrupt these key sea-based platforms.[146] In addition to these espionage and sabotage driven approaches to naval power, naval power projection has been used throughout history, including the notable examples of Commodore Perry opening relations with Japan and the tour of the Great White Fleet in the early 1900s. Coupled with traditional naval tactics, these examples of naval power in hybrid warfare allow states to use their military forces to extend their influence without engaging in hostilities.

Russian Use of Naval Power in Hybrid Warfare

Russia continues to develop and expand its navy, with the major addition of 80 warships to the Black Sea Fleet expected by 2020 and a plan to construct a second naval base near Novorossiysk to house these additions to the fleet.[147] As this growth and modernization of naval assets continues, concerns regarding Russian uses of sea power as part of their hybrid warfare strategy also increase.

In an October 2015 meeting, Admiral Mark Ferguson III, then commander of U.S. Naval Forces Europe and U.S. Naval Forces Africa, and commander of the Allied Joint Force Command in Naples, highlighted the rising prowess of the Russian navy. "We are observing the manifestation of a more aggressive, more capable Russian Navy … It is naval capability focused directly on addressing the perceived advantages of NATO navies. And they are signaling us and warning us that the maritime domain is contested."[148] Ferguson also discussed what he referred to as an "arc of steel from the Arctic to the Mediterranean."[149] This increasing expanse of Russian power projection includes Russia's efforts to protect its sole naval base in Syria, which serves as a key

location for Russian vessels to refuel in the Mediterranean.[150] In the Arctic, Russian action is seen as increasingly aggressive, particularly by states in the region. The Russian strategic nuclear submarines have engaged in several training exercises in the Arctic[151] and concerns about potential implications for Russian expansion in the Arctic Circle remain high.[152]

The United States has also become increasingly concerned about the modernization and adaptation of a leaner Russian submarine fleet,[153] and the potential rearming of submarines with nuclear missiles. A Russian news channel recently showed 'leaked' plans for a long-range nuclear torpedo, which would be mounted on a submarine and is designed to "destroy important economic installations of the enemy in coastal areas and cause guaranteed devastating damage to the country's territory by creating wide areas of radioactive contamination, rendering them unusable for military, economic or other activity for a long time."[154] Concerns about the inability of the U.S. to track these submarines has increased fears and led to the launching of experimental blimps meant to detect cruise missiles.[155] Russian submarine operational tempo has also increased dramatically, with Ferguson noting in 2015 that "[a]ccording to Russian Navy chief Admiral [Viktor] Chirkov, the intensity of Russian submarine patrols has risen by almost 50 percent over the last year. Russia has increased their operational tempo with this force to levels not seen in over a decade."[156]

Ferguson also views Russia's naval expansion as geared toward projecting Russian power and deterring NATO action. "This is a sea denial strategy focused on NATO maritime forces. Their intent is to have the ability to hold at risk the maritime forces operating in these areas and thus deter NATO operations."[157] This deterrent serves both political and economic purposes, with many of the Russian military drills in the Baltic focused on protecting the Nord Stream pipeline.[158]

Lastly, Russian involvement around key underwater cables is also a source of major concern.[159] While no cable cutting has been witnessed yet, key military leaders in the United States remain concerned that Russia may be planning to sabotage the cables and thus compromise key communication technology. David Sanger and Eric Schmitt wrote in *The New York Times* in October 2015 that: "The ultimate Russian hack on the United States could involve severing the fiber-optic cables at some of their hardest-to-access locations to halt the instant communications on which the West's governments, economies and citizens have grown dependent."[160]

All in all, many scholars have recognized the central importance of naval power to Russian strategy, even in unconventional functions. According to Richard Weitz, a senior fellow and director of the Center for Political-Military Analysis at Hudson Institute: "The state of the Russian navy will be a major factor in determining Moscow's global power. Having the ability to project sea power is critical to realizing Russia's ambitions in several domains, ranging from energy to economics to security."[161]

Use of Proxies

Definition of the Use of Proxies

The use of proxies is a time-honored tradition among great powers. The use of a proxy party within a conflict is broadly defined as using an actor within a given context to "do one's dirty work," rather than intervening directly.[162] Some of the more prominent examples of this come from the intervention in internal conflicts during the Cold War on the part of the U.S. and the Soviet Union.

As such, a more commonly accepted definition is perhaps one that refers to proxies as the militaries and non-state armed groups through which more powerful states wage their wars indirectly.

However, this definition misses an important point in the definition above—that nowhere in it do arms come into play. While the conflict context may imply a fighting force, the proxy does not necessarily have to be a militarized one. This may not have been an important distinction in relation to conventional warfare; it is a crucial one when considering hybrid warfare. Given the many tactical options that are available as part of a hybrid warfare campaign that are not traditionally considered the realm of CF, it would be a mistake to limit proxies to paramilitary operations alone.

Take relations between states as an example. States themselves can act, and often have acted, as proxies for other states in a variety of capacities outside of military operations.[163] For instance, states within the Warsaw Pact acted according to the wishes of the Soviet Union for much of the 20th century, even outside of conflicts. As such, this project will refer to the use of proxies as the use of actors that are not directly or officially affiliated with a state to allow that state to intervene indirectly in a given context. Specific manifestations of the use of proxies will be examined further in subsequent sections of this project.

Russian Use of Proxies

The question here is not whether the Russian Federation has been using proxies in its interventions, but how it has been doing so. The unique feature of Russian use of proxies is the sheer variety of proxy elements in play and the motivation behind that variety. An easy example is that of Russia supporting separatist militias in Ukraine. This is an example of the traditional form of proxy use—the support of a local group to accomplish one's political goals without direct intervention. For our purposes, Russia's use of more unconventional proxies is far more interesting.

Take, for example, the Russian government's affiliation with the Night Wolves.[164] This is a motorcycle gang with a history of flouting the law and committing violence against its rivals, and yet they have been receiving funding from the Kremlin. The purpose of this relationship is two-fold. In the short term, Putin was able to remove a potential threat, as the Night Wolves were a pillar of the counter-culture. By putting the Night Wolves on his payroll, Putin was able to undermine their legitimacy in the counter-culture movement and the integrity of the movement as a whole.

In the longer term, this relationship has given the Russian government yet another mouthpiece through which to spread their propaganda. The Night Wolves have become fiercely patriotic, with one of their mottoes claiming that "wherever the Night Wolves are, that should be considered Russia."[165] The Night Wolves are not an overtly violent organization, though their history has proven that they are ready to fight when need be, and are therefore able to go places and do things for the state that a militia would be unable to do, such as their ride-and-rally from Moscow to Berlin to commemorate the 70th anniversary of Victory Day and remind the world of who took Berlin in 1945.[166]

Another proxy worth noting when discussing Russia's indirect intervention is what Russian Chief of Staff General Valery Gerasimov refers to as the "protest potential of the population."[167] This is not the potential utility of militants or criminals, but that of the people themselves—average citizens who are unhappy in some way, particularly if that unhappiness stems from being a Russian minority abroad. In this, Gerasimov encourages the support of subversive elements within a target

state to weaken that state in conjunction with other efforts within an overall campaign. We saw this in action as Russia supported separatist movements in Crimea, which will be elaborated upon in a subsequent case study.

In short, Russia has used a broad definition of 'proxy' in their indirect interventions. As such, any power hoping to counteract such effects should adopt this broader definition as well. This is particularly useful when considering a hybrid campaign as a whole, as much of such a campaign rests on activities performed outside of kinetic forces, both conventional and otherwise.

Power Projection

Definition of Power Projection

Projecting one's power abroad is one of the key interests of any Great Power.[168] It is not new and has been at play on the global stage for centuries. However, with the advent of increasingly destructive weapons after WWII coupled with a progressively shrinking world, power projection has become ever more closely tied to a strategy of deterrence.[169]

At its more basic, power projection is most broadly defined as a nation extending its military forces well beyond its borders.[170] In short, power projection is less about any specific action that the projecting nation takes, but rather about making one's presence felt as part of a deterrence strategy. Modern power projection tends to rely heavily on sea and air power,[171] but can also manifest in more "soft power" forms by establishing a presence in a region via base construction, for example.[172] Again, the specific manifestations of this tactic will depend heavily on context and target, however the overall theme of using CF to assert one's presence in a given region or conflict is at the heart of power projection operations.

Russian Use of Power Projection

While one can certainly argue over which of the various hybrid tactics have been most widely used by the Russian Federation in recent years, power projection would certainly be one of the top contenders. With its budgetary struggles and outdated military,[173] power projection provides a logical outlet for Russia to reassert its military might without having to back up that assertion with open war.

Rather, it has been reasserting itself in regional conflicts, such as Syria,[174] used its navy to threaten key communications infrastructure,[175] and violated sovereign airspace to remind the international community that it is able to do so.[176] A more creative interpretation of power projection can even include the supposed 'leak' of the new nuclear torpedoes[177] into mainstream media and a technique to reassert its military prowess. While there is no evidence of these weapons leaving Russian soil, tales of their existence reached smartphones and nightly news broadcasts in homes all over the world. Despite the lack of physical presence, one could certainly argue that the Russians were able to make their presence felt via stories of these weapons.

Taken at face value, these accounts give the impression that the Russian military is everywhere and can strike at any time. However, a closer look reveals that not only would it be unprepared for a large-scale conventional fight,[178] but the current model is likely unsustainable.[179] Still, through power projection techniques, it is able to give the illusion that it is a force to be reckoned with and has used this impression to catapult itself back onto the center-stage of world

politics. This is particularly useful when considering a hybrid campaign as a whole, as much of such a campaign rests on activities performed outside of kinetic forces, both conventional and otherwise. To that end, this piece will not treat proxies as a separate component going forward. As with covert action, the use of proxies is an overarching component of a hybrid warfare campaign, and therefore will be characterized according to the tactics used by these groups, rather than the nature of the actors.

Economic Warfare

Like so many other components outlined already, the concept of economic warfare is not a new one. From Napoleon's Continental System to the sanctions deployed against Iran, economic interests have been used to manipulate states into desirable behaviors. With such a long history of use, it is not surprising that there are nearly as many definitions of economic warfare as those who have attempted to define it. Definitions often focus on disruption of war-making capabilities via denial of resources or capital, or the use of economic interests in statecraft to alter behavior of other states. However, these definitions rarely mix.[180] Given the complex nature of a hybrid threat and the lack of clear delineation between war-making capabilities and diplomatic relations, these compartmentalized definitions are of little utility when analyzing a hybrid threat.

For our purposes, the definition used by DOD and many of its allies is the most useful. It states that economic warfare is: "[a]ggressive use of economic means to achieve national objectives."[181] It is worth noting that this definition neglects to mention any specific targets, tactics, or theatres. Rather, it simply adds economics to the array of tools available to the military and diplomatic strategists.

Purpose and Manifestation of Economic Warfare

The goal and means of waging economic warfare are necessarily case-specific, though there are common themes: those of resource denial or resource provision. Both can be done in the service of affecting behavior or war-making capabilities. It is important to note that, arguably more so than any other aspect of hybrid warfare, economic strategy is completely dependent on the position of both the target and source. As such, an economic strategy that a state uses against Target A could be completely different from the one used against Target B and both strategies could change in an instant as the market shifts.

Resource Denial

Resource denial is arguably the more commonly considered of the two. In this realm are tactics such as blockades, sanctions, and destruction of industry and resources.[182] These are typically used in the service of disrupting war-making capabilities and/or affecting behavior. One of the more famous examples of resource denial, albeit a failed one, was Napoleon's attempted blockade of Britain via the Continental System. The Continental System was designed to cripple Britain's economy, which would lead to political strife and therefore render it weak and ripe for conquest. This was an interesting case in that Napoleon did not deny goods from going into Britain, rather he blockaded himself and his allies, refusing the import of British goods. However, the system backfired because Britain found other markets for its goods, which proved of great benefit in the long term.[183] In this case, capital was the resource which he denied his enemies. Although the Continental System failed, its echoes are still evident in the sanction regimes of today.

Rather than denying access to specific goods, sanctions rely on the denial of trade itself. For example, Lowenthal says, "the United States attacked Cuba's economy directly as well as indirectly via a trade embargo."[184] While the U.S. embargo against Cuba has not been successful, the economic hardship that results from the imposition of a sanctions regime is often incentive enough to cause an actor to change its behavior, as is evidenced by the prospect of a cessation of Iran's nuclear program in exchange for lifting of sanctions leveled against it.[185]

Another common strategy is the control of resources that are central to a target's war-making efforts. This can come in different forms, including a contraband regime, which involves the identification of goods central to the enemy's war efforts, followed by the seizure of any of those goods if discovered en route to the enemy. Although less commonly used now than when the tactic hit its heyday in the mid-20th century, contraband regimes capitalized on civilian and military populations alike to identify and seize goods deemed central to the enemy's war-making efforts.[186] Similarly, states have used military action to destroy resources central to the war-making effort for the enemy either by destroying their own resources during a retreat[187] or targeting industry central to its production.[188]

Resource Provision

Of the two themes, this has been studied far less frequently. The first and most obvious use of resource provision for a strategic goal is the provision of goods to an ally to aid in its war-making capabilities. An example of this is the U.S.'s preemptive provision of arms and other supplies to the Allies during both WWI and WWII. Provision of strategic goods to an ally, or even a party in which the intervening state has a vested interest, during wartime, can have a dramatic effect on that actor's war-making capabilities. As such, provision of strategic goods should not be ignored within the framework of economic warfare.

An even more rarely considered manifestation of economic warfare is in the provision of key resources to a state or other actor in the interest of affecting its behavior. The behavior change could take a variety of forms, but the one most likely to be of concern within the framework of hybrid warfare is resource provision. This manifestation has the potential to discourage powerful actors who may intervene in a 'grey zone' context from taking decisive steps, in order to preserve access to that resource, as Russia does in the example below. As this method is generally undertaken in peacetime, it is often ignored when considering methods of waging economic warfare. The most prominent example of this manifestation is in the oil and gas industry, in which the oil-producing nations are able to manipulate the actions of oil-consuming states. Russia's use of this tactic is one of the more prominent examples of this economic warfare tactic and will, therefore, be explored in the following section.

Russian Use of Economic Warfare

On a smaller scale, Russia has attempted to adopt the resource denial tactic in an effort to both cripple the trade of rest of the world, and specifically NATO countries, by banning imports of foodstuffs from the U.S., Canada, and much of Western Europe. [189] The Russian government has gone so far as to destroy massive amounts of food to drive home these efforts.[190] The goal of this move could be threefold. First, it reduces the strength of the economies that rely on trade with Russia. Second, it could strengthen Russia's own food-production industry as it races to fill the gap, thus reducing Russia's dependence on foreign imports in the long term. Third, the move sends a strong message of protest against sanctions leveled on the country as punishment for its

aggression in the region.[191] However, reactions to the move have been mixed, with many expressing concern that this could push Russia close to another famine, as food prices soar under the sanctions regime.[192] Despite attempts by all the Baltic States to reduce their economic dependence on Russia, a dependence remains.[193] Given this dependence, it is not inconceivable that Russia could use resource denial tactics, particularly blockades and embargoes, in the future to weaken them.[194]

However, the cornerstone of its economic warfare strategy is resource provision, via its role as a major oil and gas supplier for Western and Central Europe, including the Baltic States. Although there was widespread, and very vocal, condemnation of Russia's actions, there was little support for taking stronger action against Russia, due in large part to the region's dependence on Russian oil and gas.[195] A halt in Russian oil and gas supply or even a spike in prices would be disastrous for the Western European economy, a fact that Russia knows as it weighs how much it is able to get away with as it expands its sphere of influence. In this, the tactic is a defensive one, relying on a deterrence of Western intervention via the threat of disruption of their oil supply.

Russia, however, needs Western Europe as a customer as much as Western Europe needs Russia as a supplier.[196] Maintenance of this influence is a key concern for Russia, as it has blocked attempts by Central Asian states to build pipelines that would bypass it entirely. Its most notable efforts include blocking potential pipelines that would run from the oil fields in Turkmenistan and Azerbaijan, through Turkey, and into Western Europe.[197]

The identification of energy production as a priority in Russia's strategy does not stop at the highest level strategy, as there were even reports of pro-Russia separatists seizing a power plant in Ukraine's Donetsk province. Moreover, cutting off supplies entirely is unlikely, as it would severely damage Russia's already limping economy.[198] Still, the threat is enough to make Western Europe consider intervention carefully. Solutions for Western Europe's reliance on Russia via clean energy or alternate sources of oil and gas are still in the medium and long term, but they are viable ones.

Diplomatic Action

While diplomacy is often viewed as the alternative to conflict, in the hybrid battle space diplomatic behavior and posturing is yet another tool employed by states in an attempt to influence the international system. The Russian Federation made very dexterous use of their diplomats throughout past conflicts and continues to engage in both positive and punitive diplomatic action in many of today's key areas of international concern.[199]

Purpose of Diplomatic Action

As a tool of state power in a hybrid conflict, diplomatic action seeks to leverage political relationships to justify behavior, garner support, discredit the claims of other belligerent nations, and strategically move forward a nation's political agenda. Diplomatic action can be geared toward both creating positive change and good will in the international system and toward punitively punishing or shaming states that have taken actions that the international system at large or an individual state does not support. Public diplomacy and public relations efforts are often the tools used to move forward positive diplomatic aims between states. To signal support or deepen relationships through diplomacy, states might sign new bilateral agreements, encourage

educational or cultural exchanges, or publically make supportive statements regarding another state's behavior. Sanctions regimes are illustrative of punitive uses of diplomacy. Energy diplomacy, particularly in the way it is used by the Russian Federation,[200] can also be an example of punitive diplomatic action.[201]

Diplomatic action, like many of the components explored in this section, has overt and covert elements. While many aspects of diplomatic action are overt, with the aim of making an international statement and moving a nation's political agenda forward, there is also extensive backroom diplomacy that occurs. Additionally, there is a personality and leadership driven element of diplomatic action that cannot be ignored. This is true both in the case of highly-centralized authoritarian states where diplomatic strategy is at the whim of the head of state, as is the case in Russia, and in Western-style democracies where diplomatic priorities and policies can change with the election of a new administration and diplomatic initiatives by the executive can be thwarted by the legislative branch. President Obama's struggle to advocate in Congress for the approval of the recent nuclear deal with Iran[202] and the Trans-Pacific Partnership agreement[203] are clear indicators that the use of diplomatic action is an instrument that democracies sometimes struggle to use as dexterously as their authoritarian counterparts, making countering this component increasingly challenging.

Russian Usage of Diplomatic Action

Two ongoing contemporary issues that show Russia's approach to engaging in diplomacy as a tool of hybrid warfare are the crisis in Ukraine and the war in Syria. In both of these circumstances, one can clearly see that the Russian regime is making active use of their diplomatic powers to try to gain international support and sympathy for their cause. In response, international opponents have taken punitive diplomatic steps to express their discontent with Russian behavior. This use of diplomatic means expresses the clear desire on the part of Western states and Russia to avoid a direct military conflict.

From a diplomatic perspective, Russia also recognizes the interconnectedness of their actions, acknowledging that steps taken in one situation can have an impact on other ongoing crises. Some have argued that dialogue between Putin and Obama at the November 2015 G-20 Summit in Turkey,[204] in the wake of the terrorist attacks in Paris just days before, could be an indicator that Russia has improved diplomatic relations with Western states or at least that other states have begun to realize the importance of working together with Russia when it comes to bringing an end to the crisis in Syria and the resulting instability that has been felt far beyond Syria's borders. This development, and the marked absence of EU and other government representatives in this bilateral meeting, could have a broader impact on Russian diplomatic activities even outside counterterrorism efforts.

Lawfare

In our international system, respect for agreed upon rules and norms underpins the relationships between states. In order to be viewed as a good faith participant in the international system, states must comply with international law. The importance of international law has only increased over time, due to both the increasingly legal focus of many nations, where litigation has become more and more common, and the increasingly interconnected nature of the world caused by revolutions in technology and communication.[205]

Definition and Purpose of Lawfare in Hybrid Warfare

Lawfare is a tactic that seeks to help states develop a legally grounded narrative that justifies their actions and couches their aggression in rational terms. This, in turn, allows the state to take any action they deem necessary while at least maintaining the ruse of compliance with the international legal system.[206] Lawfare can also be used as a tool employed by weaker parties in a conflict or non-state actors to magnify their power and to allow them to have greater influence in the international arena by making use of international laws and norms. This expands their realm of authority and the actions they are able to take.[207] The use of lawfare in hybrid warfare serves both domestic and international ends, with states making use of the law to legitimize their behavior to their people and to the broader international community in order to appear legitimate in their grievances and compliant in their behavior.

Many international legal scholars have cited the U.S.'s justification for the invasion of Iraq in 2003 as a prime example of the manipulation of international law to legitimize self-serving behavior on the part of a state.[208] While the justification provided by the U.S. for the invasion was contested by many states, the fact that the U.S. felt that it was necessary to provide an international legal reasoning behind their behavior highlights the important role that international law plays in legitimizing or delegitimizing state behavior. The conflict between Israel and Palestine has also seen both international laws and national laws applied by Israel to increase their position of power through means other than military action. By launching numerous lawsuits against Palestinian authorities in the U.S., this Israeli legal campaign has sought to exploit "loosely defined anti-terrorism laws in the U.S., [and] appears designed to exhaust the Palestinian authority's existing financial reserves and isolate it from funding sources in the region."[209]

Russian Use of Lawfare in Hybrid Warfare

A savvy participant in the international system, Russia has often made use of legal justifications to legitimize their expansionist and interventionist behavior in states from Georgia to Ukraine to Syria. The challenge in Russian implementation of lawfare, however, is that Putin's arguments often contradict themselves, showing the logic to be driven primarily by Russian self-interest and only secondarily by the actual international laws and norms citied. The legal rationale that Putin has used to justify Russian action in Crimea fundamentally contradicts the arguments he had made in the case of Syria, Libya, and Iraq.[210] Scholars have argued that Russia's stance on non-intervention and territorial integrity, highlighted by Russia's strong condemnation of Western involvement in Syria, Libya, and Iraq, only extends as far as Russian interests. Once Russian interests are threatened, as is the case in Crimea, Putin's argument about non-intervention in the internal matters of another state becomes increasingly murky.

Russian action in Ukraine is held up as the clearest example of Russian manipulation of the law to justify their behavior and action. In a report titled "Ten Myths Used to Justify Russian Policy in the Ukraine Crisis,"[211] German scholars highlight the specific arguments that the Russian government made to the international community to justify their involvement and highlight NATO's continued overstepping of its bounds and disrespect for Russian interests.[212] These myths range from "The West has meddled in Ukraine's internal affairs, organised and orchestrated the Euromaidan protests with the help of fascist groups" to "The transitional government in Kiev came to power through a coup and therefore has no legitimacy."[213] Russian behavior in Georgia in 2008 also shows their willingness to manipulate the law to make a case for intervention.[214]

Hybrid Warfare and the Netwar Theory

There has been much discussion in recent months surrounding the definition and use of hybrid warfare. Defining the phenomenon by the presence of conventional and unconventional tactics within a single campaign, these discussions typically present hybrid tactics as a menu of options available to a state. While alerting followers of conflicts in which hybrid techniques are being used to the presence and absence of certain tactics is certainly valuable, framing analysis of the phenomenon in this form misses a key aspect of hybrid warfare: the whole-of-government approach that characterizes it.

Netwar

Instead, those analyzing hybrid warfare should consider the phenomenon itself as a network, with each tactic as a node. In doing so, the hybrid conflict takes on the characteristics of a netwar, with actors of various sizes and functions interacting with each other without a clear hierarchy.[215] This networked structure is key to maintaining the ambiguous attribution that is characteristic of hybrid warfare campaigns. As predicted by Arquilla and Ronfeldt, the network is able to "swarm," attacking the target from multiple angles, and in this case using a variety of means, ultimately overwhelming it.[216] The simple menu framework is unable to accommodate this coordination and the mutual reinforcement present in the hybrid attacks that have occurred in recent history, some of which will be examined in more detail in a subsequent section of this piece. By framing it as a network, one is able to see how the different components, and indeed the actors perpetrating them, support each other and further elucidate their underlying purpose.

The Dow Jones Attack

Take, for example, the case of the cyber attack on the Dow Jones by Russian hackers in 2014.[217] Conventional analysis of the attack would characterize it as a simple cyber attack targeting Dow Jones. It notes the presence of the component 'Cyber Action' and the target 'Dow Jones.' A visualization of this understanding would look something like Figure 2.

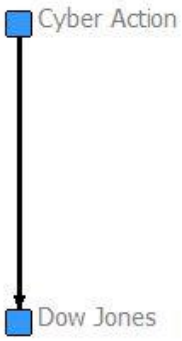

Figure 2: Simple Characterization

Here, one can understand the attack as the use of one of the tactics typically associated with hybrid warfare against Dow Jones. However, this view seems overly simplistic, as it ignores the specific means of the attack, as well as its larger consequences on the geopolitical stage.

Take, for instance, the method of attack. It did not disrupt the systems of the target news organizations, and therefore the cyber attack was not the end in and of itself. Rather, it was the means to get insider trading information. This insider trading information was specific to Dow Jones and was the aspect of the attack that was truly damaging. If Dow Jones is considered the target, and therefore the adversary, then this attack fits under the first part of our definition of an IO: gathering tactical information of the adversary. Instead of the simpler visual above, one could consider a networked reading of the attack, as outlined in Figure 3.

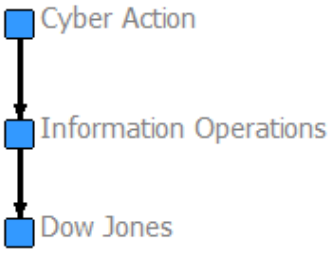

Figure 3: Network Attack

While this model is more nuanced than its predecessor, it still ignores the wider consequences of the attack. The gathering of insider trading information can certainly be for personal gain, but why Dow Jones? There are plenty of other potential targets for such an attack, particularly ones that would not be watched as carefully as this one.

Dow Jones is a staple of the U.S. stock market, an overall indicator for the health of the market itself. Therefore, any attack on it puts the market itself at risk. Moreover, the attack was done with the purpose of taking advantage of traders in the U.S. stock market. Within the context of our hybrid warfare model, this takes the form of a resource denial economic attack, as it denies capital from traders who could have potentially earned or preserved their investments via legitimate means. Both this weakening of Dow Jones, a pillar of the American economy, and the use of the economy as a weapon ultimately harmed the U.S. as a whole. As such, a more accurate visualization would likely be Figure 4, below.

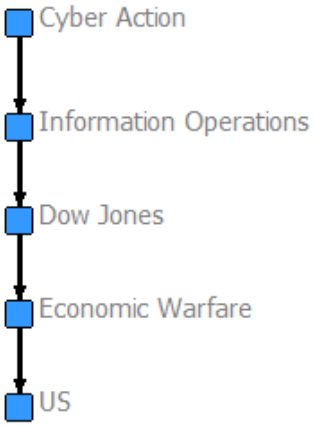

Figure 4: Broader Network Attack

Here, the presence of other hybrid warfare components is clear. It was not a cyber attack aimed at harming Dow Jones, as Figure 2 might imply. Rather, it was a cyber attack performed in the service of an IO: namely to get insider trading tips. It is through this breach of information that the attack weakened Dow Jones and, via an economic attack, the US as a whole. Here, the attack bears a striking resemblance to Arquilla and Ronfeldt's chain network, commonly found in smuggling operations.[218] In this type of network, information, resources, and in this case the attack itself, must flow from one end of the network to the other. In other words, there is no alternate path to get from the cyber attack to either of the targets without going through an information and/or economic operation.

By visualizing the attack in this way, additional vulnerabilities become apparent, particularly those exploited by the IO. If the vulnerabilities exploited by the cyber attack can be addressed, the network collapses, as seen in Figure 5.

Figure 5: Countermeasures Deployed

It is here that one can see the true value of a networked approach to analyzing hybrid threats: it offers more and clearer options for countermeasures. Rather than requiring intervention for each tactic, the network can be disrupted by securing Dow Jones against IO. In short, thinking of hybrid attacks as networked ones allows a defending actor to focus its efforts on securing key nodes against specific forms of attack in order to disrupt the entire operation, instead of countering each tactic individually. While this may seem like an overly simplified example, the more complex examples of networked hybrid warfare will be discussed in further detail in the case studies.

Russia's Hybrid Warfare Approach

While Russia does not use the term 'hybrid warfare,' instead using the term 'non-linear warfare,'[219] the 2013 doctrine laid out by General Gerasimov in the *Military-Industrial Kurier* bears a striking resemblance to a call for an institutionalized hybrid warfare strategy.[220] In this piece, colloquially known as the Gerasimov Doctrine, he argues that the character of war has changed. Wars are no longer solely CF clashing in easily delineated battlefields. Rather, they are being supplemented, and even supplanted, by a wide array of non-military measures. In particular, he highlights the use of political, economic, humanitarian, informational, and covert operations.

Gerasimov claims that Russian military strategists have a comparatively poor understanding of asymmetric warfare. To combat this, he calls upon military scientists to develop means of using asymmetric tactics to weaken the enemy's ability to fight, emphasizing the need for interagency forces aimed at employing the non-military measures outlined above. It is worth noting that he placed special emphasis on the development and use of protest populations within the enemy's territory, extending the traditional concepts of proxy warfare to include non-violent groups. Unsurprisingly, this bears a striking resemblance to the predicted evolution of netwars, blending violent and non-violent actors in the pursuit of a common objective.[221]

Despite the lack of common terminology, it is clear that the Russian Federation has set its sights on the intentional development of the nodes of its hybrid warfare network, though how these nodes interact with each other will necessarily depend on the context of the attack or campaign. Specific manifestations of this network in play will be discussed within the context of selected case studies in a subsequent section of this piece.

Conclusion

The above provides an overview of the various components associated with hybrid warfare, as well as an overview of the concept itself. Specifically, we described how Russia has used all of these components in one way or another throughout history. Finally, we provided a theoretical framework, netwar, that we believe best describes hybrid warfare and best provides a theoretical solution to countering it.

In Part II, we will dive deeper into the components and the theory by looking at three case studies: Crimea, Estonia, and the South China Sea. We will then provide a fictional case to better describe how we believe an effective hybrid strategy would be deployed in the Baltic.

Part II

Case Studies

Introduction

In part I of this project, we looked at the components of hybrid warfare and the netwar theory. In the following cases we will provide a summary of the case, an analysis of how hybrid techniques were used in the case, a look at how each case fits into the network theory construct, and the responses from actors in the international community to the hybrid techniques. We chose two cases where the Russians used hybrid techniques against their neighbors in Ukraine and in Estonia. Our final case is outside of Eastern Europe and describes how China and other co-claimants in the South China Sea are using hybrid warfare to accomplish political goals.

Crimea: A Successful Case

The Russian annexation of the Crimean Peninsula, which had been under the control of the Ukrainian government since the fall of the Soviet Union, came as a shock to most of the world. Many thought that these unilateral annexations had vanished from a modern, peaceful European continent. However, the Russian government, and its leader Vladimir Putin, proved that this view of the disappearance of realpolitik actions in Europe was a fallacy. Instead, the annexation of Crimea and Russia's role in propelling the crisis that eventually led to the annexation compose our most recent and conclusive example of a successful case of Russian use of hybrid warfare techniques to achieve a political goal. However, because the case is so recent, much of the most useful information about Russian actions within Crimea has not been made public. Therefore, this case study relies on media reporting, statements by the Crimean and Russian governments, and academic analyses from both Europe and the United States.

Background

Political Crisis in Kiev

The Russian annexation of Crimea began with the Ukrainian political crisis that gripped the country and most of Europe from the end of 2013 into 2014. The key inciting incident came when Ukrainian President Viktor Yanukovych declared that Ukraine would no longer pursue a trade deal with the EU and instead would look to the Russian Federation for improved trade ties.[222] Since the fall of the Soviet Union, there has been an ideological and political battle within Ukraine about its relations with Russia. Many, and most in the western regions of the country, wanted to move closer to the EU and the U.S. by integrating through trade and military deals, while many in the eastern provinces, especially those of Russian ethnic origin, wanted the government in Kiev to move closer to Putin and Russia. This ideological and political battle would have practical consequences following the November 2013 announcement on the trade deal by Yanukovych. With the announcement, anti-government protests began in Kiev, and by 1 December, those protests included more than 300,000 Ukrainian citizens.[223]

As the protests continued to get larger and more intense, Putin attempted to bolster the Yanukovych government. On 17 December, he announced that Russia would buy $15 billion worth of Ukrainian government bonds and would cut the cost of Russian natural gas flowing to

Ukrainian markets.[224] Over the following two months, the protests continued to rise in intensity, with the protesters at one point taking control of the Kiev City Hall until political prisoners were released.[225] The Yanukovych government's response also became increasingly hard-lined. Opposition leaders were imprisoned and tortured while street protesters were being shot by snipers from Kiev rooftops.[226] The worst days of fighting were 19 and 20 February. In 48 hours, more than 88 people were killed on the streets of Kiev.[227] The next day, the political opposition, the protesters, and Yanukovych agreed to a new government in which the president's powers were significantly slashed and the opposition leader Yulia Tymoshenko was released from prison.[228] This was a significant step forward, however the country never saw how this arrangement would function because Yanukovych fled Kiev the same day.[229]

Problems Begin in Crimea

As Yanukovych fled, the opposition, with their protester allies, solidified their control over the Ukrainian government. On 23 February, the Ukrainian Parliament, now controlled by the political opposition, shifted presidential powers over to the new speaker of the parliament, Oleksandr Turchynov.[230] In response to these changes in Kiev, pro-Russia Crimean citizens began protesting on the peninsula against the new government.[231] On 25 February, a pro-Russia Crimean, Aleksey Chaly, was appointed the mayor of the largest city on the Crimean peninsula, Sevastopol.[232] Besides being a population center on the peninsula, Sevastopol is also the site of the Russian Black Sea Fleet and is the traditional warm-water port of the Russian Navy.[233]

As protests in Crimea intensified, clashes occurred between pro-government citizens, like the Crimean Tartars, and pro-Russia Crimeans. On 27 February, armed pro-Russia protesters seized Crimean government buildings in Simferopol and the Russian government granted refuge to Yanukovych.[234] This action by the Russian government further inflamed the anti-Russia sentiment in Kiev and invigorated the pro-Russia protesters in Crimea. The next day, men in unmarked uniforms seized the Simferopol International Airport and the military airfield outside of Sevastopol.[235] As the pro-Russia armed men moved against the Ukrainian government in Crimea, the Russian government began to formally intervene in the conflict.

Russia Intervenes

On 1 March, the upper house of the Russian Parliament approved the use of military forces by Putin in Ukraine. The next day, Russian troops entered Crimea.[236] Concurrently, the Russian Black Sea Fleet informed the Ukrainian Navy in Sevastopol that they must surrender or face an attack from Russian forces.[237] While the Russian government had issued statements regarding the legality of the Ukrainian actions in Kiev, these two actions were the first military responses to the collapse of its pro-Russia government in Kiev. However, many would argue that these were not actually the first military actions taken by Putin's government; instead, these analysts would point to the seemingly pro-Russia Crimean protesters and their armed and uniformed comrades who seized government buildings and military assets throughout the peninsula.

On 4 March, during his first public statement on the Ukraine crisis, Putin declared that Russia reserved the right to use any means necessary to protect its citizens in eastern Ukraine.[238] The same day, Russian forces fired warning shots at unarmed members of the Ukrainian military who were on their way to the military airbase outside of Sevastopol.[239]

Crimean Separatists Take Political Action

The Crimean Parliament had already set a public referendum for independence for a future date, but with the clear military and political support indicated by Russia's actions during the first week of March, the Crimean separatists began taking actions to secede from Ukraine and join the Russian Federation. On 6 March, the Crimean Parliament[240] voted unanimously to secede from Ukraine and join Russia.[241] The next week, on 11 March, the Parliament adopted a declaration of independence from Ukraine. Over the following week, the Crimean government moved toward the 16 March referendum date. Despite calls to cancel by the international community, the Crimean separatists went ahead with the vote, which according to the separatists, resulted in approximately 95 percent of the Crimean population voting in favor of secession and federation with Russia.[242] Most members of the international community challenged the result, but the Russian Federation recognized it and moved forward with the annexation.

The Annexation

On 17 March, the Russian government recognized Crimea as a "sovereign and independent" country.[243] The following day, Putin, Crimean Prime Minister Sergey Aksyonov, Chairman of the Crimean State Council Vladimir Konstantinov, and Mayor of Sevastopol Alexey Chaly, signed a treaty of reunification, which completed the annexation of the Crimean peninsula by the Russian Federation.[244] While the formal annexation of the peninsula was certainly not the end to the Russian-Ukrainian conflict in 2014, it does provide a good ending point for our discussion of hybrid warfare in Crimea. In the following section, we will dive deeper into the history described above and analyze the ways that Russia used hybrid techniques to destabilize and then eventually annex the Crimea.

Analysis of Key Components Used

Below are several hybrid techniques deployed by Russia during the Crimean crisis. While we describe these techniques independently, it is important to remember that they are part of a broader, networked approach that focused on one specific political goal: the annexation of Crimea. This networked approach will be highlighted in the following section.

IO or Strategic Communications

Of all the components used by Russia during the annexation of Crimea, the information component was the most far-reaching and diffuse. IO, or strategic communications, were used by all Russian actors in a coordinated approach to make way for the annexation. As an example of the coordinated nature of this strategic communications approach, we can look at an analysis done by Maria Snegovaya at the Institute for the Study of War. She writes:

> For example, contemporary analysts describe Russia's current campaign of obfuscation as the 4D approach: "dismiss- as Putin did for over a month with the obvious fact that Russian soldiers had occupied Crimea in the Russian 'news;' distort- as an actress did in playing the role of a pro-Russian Ukrainian; distract- as Russian media did with ludicrous theories about what happened to Malaysian Airlines Flight 17; dismay- as Russia's ambassador to Denmark did in March when

> he threatened to aim nuclear missiles at Danish warships if Denmark joined NATO's missile defense system."[245]

This coordinated approach is part of a Soviet-era IO strategy called reflexive control. Reflexive control is designed to cause a "stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[246] The reflexive control strategy was aimed at Western countries during the Crimean crisis in an attempt to prevent those countries from taking actions to prevent the annexation. It also shows that, in hybrid war, potential target actors for hybrid techniques go beyond your adversary on the battlefield and target actors who have the potential to become players in the conflict.

In addition to the IO targeted at the West, there were also significant efforts designed to consolidate the support of Russian domestic populations behind the annexation, as well as smooth the way for annexation by targeting strategic communications toward the Crimean population. For example, later in the conflict, according to the same report from ISW:

> Russian domestic and international media channels actively misrepresent events in Ukraine, calling the Ukrainians 'Banderites'[247]…describing them as the fascist junta, and claiming they committed atrocities that never happened, the most notorious being the alleged crucifixion of a boy in the city of Slovyansk. Some pro-Kremlin journalists went so far as to allege that Ukrainian forces were mailing residents of separatist-held Donetsk the severed heads of their relatives.

These descriptions of the Ukrainian government as fascist and brutal serve a dual purpose, both by infecting the Russian domestic population with righteous outrage and by injecting fear into the hearts of the Russian ethnic minorities in places like Crimea or the Donbas. It is important to note that these efforts are coordinated through the central node of the government. The Russian media and the Russian government should not be seen as independent entities.

Finally, as we continue to document the other components used below, many of the components that will be described also have an information component and feed into this overall approach directed by the Kremlin. We will provide a visualization of this interconnection in a following section.

Lawfare

International law was a central part of the hybrid strategy used by Russia in its annexation of the Crimea. As we explained in Part I of this report, lawfare is "a tactic that seeks to help states develop a legally-grounded narrative that justifies their actions and couches their aggression in rational terms. This, in turn, allows the state to take any action they deem necessary while at least maintaining the ruse of compliance with the international legal system."[248] Within hybrid warfare strategy, lawfare works to help justify the actions taken in other arenas and to help solidify the claims an actor has for a particular political goal.

From the very beginning of the Crimean crisis, the West and the broader international community used legal and normative arguments to explain why Russia's actions were illegal. According to international observers: "By annexing Crimea, Vladimir Putin has violated the fundamental texts of the United Nations, the statutes of the Council of Europe of which Russia is a member, at least two regional treaties that established peace in Europe and two bilateral treaties

signed with Ukraine, as well as the Constitutions of Ukraine and Crimea."[249] In addition to these formal documents, Russia also broke various international norms. Putin and his government did not acknowledge that they had broken international laws. Instead, they used a bastardized view of international law to justify their actions. The following are examples of how the Russian Federation used legal arguments to justify their actions in Crimea:

- *The Kosovo Precedent:* Putin argued that the secession of Kosovo from Serbia in the 1990s provided an international legal precedent for the secession of Crimea from Ukraine in 2014.[250]
- *The Illegal Transfer:* Putin argued from the beginning that the original transfer of Crimea from Russia to Ukraine by Nikita Khrushchev in 1954 was illegal under Soviet law. Thus, the annexation of Crimea by Russia corrects this illegal action.[251]
- *Illegal Seizure of Power:* Putin argued that the Ukrainian government illegally seized power from the elected government of Victor Yanukovych, thus the actions Russia took to defend Russians in Crimea were justified. He argued that this shows that the West only supports international law when it suits their views.[252]
- *Western Precedent:* Putin pointed out that the actions of the West in Afghanistan, Iraq, and Libya provided Russia with the necessary precedent to intervene in Crimea.

These justifications are all based in legal arguments and precedents for action. Overall, since there is no central international legal authority that they had to justify their decisions to, these arguments were, in many ways, directed toward the domestic Russian population and Western audiences.

Political Action

Political action was used extensively by the Russians as they prepared for and then executed the annexation of Crimea. As a reminder from Part I, political action is a type of covert action aimed at influencing political leaders or the political situation in other states. Political action comes in two forms: support to influential political elites or parties, and influence and infiltration of established political regimes. The Russians used both to turn the situation in Crimea in their favor. While we likely will never know the full extent of the covert actions taken by the Russians in this realm, we can surmise where these two streams of political action were used during the Crimea annexation.

The Kremlin's connection to and influence over the pro-Russia separatists in Crimea was clear from the beginning. That connection became full-fledged support in the middle of the crisis when the separatist leaders were invited to Moscow.[253] The best example of this support and influence is the story of Sergey Aksyonov, the man who would eventually become the prime minister of an independent Crimea. Aksyonov was a little known politician prior to the crisis, even in Crimea.[254] He led the Russian Unity Party in Crimea,[255] which controlled only three seats in the regional legislature and had no seats in the parliament.[256] However, his connection to the Kremlin and the clear influence that the Russian government had over him and his party was significant.[257] He was Putin's man in Crimea.

Aksyonov eventually came to full power when masked men seized the Crimean parliament, likely under his orders.[258] Hours later, he entered the parliament building, spoke with the masked men, and then proceeded to allow only parliamentarians who were aligned with his party to enter the building.[259] While, according to *Time*,[260] Aksyonov had never met with Putin, the influence

that the Kremlin had over his actions was clearly significant, although we do not know the specifics. In terms of infiltration of the political parties by Russian agents, we probably will never know the full extent of this activity; however, we can assume that there were likely Russian agents throughout the support structure of the Crimean political establishment.

Overall, the Kremlin used both streams of political action to great effect in Crimea. While it seems as if they focused their support on Aksyonov and his pro-Russia party, presumably there were other targets of influence and infiltration Russia would have deployed had Aksyonov not been compliant.

Military Operations—SOF

The use of SOF by the Russian government in Crimea has been essentially confirmed by the international community and Russia. These 'little green men,' as they came to be known because of the color of their fatigues, were Russian operators sent into Crimea to advance the destabilization and annexation process, by supporting local proxy organizations and working independently on operations. Specifically, these soldiers manned checkpoints and barricades throughout the peninsula and took key government buildings.[261] They also served administrative purposes. For example, while this came later in the battle for the Donbas, the BBC interviewed a 'little green man' who had become the military commandant of Kramatorsk, a small city in eastern Ukraine.[262]

These 'little green men' carried modern Russian-made light and heavy weapons but had no insignia on their uniforms,[263] so while they looked and spoke like Russian SOF, in actuality no one could definitively prove that they were not part of the Crimean resistance or individual Russian citizens who came to Crimea to help free it from Ukraine. President Putin doubled down on the ruse by stating emphatically that these forces were not Russian but in fact Crimean self-defense forces.[264] As we described in Part I of this report, this ambiguity in the use of SOF is key to their effective use.

These forces also served the role of preparing the battle space for the eventual insertion of Russian CF later in the conflict. They worked with pro-Russia Crimeans to secure a variety of critical infrastructure that allowed these forces to move into Crimea quickly and en masse. Specifically, the Russian special operators focused on securing the airfields in both Simferopol and Sevastopol.[265] They also secured naval and land points of entry to the peninsula.[266] Their efforts to prepare the battlefield were key to the implementation of the hybrid strategy in Crimea.

Military Operations—Conventional Forces

As with most hybrid strategies, CF played the biggest part at the end of the crisis. While Russian conventional naval forces were already present in Crimea as part of the Black Sea Fleet, ground forces did not enter the conflict until later. One of the first large deployments of troops occurred on 28 February, when approximately 2,000 Russian troops were flown into Crimea. According to Serhiy Kunitsyn, the Ukrainian president's special representative in Crimea, "Thirteen Russian aircraft landed at the airport of Gvardeyskoye [near the city of Simferopol] with 150 people in each one."[267] These forces would be followed by others as the crisis grew toward annexation, but this first large deployment was seen by the Ukrainian government and most observers in the West as the initial Russian 'invasion' using CF.[268] These troops were used to seize Ukrainian

government buildings and military bases.[269] Where the 'self-defense forces' could not fully expel the Ukrainian government from the peninsula, the CF could.

In addition to the actual use of these forces, the Kremlin also used the threat of conventional intervention as part of its hybrid strategy in Crimea. As indicated in the IO section above, the threat of CF served as a significant information warfare tool against the Ukrainian government and against their Western supporters. Overall, the threat and, then later, use of Russian CF played a big part in their Crimean strategy.

Economic Warfare

Russia directly used economic warfare against the new Ukrainian regime; however, economic warfare was not directly instrumental in the annexation of Crimea. Instead, we look at economic warfare as a long-term destabilization effort on the part of Russia against the Ukrainian state.

After the fall of the Yanukovych government in Kiev, the Russian Federation and their client gas companies began to threaten the new Ukrainian government with a complete shutoff of gas to the country.[270] This threat was not new, and represents a continuous, hostage-like relationship between Ukraine and Russia on economic matters. While the Kremlin did have a good relationship with Yanukovych, they still used economic warfare, specifically focused on the energy sector, to control his actions and keep the Ukrainian government subservient to the desires of the Kremlin. For example, they provided Yanukovych steep discounts on gas imports to keep costs for his citizens down and his popularity up.[271]

Prior to Yanukovych, the Russians had used the same strategy throughout the 2000s with a gas supply crisis between the two countries nearly every year since 2005. Primarily, disputes between Russia and Ukraine focused on lack of payment by Ukraine to Russian firms, however, it is clear from these disputes that Russia engineered problems into the deals that were made with the Ukrainian government. These disputes and the resulting restrictions on gas supplies to Ukraine not only destabilized the Ukrainian government but also served as an information warfare tool. It showed the Ukrainian people that Russia was in control and that the Ukrainian government could not be trusted to provide energy supplies for its own people.

Overall, economic warfare used by Russia was not directly linked to the annexation of Crimea, but like most aspects of hybrid warfare, the indirect connection is just as important. In the end, the long-term destabilization of the Ukrainian state using economic warfare helped Russia annex Crimea.

Network Analysis

It is clear from the narrative above that many components and targets within the attack were mutually reinforcing. When modelled as a network in Figure 6, the complex structure of the attack becomes even more clear.

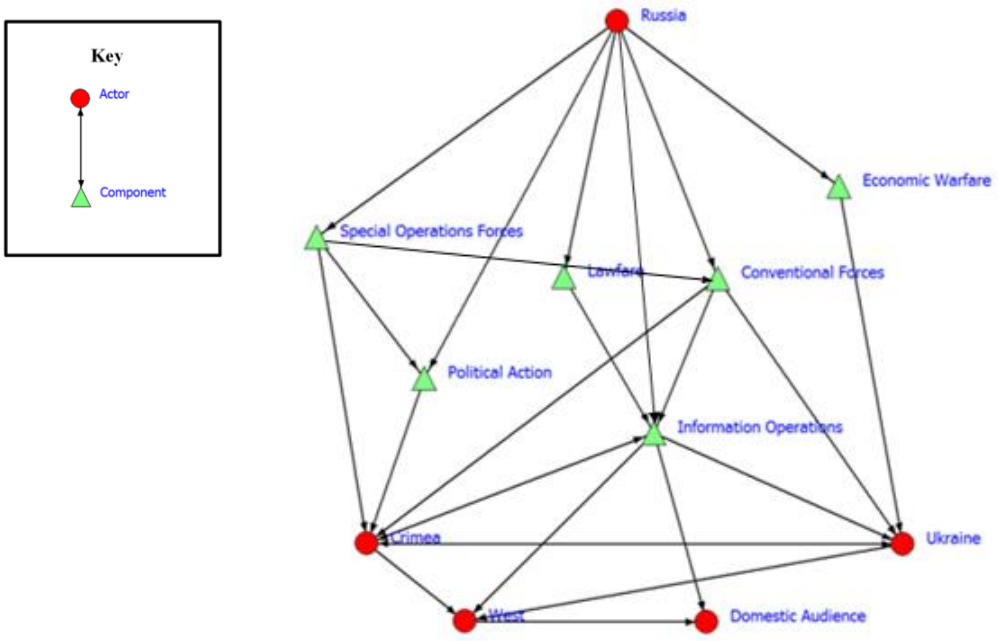

Figure 6: Crimea Network Map

Particularly notable are the relationships between the targets, as an attack on one would often contribute to action against another. For example, the campaign often used the attack against Crimea to target a wider audience. Moreover, certain components were used extensively in the support of others, culminating in a highly interdependent attack. To further illustrate these relationships, the analysis will turn to the networks of two components in particular: SOF and IO.

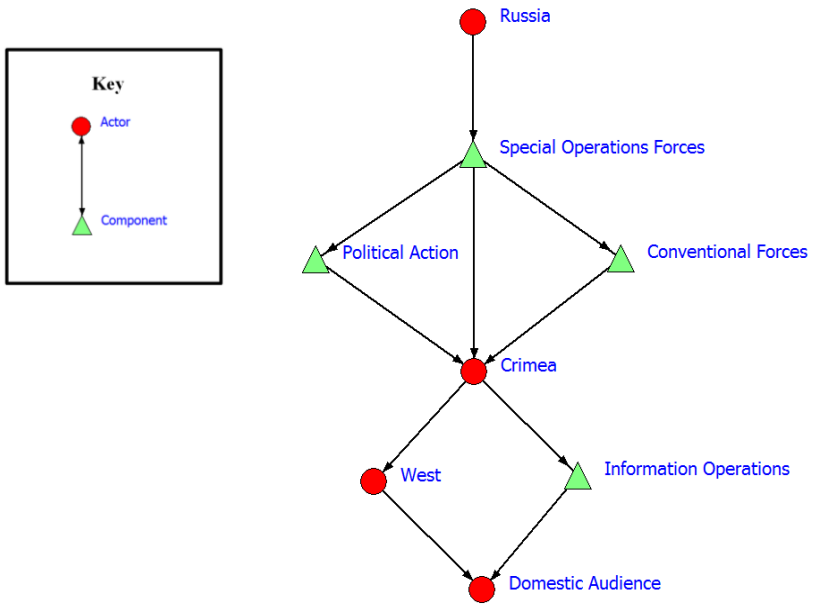

Figure 7: Crimea Special Operations Forces Network Map

In Figure 7, one can observe the far-reaching effects of SOF within the wider campaign. The presence of these forces became something of a sensation in the coverage of the Crimean campaign, though their use often focused more on their presence in the battle space than their actual actions. However, they were also instrumental in both preparing the battlespace for future CF and in inspiring the political action that would facilitate Crimea's eventual secession from Ukraine and annexation by Russia.

All three components then converged on Crimea, significantly affecting the wider campaign. Interestingly, the wider Crimean campaign was then used, in turn, as both a symbolic blow to the West and within a wider IO aimed at the Russian domestic population to shore up support for the regime. This relationship between the status of the West and domestic support for the regime is also reflected in the relationship between the West and the Russian domestic population. In short, SOF were instrumental in laying the groundwork for a chain of events that would touch the legitimacy of Western influence in the region.

Similarly, the IO used within the campaign had both origins and results that were far-flung and complex. Although Russia did directly wage an information campaign in the region, targeting ethnic Russian populations in Crimea, and in Ukraine as a whole, it had a more indirect effect on both its domestic audience and those of the West as a whole, as shown in Figure 8, below.

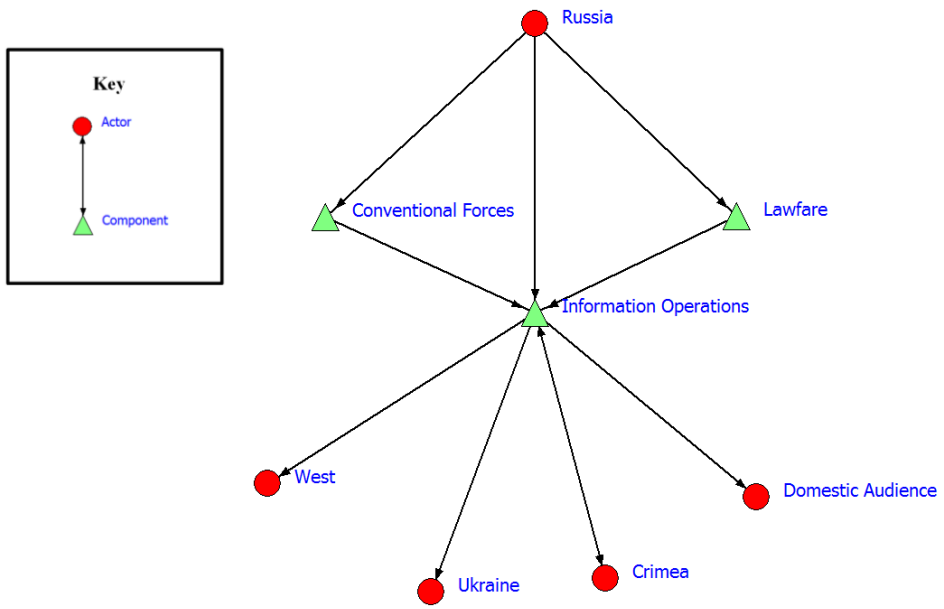

Figure 8: Crimea Information Operations Network Map

Through its conventional warfare campaign, Russia was able to signal that it is still a major conventional player in Eastern Europe. This has the double effect of providing a show of strength to the Russian people, who traditionally respect strong leadership and signaling to the West that attempts to meet Russia in conventional conflict would not be as easily handled as previously believed. Moreover, its use of legal norms in the international system increased the legitimacy of its actions at home and abroad, while signaling that it can beat the West at its own game. Far from

being cowed by an international community that has regarded it as a fading star, Russia used the Crimea campaign to communicate that it was an active player on the international stage.

Responses from the International Community

Ukraine

Ukraine's response to the hybrid tactics used during the annexation of the Crimea was two-fold: rhetoric and action.

Like most countries in the international community, Ukraine described Russia's actions in Crimea as illegal and demanded that they withdraw their forces from the peninsula.[272] They repeated this rhetoric throughout the crisis in an attempt to get Western states involved. Specifically, the government began to compare the Russian actions in Crimea to those of the Russian Federation in Georgia in 2008. The Ukrainian interior minister, Arsen Avakov, said: "I see what has happened as a military invasion and occupation in violation of all international treaties and norms … This is a direct provocation aimed at armed bloodshed on the territory of a sovereign state."[273] Following the annexation, Ukrainian Prime Minister Arseniy Yatsenyuk put it simply when he said that the annexation was "a robbery on an international scale."[274]

In terms of action, Ukraine had few options once Russia had decided to annex the peninsula. Ukraine could not risk open war with its neighbor and, because of Russian shaping operations in Crimea, the new government could do little beyond the rhetoric above to dissuade Crimeans from voting for the referendum to join Russia. However, after the annexation was formalized, Ukraine could take action against Russian occupation.

Crimea is reliant on electricity and water from Ukraine to function. Approximately 85 percent of Crimea's fresh water supply and nearly all electricity come from Ukraine.[275] Additionally, Ukraine controls the transportation routes to and from Crimea, which allowed the government to limit the ability of commerce to pass between the peninsula and Ukraine.[276] Ukraine took direct actions against the new government in Crimea using all three of these sources, along with several others. In April 2014, Ukraine cut off fresh water and electricity access to the peninsula.[277] The Ukrainian government also shut off all over-land access to Crimea.[278] At least one goal of these actions was to show that the Russians could not live up to the promises they gave to the Crimean people prior to annexation. Since this action was non-kinetic there was less of a risk of inciting open war—although near open war was already occurring in the Donbas.

Unfortunately, all of these actions were too late to stop the Russian hybrid strategy from being successful in annexing Crimea. While these responses were an attempt to counter the arguments being made by the Russians, Russian control over Crimea was secure at this point in the crisis.

European Union

The EU responded to the Russian annexation through condemnation before, during, and after the Russian intervention and annexation. On 17 March, the EU, working with the U.S., established visa bans and froze the assets of individuals involved in the Crimean separatist movement.[279] On 18 March, President of the European Council Herman Van Rompuy and President of the European

Commission José Manuel Barroso issued a joint statement formally condemning Russia's actions in Crimea. They wrote:

> The sovereignty, territorial integrity and independence of Ukraine must be respected. The European Union does neither recognise the illegal and illegitimate referendum in Crimea nor its outcome. The European Union does not and will not recognise the annexation of Crimea and Sevastopol to the Russian Federation.[280]

Later, the EU would work with the U.S. to implement economic and political sanctions against the Russian economy and members of the Russian government. Additionally, the EU would work with the Ukrainian government to support it economically against Russia's actions. The EU did this through loan forgiveness and trade packages.

Like many multi-lateral institutions, the EU is hurt by its inability to act quickly and its impact is limited by the support it has from constituent member states. For example, during this crisis, the constituent members, especially Germany, proved to be much more important in responding to Russia's actions. Additionally, as a non-military alliance, the EU had limited ability to respond to the military and covert actions taken by Russia in Crimea. However, the EU did have significant ability to punish Russia for its actions. Along with the U.S., the EU implemented targeted sanctions against members of the government and against companies, especially banks, with significant ties to the state.[281] However, the targets of these sanctions were limited by EU member states' reliance on Russian natural gas.[282] No Russian energy firm was targeted despite Russia's reliance on fossil fuel income for foreign currency reserves and economic growth. The implementation of these sanctions was an attempt to hurt the Russian economy and to force it to reverse its actions in the Crimea, but it was not a direct response to Russia's hybrid techniques in Crimea.

The EU did combat the Russian hybrid technique of economic warfare by providing Ukraine with several financial lifelines when the country neared default.[283] Additionally, the EU proposed a trade package with Ukraine to bolster its economy against the actions being taken by Russia, including cutting off natural gas shipments and calling in Ukrainian bonds.[284]

Overall, the EU reacted too slowly to provide any tangible counter to Russian hybrid strategy in the Crimea. The EU does not have the threat of military force behind its actions and thus it could only use economic means to try to counter Russian actions. However, because of the EU structure, even these economic actions came too late to have any effect on the Crimea crisis.

Germany

As the Crimean crisis took form, the German government approached the problem pragmatically from its perspective, but for many Russia hawks in the western world, this approach appeared weak and dangerous.[285] Germany's economy was and is reliant on Russian natural resources to drive its industry, as Russia is the leading import source for the three main energy-producing fuels: natural gas, crude oil, and coal.[286] Thus, when approaching the Crimean crisis, the Germans did not react quickly against Russia. Instead, they used a slow approach that focused on limiting Western sanctions against Russia and looking for a peaceful solution to the problems through diplomatic negotiations.[287] The Germans viewed any other action as an approach that would drive Russia further into isolation, leading to an increase in the West-versus-Russia mentality that pervades the current relationship. At the heart of this action was German Chancellor Angela

Merkel's relationship with Putin. She spoke directly with him often in the lead-up to the annexation, attempting to de-escalate the situation.[288]

In many ways, the German actions around Crimea and the broader Ukraine crisis showed that Germany could take the lead on issues in European foreign policy. They have the diplomatic clout and economic power to be a strong foreign policy player.[289] However, the crisis also showed Germany's weaknesses: its reliance on Russian natural resources and its lack of a military option when discussing potential responses to aggression in its sphere of influence.[290] Overall, Germany's reaction to the hybrid techniques used by Russia in Crimea was slow and ineffective, given the goal of preventing the annexation.

United States

Like the EU and Germany, the U.S. limited its response to Russian actions in Crimea to rhetoric and support to the Ukrainian government. Since Ukraine was not a member of NATO, the U.S. government was not willing to risk open war with Russia over the Crimean Peninsula.

Rhetorically, the U.S. response was very similar to that of the EU and of Germany. They declared the actions taken by the Russians to be illegal under international law and said that any use of force would be met with grave consequences.[291] Specifically, Secretary of State Kerry told Russian Foreign Affairs Minister Sergey Lavrov that: "continued military escalation and provocation in Crimea or elsewhere in Ukraine, along with steps to annex Crimea to Russia, would close any available space for diplomacy."[292] The State Department, and the U.S. government as a whole, became even more forceful in trying to counter the IO used by Russia. Specifically, they focused on debunking the Russian claim that its actions were legal under international law.[293] The State Department went so far as to say that Russia was spinning a "'false narrative to justify its illegal actions in Ukraine" and accused Russian President Vladimir Putin of disseminating myths about the crisis. "The world has not seen such startling Russian fiction since Dostoyevsky wrote, 'The formula "two times two equals five" is not without its attractions.'"[294]

In terms of actions taken, the U.S. spearheaded the implementation of sanctions against Russian companies and government officials who were seen as key enablers of the Russian annexation.[295] With some cajoling, the U.S. was also able to get its European allies on board with the action.[296] In addition to the sanctions, the U.S. Congress approved $1 billion in loan guarantees for the government of Ukraine and the U.S. military suspended all military-to-military contracts with the Russians.[297] Also, the U.S. government suspended all bilateral trade meetings and put on hold the planning for the G-8 summit that was meant to take place in Sochi, Russia.[298] These actions combined were meant to put enough financial and international pressure on the Russian regime so that it would pull back its forces from Crimea and reverse the annexation process.

Overall, these actions were unsuccessful in preventing the hybrid strategy used by Russia in Crimea. Instead, the rhetoric led to a 'he said, she said' situation, in which one side would claim that the other was violating international law through its actions. Neither side was able to convince the other of the merits of its arguments.

NATO

NATO's response to Russia's actions in Crimea and the annexation were limited because of Ukraine's status as a non-member of the alliance. While Ukraine had expressed interest in joining NATO in 2008, there were many barriers to entry for the country.[299] If Ukraine had been a member,

NATO's Article 5 mutual defense agreement would have required action from the alliance against Russia for its actions in Crimea. Instead, NATO could do little but issue a condemnation. NATO Secretary General Anders Fogh Rasmussen, stated:

> Russia has disregarded all calls to step back into line with international law and continues down the dangerous path. Russia continues to violate Ukraine's sovereignty and territorial integrity, and remains in blatant breach of its international commitments. There can be no justification to continue on this course of action that can only deepen Russia's international isolation. Crimea's annexation is illegal and illegitimate and NATO Allies will not recognise it.[300]

In addition to the condemnation and rhetoric, NATO was able to do little else to directly counter Russian actions in Crimea. However, the alliance did cut its cooperative exchanges with Russia. It also provided increased partnership opportunities with the Ukrainian government and sent AWAC aircraft to southeastern Europe to help observe the Russian movements in Ukraine.[301] Beyond these steps, the alliance did little else to substantially counter Russian actions.

United Nations

The UN reacted to the crisis in Crimea in the way that it most often reacts—with a meeting. On 28 February, the same day that armed, uniformed men captured the Ukrainian airbase outside of Sevastopol and the civilian international airport, the UN Security Council (UNSC) met in a closed door meeting to discuss the crisis.[302] On 15 March, members of the UNSC voted overwhelmingly to condemn the Crimean independence referendum set to be held the next day, however Russia vetoed the resolution, so the UNSC response to what many on the council called an illegal vote was nothing.[303] With the continual block by Russia of all resolutions on Crimea in the UNSC, opponents of the annexation went to the UN General Assembly (UNGA), where they were successful in passing a resolution stating that the annexation was illegal.[304] However, because of its inability to enforce, the UNGA's resolution did nothing to reverse the actions that had already been taken.

In terms of responding to Russian hybrid techniques in Crimea, the UN, through its actions, was attempting to combat the lawfare being used by the Russian Federation in support of their actions in Crimea. If the international community, under the banner of the UN, was able to declare that the actions taken by the Russian government were in fact against international legal norms,[305] then there may have been some legal or other recourse under the auspices of the international community for Ukraine against the annexation. However, because Russia was able to block all but the most toothless resolutions in the UN, the UN failed in combatting the hybrid strategy used in the Crimean crisis.

Conclusion

The simple answer to the question of whether the responses of the international community were successful in combatting Russia's hybrid techniques during the Crimean crisis is no. While the international community has been able to make Russia suffer economically for its indiscretions in Crimea, they were not able to successfully counter the techniques that Russia used so successfully to gain Crimea.

The case of Crimea is a clear victory for the Russian hybrid warfare strategy. The Kremlin had two specific political goals: destabilize Ukraine and annex Crimea. They were able to accomplish both goals by deploying a coordinated series of hybrid tactics, all focused on impacting actors who had control over these goals. Overall, we believe that, while the lessons that can be learned from Crimea must be taken with a grain of salt because of the unique nature of this case, it is still worth looking at this case to see how the Russian government is implementing and constantly improving their hybrid strategy.

Estonia: A Focused Case

When asking Estonians about the current Russian hybrid threat, you will hear many different opinions about Russia's true intentions, planned actions, and desired end state. However, despite this variety of viewpoints, there remains one fact on which all are in agreement: the threat from Russia is nothing new and it all goes back to a fateful winter morning in 1924.

Background: Hybrid Tactics Through History

On 1 December 1924, Estonian communist supporters, largely infiltrated by the Soviet Union, attempted to stage a coup that continues to live in infamy in Estonian collective memory. The roots of this coup started in the spring of 1924, when the Soviet Union sent 60 Razvedupr intelligence officers to Tallinn, the capital of the newly independent Estonian state. These operators were tasked with helping to organize and inspire the uprising.[306] Many of the ambitious plans developed for the coup were derailed by the Trial of the 149 in November 1924, during which authorities brought charges against 149 communists in Estonia. The proceedings resulted in numerous convictions and a substantial culling of the local communist ranks.[307]

Undeterred, the coup was launched early in the morning on 1 December, with coordinated attacks occurring at the Estonian National Defence College outside of Tallinn, a main railway station, and Toompea Castle, which housed numerous government functions including the office of the State Elder (head of state) and the Riigikogu (parliament).[308] Despite the significant level of chaos caused by the initial string of attacks, the siege itself lasted only five hours before government forces were able to retake all captured buildings from the insurgents. In total, 12 rebels and 21 civilians were killed in the attacks.[309] In the end, it is estimated that about 250 rebels participated in the coup attempt, more than 100 of whom were captured, court martialed, and found guilty of treason.[310] The failure of the coup was due largely to the false belief that the workers and soldiers would fall in line with the insurgents and help them seize the capital.[311] This strategic miscalculation allowed the Estonian government to reassert control. In the aftermath of the coup, the Estonian Defence League, a National Guard–style voluntary military organization, was reinvigorated. This organization remains active in Estonia to this day.[312]

Despite the Estonian security force's ability to hold off this coup attempt and the general population's unwillingness to join the rebellion as the communists had hoped, this uprising was still deeply jarring for the Estonian people. The legacy of deep-rooted Russian meddling in Estonian internal affairs may have reached a high point in this Soviet-sponsored insurgency, but it is far from over, and the concerns about Russian non-conventional tactics within Estonia's borders still remain.

Ever since breaking free from the Soviet occupation, which lasted from 1940 until 1991, Estonia has faced numerous threats from its eastern neighbor. Russia's strategy in Estonia has been one of attrition. Rather than there being only one decisive event that epitomizes this expression of hybrid warfare in Estonia, Russian actions have been an attempt at death by a thousand cuts, making use of a variety of hybrid tactics across decades to influence Estonia in a wide range of spheres through a wide range of means. The most notable of these activities occurred in 2007, when a debilitating cyber attack shut down several key sectors in Estonia. By examining this case in detail, one can see clearly that the threat Russia poses to the Baltics, even by non-conventional means, cannot be ignored.

Background: The Cyber Threat

Estonia: A Cyber Nation

Today, Estonia is among that most technologically advanced and wired countries in the world.[313] After the collapse of the Soviet Union in 1991, Estonia lacked even basic technological services, with less than half of the nation having a telephone line.[314] Since that time, the cyber industry in Estonia has boomed, with many key politicians, including recent President Toomas Hendrik Ilves, recognizing the potential force multiplying effect that increasing cyber capacity could have to compensate for Estonia's small population.[315] Estonia is the birthplace of Skype and Kazaa (an early file-sharing network),[316] and serves as the home to numerous cyber security companies.

Estonia's society and economy are largely driven by the Internet, with many key social services now managed digitally, including e-voting, which Estonia pioneered in 2007.[317] This system allows Estonian citizens to vote from any location by using an Estonian ID card that is inserted into their computers. This card allows them to vote online, transfer money, and access their information file held by the Estonian state.[318] Beyond just government systems, 99% of Estonian bank transfers are conducted online[319] and doctors prescribe medications electronically.[320] Estonians also actively engage with digital media.[321] According to the Open Society Foundation, "More than three-quarters of the population accesses the internet regularly, and more than half of those are active on social networking platforms. Recent surveys suggest that nearly a quarter of internet users now connect via smartphones."[322]

These uses of the Internet present a great many opportunities for Estonia and her people, but they can also open the nation up to serious system vulnerabilities. This strategic vulnerability was thoroughly exploited by a devastating three-week DDoS attack that lasted from 26 April to 18 May 2007.

The Attack

This attack was ostensibly sparked by the Estonian government's decision to move the Bronze Solider, a Soviet-era WWII memorial, from Tallinn's main square. In 2007, this statute and several other grave markers were moved from Tõnismägi park in central Tallinn to the Defence Forces Cemetery of Tallinn following the exhumation and identification of the remains they were marking. This decision was politically charged given the differences in public opinion regarding the events symbolized by the monument. Many ethnic Russians living in Estonia continue to view Soviet arrival in Estonia at the end of WWII as a time to be celebrated and saw this monument as a symbol of both the Soviet victory over Nazi Germany and the equal rights of Russians in Estonia.

Many Estonians viewed the statue much differently. For them, it marks the beginning of a devastating era of Soviet occupation.

Public discontent over the relocation of this statue peaked in two nights of riots in Tallinn from 26 April to 27 April 2007, which are known collectively as Bronze Night. These mass riots and looting, involving more than 1,000 protesters,[323] were the worst that Estonia had experienced since gaining its independence. The Estonian Embassy in Moscow was also targeted and the Russian government spoke out strongly against the removal of this monument, with both houses of the Russian parliament calling on President Putin to impose sanctions in response to this act or even to sever relations with Estonia altogether.[324] Russian Foreign Minister Lavrov went as far as to say: "This is blasphemous, and will have serious consequences for our relations with Estonia."[325]

Concurrently with these riots and strongly worded statements by the Russian government, the cyber attack began. Operating in two phases, Phase I from 26 April to 29 April and Phase II (the main attack) from 30 April to 18 May, this attack would go on to cripple Estonian cyber infrastructure, representing what could be viewed as the world's first offensive cyber war.[326]

The use of cyber warfare techniques is the most widely recognized component of the Russian hybrid warfare strategy in the past decade in Estonia. While the Russian government has denied any involvement in the 2007 cyber attack, it is widely speculated that there was at least some level of Russian sponsorship. This case study also highlights the challenge of attribution in cyberspace, making this tool an even more useful component to employ as part of a hybrid warfare strategy.

Analysis of Key Components Used: 2007 Cyber War

2007 Estonia Cyber War Timeline[327]

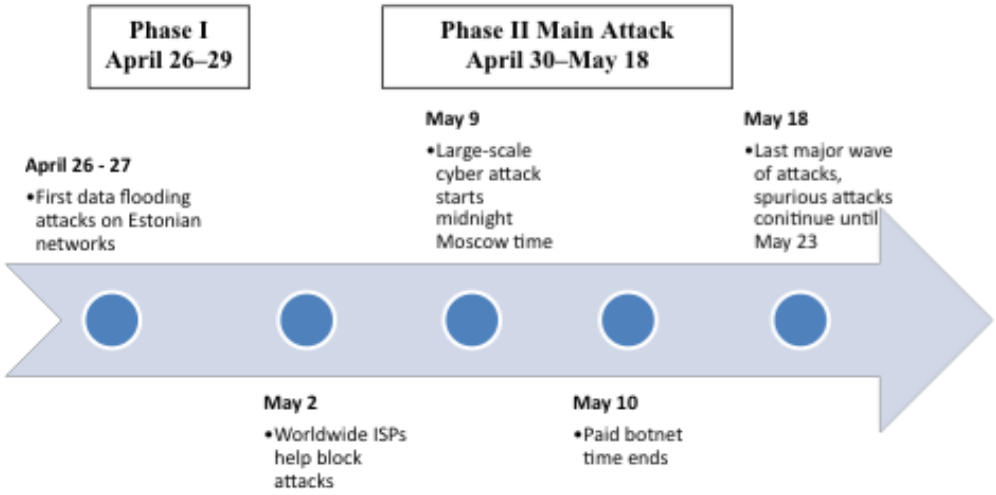

Figure 9: 2007 Estonian Cyber Attack

Phase I

Phase I of the attack, which lasted from 26 April to 29 April 2007, was relatively simple and unsophisticated. This phase first targeted government web servers, news portals, and other sites in order to deface them and manipulate their content.[328] This stage of the attack emphasized the IO and propaganda component of hybrid warfare by manipulating government messaging in an attempt to achieve a desired political effect. This included creating a fake apology letter from Estonian Prime Minister Andurs Ansip for relocating the statue, which was circulated through seemingly official channels.[329] More blatant defacing of the government websites also occurred. For example, hackers added a Hitler-type mustache to a picture of Prime Minster Ansip on his political party's website[330] and government website traffic "included phrases like 'ANSIP_PIDOR=FASCIST.'"[331]

While offensive and spreading misinformation, these elements of Phase I of the attack were largely manageable and were quickly shut down. The flooding of government websites to deny service proved to be a more substantial problem. Websites that "normally receive 1,000 visits a day were receiving 2,000 visits every second."[332] This increased traffic shut down some sites for just a few minutes, but others remained offline for several hours.[333] A similar approach was taken to bogging down Estonian parliamentary emails. Attackers posted the email addresses of Estonia's parliament deputies to the social media site LiveJournal and encouraged followers to blast emails to these addresses. In response to this call for involvement, millions of emails were sent to the addresses on the list, sending the servers offline for two days.[334]

Composed of traditional DDoS elements, Phase I of this attack also represents a sort of IO aimed at misinforming the Estonian public and encouraging individuals to act out against the Estonian government as a participant in this cyber war.

Phase II

Phase II, which represented the main part of the attack, was significantly larger in scale, more sophisticated, and very well coordinated. This stage of the attack mainly consisted of offensive DDoS actions against critical Estonian information infrastructure. This included targeting the backbone routers of the data communications network and the Domain Name System (DNS) servers.[335] This second phase was clearly well funded, with attackers using botnets to control millions of computers around the world and aim them against Estonia. During the worst of the attack, Estonia was receiving 1,000 times its usual inbound email flow, weighing down the system and forcing services to go offline.[336]

Attacks were aimed against many different sectors within Estonia, including "government, the president, the parliament, police, banks, Internet service providers (ISPs), online media, as well as many small businesses and local government sites."[337] The following table indicates the specific sites targeted and the number of attacks against different key government targets.

Analysis of Phase II Targets—May 2007[338]

# of Attacks	IP Address	Target
35	pol.ee	Estonian Police
7	www.riigikogu.ee	Estonian Parliament
36	www.riik.ee www.peaminister.ee www.valitsus.ee	Official State Web Center Prime Minister Estonian Government
2	m53.envir.ee	Ministry of the Environment
2	www.sm.ee	Ministry of Social Affairs
6	www.agri.ee	Ministry of Agriculture
4		Estonian Computer Emergency Response Team (CERT)
35	www.fin.ee	Ministry of Finance
1	starman.ee	Private telecom provider

Table 1: Targets in Estonia Cyber Attack

During Phase II, the attacks' impact on Estonian news outlets forced the news sites to block incoming international traffic, thereby effectively cutting off Estonia from the rest of the world during a critical period of time. Moving forward, the private sector also became a target for the attack. On 9 May, the heaviest attack occurred. During this time, attackers sent up to four million packets of information per second for 24 hours.[339] This attack eventually forced Hansabank, Estonia's largest bank, to suspend all Internet-based operations.[340] According to a researcher at George Washington University's Elliott School of International Affairs, "This was disastrous on three counts. First, it ceased online banking capabilities for Estonians in a country where an estimated 97 percent of all banking transactions occurred online; second, it severed the connection between Hansabank and its ATMs throughout Estonia; and third, it broke the connection between Hansabank and the rest of the world, thus preventing Estonian debit cards from working outside of the country."[341]

Throughout Phase II, Russian websites continued to provide sources for attack instructions and target lists.[342] This further highlights Russian involvement, even if not formally state-sponsored. This phase of the cyber attack continued the IO component of hybrid warfare, by compromising the integrity of the Estonian media system. Additionally, there was a strong economic warfare element of this attack that is exemplified by the paralyzing of Hansabank

through the most aggressive of the series of attacks in Phase II. Lastly, the political element of this attack cannot be ignored. More than just shutting down government websites and emails, this attack served to highlight critical weaknesses within the Estonian government, which effectively threw into question the government's ability to provide critical services for its people. By casting this level of doubt, the attack damaged more than just the websites it targeted.

The End of the Attack

On 18 May 2007, just as suddenly as it started, the cyber attack stopped. While international efforts to mitigate the impact of the attack certainly hindered hackers' efforts, it is unlikely that Estonian or NATO responses can be fully credited for ending the attack.

Attribution and Russian Involvement

The highly detailed and methodical nature of this attack is what is most concerning, because it seems to indicate a level of organization beyond what is achievable by a group of 'hacktivists.' While it has not been possible to directly link this attack back to the Russian government, many actors in the international community agree that a level of Kremlin sponsorship is highly likely.[343]

The vitriolic rhetoric coming out of Russia following the moving of the Bronze Solider, certainly served as a motivator for ethnic Russians who participated in the attack, establishing a cadre of "homegrown cyber patriots"[344] eager to protect Russian honor against "Estonian Fascists."[345] That being said, researchers have argued as to whether this propaganda and stirring up of tensions truly makes Russia culpable for the attack. Studies have indicated that many of the actors involved in the attack were "motivated to strike at Estonia as an act of protest and that while official Russian sources may have provided inspiration, it appears they acted on their own accord."[346]

The question of funding is also critical when considering Russia's role in the attacks, as many have speculated that the Russian government provided funding to hire the botnets that were critical in Phase II of the attack. Finally, the involvement of the Russian youth group Nashe seems to indicate a level of Kremlin involvement. This group, which is connected to the Russian government, perfectly exemplifies the government's three-tier system that allows them to fund and support different causes, but to remain far enough removed from the actual actions to claim plausible deniability. This issue of attribution creates great challenges for responding to cyber threats.

Network Analysis

The attack against Estonia in 2007 clearly represents the cyber warfare component of hybrid warfare, but this element also influences several other hybrid warfare techniques. Through the tool of cyber attacks, the hackers were able to use elements of IO, economic warfare, and political warfare all to work toward the final goal of discrediting the Estonian government and highlighting the assailants' ability to shut down this highly sophisticated cyber system. This complex structure is provided in Figure 10.

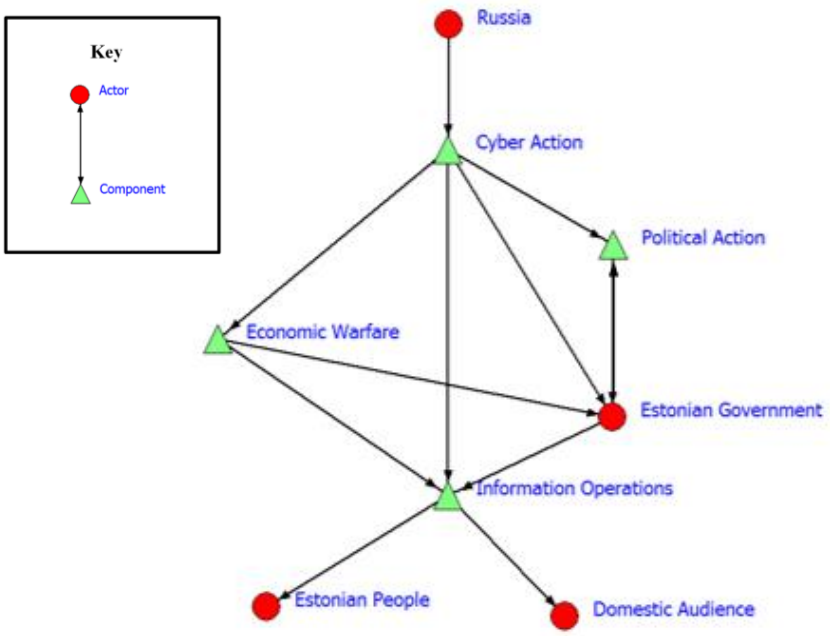

Figure 10: Estonia Cyber Attack Network Map

As is evident in the visual above, Russia only implemented a cyber attack. However, the method in which it was carried out had follow-on consequences. The cyber attack targeted the banking systems, which allowed it to take on an additional form as an act of economic warfare, preventing access to trade and finance. It also directly targeted the Estonian government, attempting to punish it for the removal of the Bronze Soldier, and thus affect political decision-making. The attackers put pressure on the government, undermining it by preventing certain functions and reducing confidence in it. These activities translated the cyber attack into political action.

Moreover, the choice of banking and government as targets, and the fact that many core functions of Estonian society were affected, converged into a larger IO directed against both Estonian and Russian citizens. The message was clear: despite its independence and relative advancement in the region, Estonia is still vulnerable to its former occupiers.

Response

The level of coordinated cyber war against a nation demonstrated in the 2007 attack against Estonia was unlike anything that had been seen before.

In the short term, in an attempt to manage the crisis, the Estonian government was forced to block all international cyber traffic. While perhaps effective for warding off the attack, this move essentially cut Estonia off from the rest of the world, which was not without significant risk.[347] NATO responded to support Estonia by sending several cyber terrorism experts to the country to advise on how best to respond to the attacks and how to recover in the aftermath. Legislation also was passed to open NATO's Cooperative Cyber Defence Centre of Excellence,

located in Tallinn. This center, which opened in August 2008, conducts research on cyber security issues and is working to develop a protocol for responding to attacks of this nature. The Estonian government also established the Estonian Defence League's Cyber Unit, an all-volunteer force geared toward mitigating these threats in the future.[348]

In addition to these actions, NATO has responded to this escalation in cyberspace by acknowledging at the Wales Summit that it is possible that cyber attacks could reach a threshold where they sufficiently threaten the security and stability of nations within the alliance, thus leading to the potential that Article 5 could be invoked.[349] This threshold remains ambiguous though, and the rhetoric emerging from Warsaw Summit in 2016 focused largely on strengthening defensive cyber capabilities and increasing cyber expertise across the alliance.[350] It remains to be seen whether these new tools and agreements will be sufficient to deter or, if necessary, respond to cyber attacks in the future.

Conclusion

The situation in Estonia reflects the current uncertainty in the Baltics, where stability is slowly being eroded by continual Russian efforts to undermine state authority and challenge the resolve of NATO on its eastern border. By making use of numerous hybrid tactics, most notably aggressive offensive cyber capabilities, Russia has cast a shadow of doubt over the Estonian government's ability to effectively respond to these unconventional threats. It is imperative that Estonia and its allies develop concrete plans to counter this multifaceted, long-game strategy if they intend to work effectively against the threatening Russian influence in the region.

South China Sea: A Continuous Case

While it has been making the news more frequently recently, the conflict over control of the South China Sea is nothing new. The rise and fall of this conflict has followed the rise of China's influence in East Asia and the Pacific. As China grew stronger, both economically and militarily, it began to assert itself more aggressively in the South China Sea. Hybrid techniques have played a major part in this bellicosity.

Background

Origins

The first U.S. policy statement regarding the dispute over the area was made in 1995, effectively advocating for a diplomatic solution to preserve stability in the region.[351] While the dispute is not new, the increasing strategic importance of the region has launched what used to be a small-scale regional dispute onto the world stage.

The dispute hinges on control over a series of small land features, ranging from reefs to small islands, which dot the South China Sea. While not inherently valuable, control of these small outcroppings is at the heart of a territorial dispute between China, Vietnam, Malaysia, Brunei, the Philippines, Taiwan, and, to a certain extent, the U.S., in which the winners gain control over potentially vast swaths of the Sea itself.[352] The South China Sea is a major shipping route in the

region, is home to plentiful fish stocks, and could contain vast oil resources.[353] In short, gaining control over the territory would be a major boon for any state that secured it. For its part, the U.S. is a status quo power in the region, preferring a diplomatic solution that preserves the freedom of the seas for all actors.[354]

Disputes over the area go back centuries, with the Paracel Islands in the northwest and the Spratly Islands in the southeast—the main island chains in the South China Sea—acting as the key battlegrounds.[355] The island grabbing picked up in earnest in the 1950s, with intermittent periods of conflict and relative peace continuing until today.[356] However, China has had control over the Paracel Islands since it took them from the occupying Vietnamese forces in 1974.[357]

It appeared as if a durable peace could be reached with the signing of the 2002 Declaration of the Conduct of Parties in the South China Sea between ASEAN and China. This statement of purpose seemed to keep the conflict at bay for a time, until Malaysia and Vietnam submitted a claim to the Commission on the Limits of the Continental Shelf in May 2009 and China responded by submitting a map with its infamous 'nine-dash line,' outlining its historical claim on the region.[358] This submission is arguably the touch point for the current crisis, as it signaled China's designs on the Sea in its entirety, rather than the piecemeal conflicts of the past.[359]

While this case has been simmering for centuries, the appearance of the nine-dash line and the end of the peace established by the 2002 Declaration kicked off a flurry of activity that will be the focus of the remainder of this analysis. That is not to say that events preceding this one are unimportant in the course of this conflict. Rather, they are being omitted for the sake of focus in this particular piece.

Aggression

Following the claim, China began to act more aggressively in the region. On 11 June 2009, a Chinese submarine collided with a U.S. warship, the USS John S. McCain, after having followed the ship for some distance.[360] On 10 April, 10 Chinese naval vessels moved through Japan's Miyako Strait to conduct anti-submarine warfare exercises.[361] In May and June of that year, both the Chinese and Indonesian navies began seizing fishing vessels that each accused of illegally fishing in the area. Almost inevitably, this led to conflicts between the two countries, as they continued to defend what each believed to be its own territory.[362] Also in May 2010, a Chinese surveillance vessel threatened a Japan Coast Guard (JCG) ship on a survey mission in the East China Sea. The Chinese ambassador released a statement promising to bring it up with his superiors back home, but little came of it.[363] On 23 June 2010, Indonesia upped its response when one of its naval patrols confronted Chinese fishing vessels northwest of the Natuna Islands.[364] However, China's ire remained focused on Japan after a JCG captain attempted to interdict a Chinese fishing boat and the fishing boat rammed the JCG vessel on 7 September.[365] A similar incident occurred between a Chinese fishing boat and a South Korean coast guard vessel on 18 December, leaving two of the fishermen dead.[366]

Despite the loss of life in December of the previous year, 2011 opened quietly in the South China Sea, with the first incident delayed until 25 February, when a Chinese vessel fired warning shots on a Philippine ship in an effort to force it to leave an area near the Spratly Islands.[367] Similarly, on 9 March, a Chinese helicopter harried a Japanese destroyer near a gas field in the East China Sea in an effort to deter the Japanese from remaining in an area where both states maintain competing claims.[368] But, the Japanese fired back by intercepting Chinese surveillance

planes in the same month.[369] On 26 May, a Chinese surveillance ship cut the exploratory cables of a Vietnamese vessel conducting a seismic survey for potential oil and gas extraction along Vietnam's Continental Shelf,[370] only to have a Chinese fishing vessel become tangled in the cables of another Vietnamese survey ship, disabling the Vietnamese vessel on 9 June.[371] In response, Vietnam began to hold live ammunition drills in the area to reassert its authority to continue oil exploration activities.[372] In July, China widened its efforts and demanded that an Indian vessel explain its presence in international waters following a visit to Vietnam.[373] However, it focused back on Vietnam on 5 July, when Chinese soldiers assaulted and expelled a group of Vietnamese fishermen near the Paracel Islands.[374] Likewise, China returned to harrying Japan on 21 August, when a Chinese patrol violated Japanese territorial seas around the Senkaku Islands.[375] Japan fought back on 6 November, when it detained a Chinese fishing boat captain who had refused to stop for inspection off the Goto Islands. Interestingly enough, the boat was only apprehended after a four-and-a-half-hour-long chase, which ended in a collision.[376]

Once again, the winter proved a quieter time in the South China Sea, with the first incident of 2012 not coming until 19 February, when China expelled two Japanese boats from its territorial waters for allegedly carrying out illegal surveillance activities.[377] Shortly thereafter, China prevented 11 Vietnamese fishing boats from landing in the Paracel Islands, when the vessels claimed to be seeking refuge from a storm. Vietnam lodged a complaint with the Chinese embassy, but China denied the allegations.[378] Throughout the month of March, China, Japan, and Taiwan issued statements naming and renaming 39 of the uninhabited islands in the East China Sea.[379] In a similar, primarily diplomatic move, the Taiwanese Ministry of Foreign Affairs claimed sovereignty over the entirety of the South China Sea on 13 March, but little came of the announcement.[380] Later that month, on 23 March, China fell back on old habits and detained 21 fishermen near the Paracel Islands.[381] On 10 April, Filipino aircraft identified a group of Chinese fishing vessels at Scarborough Shoal, prompting the Philippines to send its largest warship to the area to demand that the ships leave. China responded by sending its own warship, leading to a standoff that lasted until the fishing vessels finally departed on 18 June.[382] On 16 April, during the standoff, the U.S. and the Philippines held their annual Balikatan military exercises in the South China Sea, near the island of Palawan. Although the exercises were nothing new, but had been going on for 28 years, they did coincide with the standoff and drew protests from China.[383]

On 17 April, the Japanese tried a different tactic, attempting to purchase the disputed Senkaku Islands in the East China Sea from their Japanese owner,[384] and ultimately closed the deal on three of the eight on 11 September.[385] Japan defended this claim on 25 September, when it repelled dozens of Taiwanese fishing vessels, accompanied by Taiwanese coast guard ships, which had attempted to enter the territorial waters around the islands.[386] In a similar move, from strictly power projection, China announced on 28 November that it would have the authority to board and search vessels it deemed to be violating its territorial waters beginning on the first of the following year.[387] However, China demonstrated that it did not have a similar respect for territorial integrity that it now demanded of its co-claimants on 13 December, when a Chinese surveillance plane violated Japanese airspace over the Senkaku Islands.[388]

These incursions and Japan's blanket response to scramble the offending flights continued through December and into January 2013, culminating in Japan dispatching F-15s and suggesting that it would authorize its aircraft to fire warning shots on any Chinese planes violating their airspace.[389] On 22 January, the Philippines filed an arbitration claim against China under the United Nations Convention on the Law of the Sea, which still continues to this day and will be

discussed further in a subsequent section.[390] The trend of low-level aggression between China and Japan continued into February, when Japan protested China's use of directed fire-control radar against a Japanese destroyer, implying China's targeting of the ship for an attack. China denied the allegations, which Japan refuted in response.[391] Despite the heightened tensions, Malaysia made a move toward diplomacy by suggesting that it could recognize China's claims over those of the other claimants, even going as far as to state that Malaysia had no problem with China's patrol of the South China Sea.[392] The remainder of 2013 was relatively quiet, with the next major incident coming in early 2014.

Reclamation

Beginning in January, China imposed a fishing permit rule in the South China Sea, despite the objections of the U.S., the Philippines, and Vietnam.[393] In May, a Chinese state-owned oil company pushed into Vietnamese-claimed territory by moving one of its rigs into the waters south of the Paracel Islands, which prompted confrontations between vessels representing the two countries and rioting against foreign businesses in Vietnam.[394] The aggressive posturing continued into August, when an American Boeing P-8 Poseidon was harassed by a Chinese Shenyang J-11. Chinese Rear Admiral Zhang Zhaozhong echoed the move with a call for Chinese fighter jets to "fly even closer to U.S. surveillance aircraft." However, the main story of 2014 was the start of China's major push for land reclamation in the South China Sea, which continues to this day.[395] These movements will be discussed further in a subsequent section.

Similarly, the main events of 2015 centered on China's land reclamations. On 9 April, satellite photos were released showing China's aggressive land reclamations, drawing criticism from the U.S.[396] In response, China's Foreign Ministry spokesperson Hua Chunying claimed that the activities were for maritime purposes only.[397] On 11 April, the U.S. Office of Naval Intelligence released a report stating that China's navy has been undergoing rapid modernization and growth over the past three years, including growing its coast guard to the largest in the region.[398] On 17 May, after meeting with U.S. Secretary of State John Kerry, Chinese Foreign Minister Wang Yi announced that China would continue its land reclamation.[399] China then ordered a U.S. military surveillance plane to stop flights over contested territory in the South China Sea on 23 May.[400] Then, on 27 May, China released a strategy paper declaring that it would extend its naval forces to defend its claims in the South China Sea.[401] However, amid rising tensions with the U.S., China declared on 17 June that it would soon end its land reclamation efforts.[402] In a statement on 31 July, Chinese Senior Colonel Yang Yujun blamed U.S. military actions.[403]

On 16 September 2015, the Center for Strategic and International Studies released satellite images showing the construction of an airfield on another artificial island in the South China Sea.[404] The heightened tensions between the U.S. and China were reaffirmed on 23 September, when Chinese President Xi Jinping visited the U.S.[405] On 27 October, the Pentagon confirmed a naval 'innocent passage' operation through the disputed territory, testing China's claims on it.[406]

A major breakthrough against China's aggression occurred on 31 October, when the Permanent Court of Arbitration at The Hague announced that it would hold hearings on the case brought by the Philippines against China in 2013.[407] On 6 November, Defense Secretary Ash Carter signaled American commitment to the conflict when he landed on an aircraft carrier in the South China Sea with his Malaysian counterpart.[408] The year closed with more strong statements from the U.S. regarding China's aggressions in the region. First, U.S. President Barack Obama urged China to stop its activities in the region and called for a peaceful resolution to the conflict.[409]

Then, U.S. Navy Admiral Scott H. Swift, commander of the Pacific Fleet, issued a statement on 16 December that China's actions have eroded the security situation in one of the world's key waterways.[410]

From the outside, China's persistent, and at times apparently petulant, actions seem to signal a simple grab at territory in an economically crucial part of the region. However, from the perspective of the Chinese Communist Party, its expansion into the South China Sea is part of a larger effort to shore up its own legitimacy and prevent foreign powers from redrawing what it considers its borders.[411] China does not refer to the region as territorial waters, subject to the United Nations Convention on the Law of the Sea (UNCLOS), of which it is a signatory. Rather, it is an extension of its own territory, referred to as 'blue soil' in the Party's newspaper, the *People's Daily*.[412] As such, it appears that the strategic goal of the operations in the South China Sea is to maintain China's legitimacy as a state by protecting what it views as its territorial integrity. To accomplish this goal, China is using a variety of hybrid techniques.

It is, however, worth noting that China is far from the only actor in the region using hybrid tactics in an effort to lay claim to more of the South China Sea. Vietnam, for example, has been building up their occupied reefs and shoals for just as long as China,[413] and Japan has been known to fire on Chinese naval vessels.[414] However, to allow for more depth of analysis, this section will focus solely on China's own actions.

Analysis of Key Components Used

Power Projection

Most of China's military activities have been small in scale and more political than kinetic in nature, thus classifying them more as power projection than conventional military operations. China has been consistently increasing its defense spending for the last two decades, rapidly modernizing and expanding its military.[415] A central tenet of this modernization strategy is hampering the American ability to access the region, via antiaccess/area denial (A2/AD) efforts[416] and drastic improvements in its airpower,[417] directly challenging the U.S. presence in East Asia.

In 2013, China declared an air defense identification zone (ADIZ) over the South China Sea, effectively stating that it had control over the sea's airspace.[418] Declaring the ADIZ was a controversial move in Beijing,[419] as it increased tensions in the region without a clear benefit for the country.[420] However, it has given the state another venue in which to project its military force, demanding that all aircraft flying through the ADIZ identify themselves.[421] In concert with the declaration, China has been developing its air force over the last two decades from a small force focused on homeland security to one more capable of power projection.[422] They proved their prowess via their longest flight mission to date in November 2015, which reached a point within 1,000 miles of Guam.[423]

Traditionally, China has also largely foregone using its navy to enforce its control over its territory, choosing instead to employ its coast guard and fishing fleet in small, incremental missions to carve out an ever growing area of influence.[424] However, it has increased the use of its navy in these operations in the last two years.[425] In general, as evidenced in the previous section of this case, operations are small in scale and tend more toward posturing and making China's presence felt than direct engagement with any of the co-claimants. The Chinese navy is also

harassing civilian ships, threatening the livelihoods of fishermen who had been using the seas for generations.[426] China has included civilian actions in its wider strategy, as well, including opening a school on Woody Island in the Paracels in December 2015,[427] further projecting its control over the region.

Most prominently, China has been building artificial islands and expanding existing ones in the area surrounding the Paracel and Spratly Islands in an effort to claim these disputed waters as their own.[428] These claims are dubious at best, given the provisions within UNCLOS, namely that artificial islands do not grant a state any claims on the waters surrounding them.[429] However, China's military and economic might have rendered efforts to challenge these claims largely unenforced thus far.[430]

The importance of these islands does not end with their implications for the claiming of territorial seas. Rather, it is their potential for providing strategic footholds in the region that makes them dangerous, as a handful of the various contested shoals, reefs, islands, and rocks have enough area to build airstrips long enough to accommodate tactical aircraft.[431] The ability to build and use airstrips on these tiny islands, as China has begun to do,[432] is of great importance in the balance of power within the region. Not only does it expand the physical presence of China in the region, but it also allows for more expansive air coverage of the South China Sea. As mentioned earlier, China has already declared an ADIZ over the South China Sea, and the ability to base its air force off these islands allows it to easily enforce that claim. In essence, artificial islands have become the cornerstone of Chinese power projection in the South China Sea by giving that projection physical form.

Lawfare

The legal arguments of the conflict center on the questions of sovereignty and the applicability of UNCLOS. Each of the claimants in the South China Sea case has a myriad of sovereignty doctrines from which to construct convincing arguments as to their claims on the small pieces of land there. For its part, China relies largely on a history of effective occupation of the land,[433] which was ruled as a legitimate source of sovereignty in the *Island of Palmas* case in 1928.[434] Its track record of patrolling the sea and successfully policing the presence of other nations within the region does lend credence to this argument.

With regard to UNCLOS, the law has been somewhat murkier. Control over the sea surrounding the various land features depends not only on who claims that feature, but also on how it is classified. Depending on how that feature is classified, the owner could get as much as 200 nautical miles of exclusive economic rights over the seas around the island,[435] in the case of a true island, or nothing at all, in the case of an artificial island or a rock.[436] Once the feature is classified, the question still remains over ownership. These legal ambiguities are frequently and consistently exploited by China to delay a definitive decision on the conflict as it continues to snap up territory by other means.

For example, much of the basis of its legal claims to the South China Sea arise from the previously mentioned 'nine-dash line,' which appears on Chinese maps of the area and which China argues allows for a historical exception to the territorial sea boundaries set out by UNCLOS.[437] There have been several cases challenging this line brought before tribunals established under the dispute resolution methods laid out by UNCLOS, with the most recent case brought against China by the Philippines in 2013. However, the Chinese refused to recognize the

case, or abide by the final ruling in favor of the Philippines, because they argue that the dispute was over sovereignty and therefore outside of the jurisdiction of the UNCLOS tribunal.[438] It is a classic use of lawfare to protect a hybrid strategy. In essence, rather than trying to argue about the facts of the case, which under UNCLOS China was bound to lose, the state instead chose to exploit ambiguities in the jurisdiction of the court to prevent decisive action against it.

Diplomatic Action

As a reminder, diplomatic action is the use of political relationships to move forward a nation's political agenda. This can take the form of using relationships to justify behavior, shore up support, and even discredit the claims of other states. To improve his country's image in the region and in the West, Chinese President Xi Jinping engaged in several state visits at the fall of 2015, including to the U.S.[439] Specific to the case, President Xi travelled to Vietnam, Singapore, and Taiwan, and sent aides to the Philippines, all of whom are co-claimants of all or parts of the South China Sea. While no decisions were made, he re-iterated his desire for a peaceful settlement of the dispute.[440] These efforts were aimed at both building relationships with co-claimants, which can be used as conflict progresses to further its aims, and creating an image of China as the 'nice guy.' These diplomatic efforts are placed alongside the more aggressive tactics to show that China is not all bad, that it can play by the rules and maintain its place as a respected member of the international community.

During an October 2015 trip to the United Kingdom, Chinese President Xi Jinping focused on building bilateral business agreements there.[441] This had the double effect of drawing Britain closer to China, making it more difficult for the UK to oppose China without damaging itself, and of sowing tension between the UK and its longtime ally, the U.S.[442] However, the move is unlikely to have substantial or lasting effect on the 'special relationship.' Still, business has become a key diplomatic tool for China, as will be revisited in the economic warfare portion of this section. Here, China attempted to build a stronger relationship with a respected western ally in an effort to solidify leverage for use in the future.

In effect, Chinese diplomatic strategy is twofold: to improve its image by discrediting the arguments of its co-claimants that China is the main aggressor in the region, and to build strong relationships with states outside of the region for increased support in the international community.

Economic Warfare

Should China gain control over the South China Sea, it would gain a great deal of leverage over trade in Asia, weakening both other states in the region and the U.S.[443] Doing so would further secure its position as the major power in its region and solidify its legitimacy in the eyes of its people and the international community. However, even without full control over the South China Sea, China has more leverage over the U.S., and the international community in general, than either would be comfortable admitting. Any outright conflict between the U.S. and China would have severe implications on global trade, though China would likely ultimately be the more negatively affected of the two.[444]

Still, the desire to avoid further economic disruption is one of the major factors at play in keeping tensions from boiling over in the region. In essence, the threat of a disruption of the global economy, in which both the U.S. and the states in the region are so entwined, is a key enabling factor that allows for this low-intensity hybrid conflict to continue unchecked. In short, rather than

actively disrupting the global economy in the service of its hybrid strategy, China is using its diplomatic actions to increasingly tether Western economies to its own, thus making it too expensive for them to act against China. In doing so, China is altering the cost-benefit analysis that the West must go through in order to decisively engage in conflict with China by providing increased access to trade and cheaply manufactured goods. Given the potential economic repercussions China has manufactured in the global economy, the West is more likely to adopt a strategy of limited engagement or even appeasement in the South China Sea, rather than risk another economic downturn. As in Crimea, economic interests continue to prevent effective action against Chinese expansion in the South China Sea.

Network Analysis

Given the ultimate goal of legitimacy, it appears as if the hybrid components outlined above are merely part of a larger IO, signaling China's strength and territorial integrity to its own people and the international community. There is no clear propaganda campaign outside of the 'blue soil' narrative in China, mentioned previously. Although there are comparatively fewer components in this case than the others outlined in this section, they very clearly fit together into a networked attack, as shown in Figure 11.

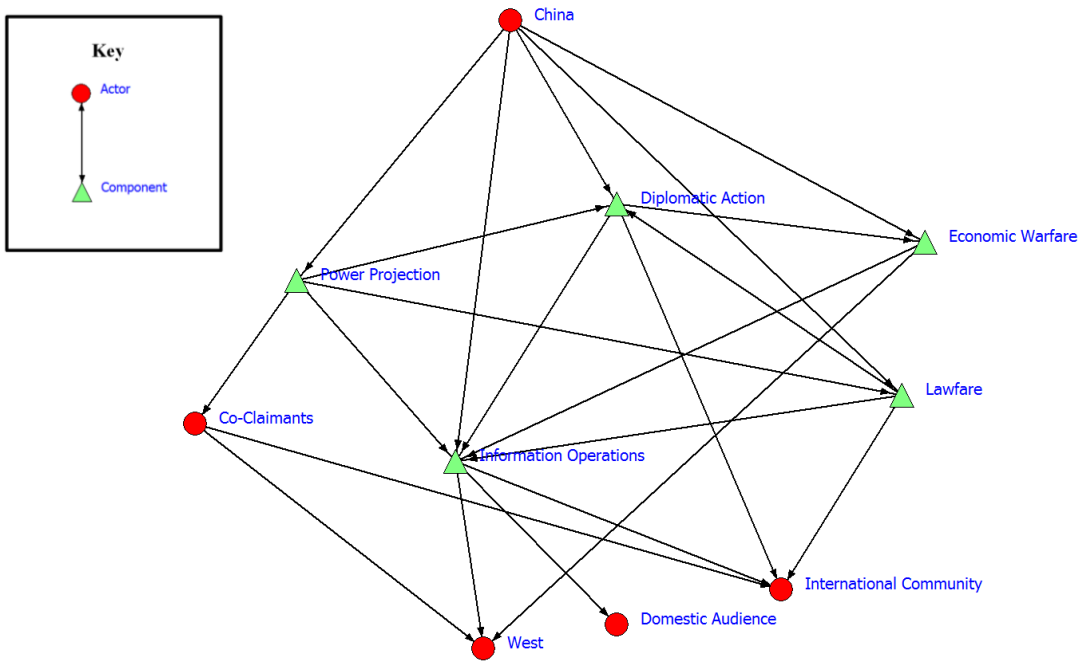

Figure 11: South China Sea Network Map

The power projection component adds legitimacy to the lawfare claims, as China's strongest argument in the sovereignty disputes is its effective occupation of territory, which the power projection methods allow it to maintain. Power projection also supports diplomatic action, as it allows Chinese diplomats to negotiate from positions of power. Regardless of whether or not China's occupation of territories in the South China Sea is legitimate, its ability to do so, and its

opponents' inability, or unwillingness, to counter that occupation, puts China at a distinct advantage in diplomatic interactions.

Likewise, the lawfare efforts give Chinese diplomats plausible deniability in their interactions with other states, allowing them to continue to maintain productive diplomatic relations with major powers, such as the U.S. and UK, while potentially violating international law. This is further aided by the pressure China is able to exert via its economic warfare tactics. The global economy is intimately intertwined with China's economy. As such, war with China would simply be bad business, a fact that China is able to exploit to prevent decisive action against its activities in the South China Sea. This sends a message to both the Western world and the international community as a whole that China is able to maintain de facto control over the South China Sea. Much is made in the media of China's power projection tactics, but in Figure 11, the only actors affected by them directly are the co-claimants. It is only through the other hybrid tactics that the West and the international community are affected at all.

What is especially interesting, in this case, is the sheer saturation of connections between components of the campaign. There are connections between nearly all of the hybrid components used in this attack. Thus, China has created a mutually reinforcing hybrid warfare campaign, in which any action it takes will strengthen the other facets of its strategy.

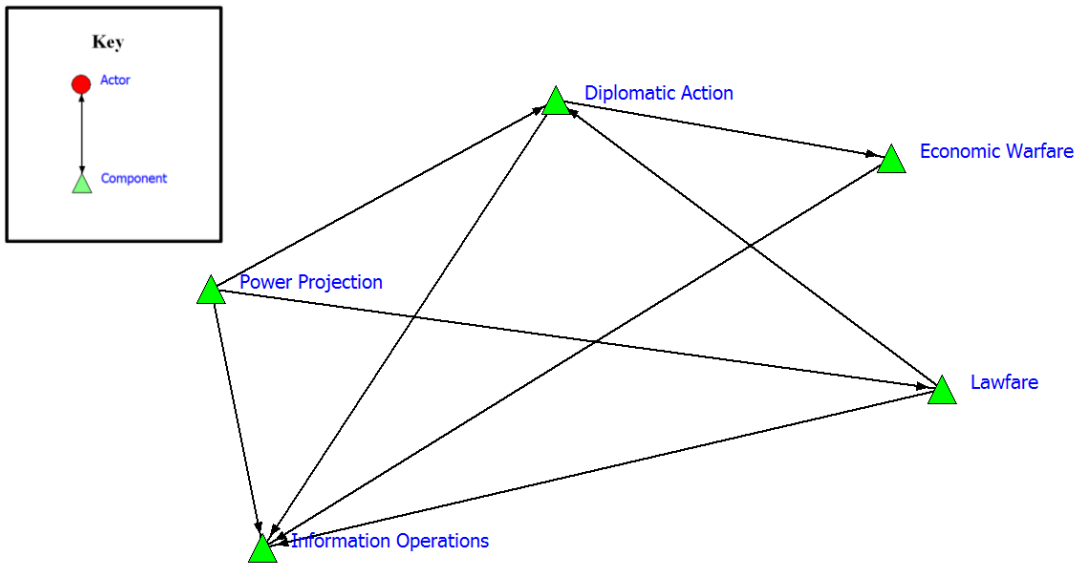

Figure 12: South China Sea Component Network

As is evident in Figure 12, this combination of power projection, lawfare, diplomatic action, and economic warfare converge into a global IO, with the message that China has become powerful enough to do as it wishes on the international stage with few repercussions. Thus, China is able to accomplish its strategic goals of preserving legitimacy and preventing international interference within its territorial boundaries. It is important to note, however, that in the larger network, the IO are the only ones affecting their domestic population. As stated previously, China's key goal in the case is inwardly focused. Thus, a strategy that targets its center of gravity and thus has a chance of affecting China's behavior in the region must address this component, rather than simply trying to match China's power projection with its own.

Responses

United States

U.S. responses to China's actions have largely taken the form of political and preparatory actions, including "expanding and diversifying U.S. force posture, strengthening our alliances, building partner capacity, engaging regional institutions and providing forward-deployed U.S. forces with the newest and most advanced capabilities," as well as direct diplomatic action with China.[445] There is no denying that the U.S. has competing priorities elsewhere. However, the U.S. has treaty obligations to the Philippines, which could draw the U.S. into conflict, should it arise in the region.[446] This may come into play, as aggressive activities from both sides draw the two closer to open aggression.[447]

The U.S. Navy has carried out a series of 'freedom of navigation' exercises, sending naval vessels into the area under the auspices of asserting its rights under international law.[448] However, these forays have effectively acknowledged China's claims and given China the ability to defend them, therefore strengthening them in the eyes of the international community.[449] To make matters worse, the increasing militarization of the region has been cause for concern among the international community, with Admiral Swift warning of a possible arms race in the area.[450] This concern, though, has not been specifically addressed in U.S. interventions in the region.

Co-Claimants

As evidenced in the background section of this case, the actions of the co-claimants have typically mirrored China's own. They tend to rely on a mix of their own power projection, using fishing vessels and scientific survey expeditions to lay claims to portions of the Sea, and diplomatic moves, including public statements and appeals to allies outside of the region, as the Philippines did with the U.S. However, much has been made of the UNCLOS arbitration case brought by the Philippines in 2013 and the hopes for peace in the region seem to be hung on the application of international law. In October 2015, the Permanent Court of Arbitration announced that the Court did indeed have jurisdiction over the case and that it would be moving forward with the claim.[451] In July 2016, an international tribunal at The Hague ruled in favor of the Philippines, citing that China has no legal basis for its historical claims. However, China characteristically boycotted the proceedings and the decision has had little effect altering China's behavior on the ground.[452]

International Community

Attempts to settle disputes legally, including via the Permanent Court of Arbitration in The Hague, in accordance with UNCLOS, have largely failed, as China refuses to acknowledge the Court's jurisdiction in the matter.[453] However, there has been a growing sense among the international community that flouting the Convention and its dispute resolution provisions is unacceptable, in part because it is seen as "key to getting China to accept international legal norms over the waterway, through which $5 trillion in ship-borne trade passes each year."[454] Likewise, the Philippines case may create a domino effect as other claimants, such as Indonesia, consider bringing cases against China.[455] However, large-scale opposition to Chinese actions in the region have been absent thus far.

Conclusion

The South China Sea case is an interesting one in that it should be far more clear-cut than it is. While China's actions clearly violate international law, a combination of diplomatic action, lawfare, and economic warfare have coalesced to protect it from decisive censure or action on the part of the international community. Here, the hybrid techniques are not strictly necessary to accomplish China's strategic goal, nor to avoid attribution, as it is very clear that China is behind many of the events in the region. Rather, the hybrid techniques are used to prevent intervention from the international community. Although outside of our region of interest, this case is a crucial one in understanding hybrid warfare, as it illustrates the flexibility of the term, even in the purpose of its use.

Lessons Learned

The above cases represent a wide variety of hybrid warfare situations. Through our analysis of these cases, we have developed a series of lessons learned which are below.

- *Unique Case:* As we can see by these three cases, no cases of hybrid warfare are the same. Crimea was a unique case where hybrid techniques were particularly effective because of its history, ethnic makeup, exposure to Russian media and culture, and the presence of Russian military forces. Additionally, Crimea was limited to a relatively short period of time, while Estonia and the South China Sea show that hybrid strategies can be used over a long period of time and during a wide variety of conflicts over that time.
- *Phase Zero Is Vital:* In Crimea, Russia showed that 'phase zero' shaping operations are key to effectively implementing their hybrid strategy. When the international community finally saw there was the potential that the Ukraine could lose Crimea to Russia, it was already too late to counter the actions taken by Russia to prepare the battlefield.
- *CF Are Crucial:* The threat and use of CF were crucial to the ability of Russia to implement its hybrid strategy and thus fully complete its annexation of Crimea. Ukraine could not risk open warfare with Russia because of the threat of conventional conflict, and once Russian CF were deployed to Crimea, they served as a cleanup force; removing the remaining Ukrainian government elements on the peninsula.
- *Slow Response:* Consistently, across all of the actors in the international community, the response to Russia's actions in Crimea was slow. This slow reaction shows a broader inability of the international community to react quickly to crises involving important players on the world stage. While the UN Security Council can react relatively quickly in these instances, when a great power is involved, it is nearly impossible for them to be rapid.
- *Constrained Responses:* The international community is severely constrained in its ability to respond to hybrid techniques in situations like Crimea. It is constrained not only by the lack of a central authority directing a response, but also by the types of responses that are palatable to both allies and international norms. The increased economic interconnectedness and the perspective of many nations that military power should not be used at any point means that the international community does not have access to all the tools necessary to respond to hybrid situations.

- *Law Is Fluid:* One cannot rely on international law to take care of questions about the legality of a state's actions. As demonstrated in the case of the South China Sea, even cases that should be cut-and-dried can be open to questions of procedure and jurisdiction, and competing interests in the international community can prevent a case from ever seeing its day in court.
- *Decisive Intervention or None at All:* Despite the whole-of-government approach necessary to wage a hybrid war, those defending against it often hobble themselves in their responses. Rather, the actors moving against hybrid action tend toward limited intervention. Often, this has the effect of not only failing to counter the hybrid threats, but also of both discrediting the defender and strengthening the claim of the aggressor, as was observed in the U.S.-led freedom-of-the-seas missions in the South China Sea. Instead, defenders should respond defensively or not at all.
- *Vulnerabilities Were Exploited, But It Could Have Been Much Worse*: While the 2007 cyber attack had a devastating effect on Estonian society, there are numerous other cyber vulnerabilities that were not fully exploited. It is imperative that this attack serves as a warning of future attacks to come and that national governments and international organizations work to close any remaining cyber security loopholes.
- *Attribution Is a Challenge*: The difficulty of attribution in a cyber war is challenging, particularly when it comes to determining the appropriate way to respond to an attack. By continuing to cast doubts about attribution of actions, Russia has been able to encourage attacks against Estonia without facing any serious consequences. This will be a trend that will likely continue, particularly as Russia attempts to threaten and undermine the NATO alliance without going so far as to provoke the invocation of Article 5.
- *Cyber Warfare Impacts Much More than Just the Internet*: While the cyber element of hybrid warfare certainly has technological implications, the Estonian case highlights the fact that these attacks have a much broader impact on society. By compromising critical infrastructure, cyber attacks have the ability to paralyze a nation. Additionally, by perpetuating misinformation, cyber action can shape public perceptions of their government. Because of this, countering cyber warfare requires more than just technical means.
- *Technological Advances Have Allowed Individual Actors to Have an Increasingly Significant Impact:* The role of individual 'hacktivists' in this attack cannot be overstated. This highlights the way in which technology has allowed individuals to have an increasing role in hybrid warfare, further complicating government responses to these attacks and attack attribution.

Notional Case: Baltic States 2020

Background

The Calm Before the Storm

On a cold night in Lithuania, during the early winter months of 2020, 50 Spetsnaz operators jump off the train between Minsk and Kaliningrad into the forests that cover the route through Lithuania.

They have come to join the large contingent of Russian special forces already operating in the country. These Russian forces have been filtering slowly into the country on tourist visas and previous train jumps over the last six months. Upon arrival, they have consolidated into small teams and taken refuge in the small Russian-speaking enclaves scattered throughout Lithuania. While the train was heavily guarded in the past, and tourist visas were restricted to those not connected with the Kremlin, the continued economic crisis in the EU has struck Lithuania hard. The Lithuanian government is having a difficult time putting together the necessary resources to prevent the train jumpers. Russia has taken advantage of this lapse and has begun the preparations for a full occupation of the Baltic states.

Russia's focus on Lithuania is not surprising. The Lithuanian government remains the most hostile of all the Baltic states, and the country sits between Belarus, which has been absorbed into Russia through a confederation agreement, and Kaliningrad. This leaves the strategic 'Suwalki Gap,' on the border between Lithuania and Poland, as NATO's only land access to the Baltics. Russia knows that to achieve their goals, the gap, and Lithuania as a whole, must fall quickly to prevent NATO from intervening.

The situations in Estonia and Latvia are different. While the Estonian government remains staunchly pro-EU and NATO, the government has been forced to make a variety of political and cultural concessions to the ethnic Russian populations in the east in an effort to maintain cohesion in the country. Despite this, there has been a rise in discontent among the Russian-speaking population. This feeling has been boosted by a strong ethnic Russian political party, whose power is concentrated in Russian-majority areas,[456] fostering a feeling of disenfranchisement among ethnic Russians, as well as a variety of pro-Russia non-governmental organizations (NGOs) operating in majority Russian areas. The party has been especially successful at a local and regional level, but, because of Estonian voting restrictions, it has not achieved power at the national level. The recovery in oil, and thus the Russian economy, has helped the Russian government assist its 'citizens' living in Estonia. Russian rubles have poured in to support not only pro-Russia political parties and NGOs, but also Russian companies, who have slowly taken over certain sectors of the Estonian economy, especially transportation, real estate, and consumer shopping. Additionally, Estonia remains isolated. While its traditional allies, Sweden and Finland, joined NATO in 2018, the economic crisis that has affected the entire EU is stifling military cooperation and exercises in NATO and preventing NATO troop rotations into the Baltic states.

In 2016, for many Western analysts, Latvia looked like the weak link in NATO's defense against Russian aggression. This view has been borne out over the last four years. Already powerful in the middle of the decade, the pro-Russia Harmony Center party has taken control of the Latvian government on the backs of ethnic Russians living in Latvia and disaffected Latvians who were looking for a change from the myriad ethnic Latvian parties, which have dominated the government since independence.[457] When the Harmony party took control of the government in 2018, they began to make overtures to the Russian government. While still a member of both the EU and NATO, Latvia has moved closer to the Russian orbit under the Harmony party's leadership.

No longer do the Baltic states present a unified front against Russian aggression. While NATO still relies on the military heft of the U.S., western European countries have been hurt by the economic crisis and slow growth over the last four years. Many are no longer in a position to substantially help their eastern allies if an attack were to occur.

Meanwhile, the economic situation in Russia has improved dramatically with the rise in oil prices over the last three years. OPEC's decision to cut supply in 2017 after years of very low oil prices, combined with the continued turmoil in the Middle East and the recovery of commodity demand in China and other developing countries, has caused oil to settle around $90 a barrel. However, Russia's domestic political climate is less stable. The long years of economic hardship have taken its toll on the popularity of Vladimir Putin, who was elected to a fourth term as president in 2018. Despite the improving economic situation, the Russian government continues to feel under domestic pressure to further show the Kremlin's strength and authority. This is no different from 2008 when, despite high oil prices and strong economic indicators, the Russian government pursued aggressive action in Georgia. While he remains popular among the poor and uneducated, there is a growing class of middle income peoples who desire a new direction for their country and they are looking west.

The Preparation

Since his reelection, President Putin has been preparing to put to rest the idea that Russia needs to turn to the West to improve its place in the world. Russian exceptionalism continues to ooze out of the Kremlin's tall towers. He has focused the government's considerable official and unofficial propaganda networks at the domestic population in an effort to convince them that the West is corrupt and dangerous. For example, the Kremlin has released a series of video games that target the young male population in Russia to indoctrinate them into a view of their country as a great power. The video games are set in the present day and, as the player, your goal is to bring Russia back to glory by conquering other countries using a variety of methods. The games have become extremely popular in Russia, but, worryingly, have also become popular in other parts of Europe and East Asia.

Putin has focused specifically on discrediting NATO and the EU in this propaganda. In addition to the domestic audience, the Kremlin has also focused its media efforts on the ethnic Russian populations along its border, particularly in Estonia and Latvia. With the introduction of ETV+, a Russian-language channel sponsored by the Estonian state in 2015, Estonia took a step forward in trying to defend against the propaganda pouring into the country from Russia. However, ETV+ can't compete with the production value or the financial support that the Russian networks provide. While some Russian speakers in Estonia have turned to ETV+, the majority still get their information from Russian networks. Lithuania's efforts[458] to highlight and prevent propaganda from Russian sources has been effective over the last few years, which has been a slight blow to the Kremlin's efforts. However, it has not been enough to undermine the propaganda campaign on the Baltic states as a whole.

In addition to preparing the ground with propaganda, Putin has also directed other activities, all designed to further discredit the EU and NATO. In 2017, right before the Latvian general election, the Russian government shut down the vitally important train transport connections between Russia and the Latvian capital of Riga, using economic tightening measures to support domestic industry as the reason. The action put a strain on the already economically fragile country and particularly its most vulnerable citizens, the ethnic Russians who work on the rail lines running across the country. Blaming the shutdown on consistent EU interference and regulation in the transport industry, Russia was able to discredit the West, while helping the Harmony party to finally come into government as the majority party in the Saeima.

Kinetically, Putin ordered further snap exercises of Russian military forces already stationed in the Western Military District. Those were combined with continued flyovers of NATO airspace by Russian TU-95 bombers and SU-35 fighters, as well as increased infiltration of NATO territorial waters by Russian submarines. He also increased the number of heavy mechanized units along the border with Estonia and Latvia. Additionally, Putin ordered the insertion of Spetsnaz special operators into Lithuania to begin planning how an insurgency could close off the Suwalki Gap if a limited war did break out between Russia and NATO. Spetsnaz operators have also been active in both Estonia and Latvia. They have been openly seen in the Russian majority city of Narva in eastern Estonia, and other parts of the country have seen men who do not carry weapons but are advising local Russian populations on civil disobedience activities.

Unfortunately, the Estonian government is limited in their response. Since the incident where an Estonian Defence League[459] volunteer killed an ethnic Russian boy in Narva two years ago, the Estonian government is concerned about deploying either the military or police into the city. The Estonian Defence League units are especially restricted from the area, as many Russians now view them as a tool of Estonian nationalists. At this point, the local police force runs the town. While they remain loyal to the Estonian government in Tallinn, their loyalty could be tested in the future. In Latvia, Russian operators now openly train ethnic Russian youth in the east. They call these 'day camps,' but in reality they are training them in insurgent operations. While the U.S. and NATO have both identified the threat that these camps pose to the Latvian government, the government has not taken any steps to disband the camps and reportedly supports them through party money.

These are just a few of the preparations that the Russian government ensured were implemented before they launched any attack on the Baltics.

The Plan

Putin's goal was simple, though his plan was anything but. His goals were mutually reinforcing—to secure his domestic position in Russia through fragmenting NATO. The plan involved a variety of methods, but followed the non-linear or hybrid warfare strategy that had been in place since General Gerasimov established the doctrine in 2014. In reality, this combination of irregular tactics and conventional tactics was nothing new for the Russians or, really, the rest of the world. However, since their failure in eastern Ukraine, Russia has worked to perfect the doctrine.

The plan combines IO, SOF, lawfare, political action, economic warfare, and, of course, CF. Some of these techniques will have been in use for years, while others will be deployed at strategic junctions in the conflict. The target—eastern Estonia and Latvia—has been saturated with propaganda and other Russian influence for years and is ripe for the taking. From its Ukraine experience, the Kremlin understands that it cannot take on too much or expect the population to tolerate oppressive and brutal rebels. Instead, this operation will be smaller in nature and be fully run by Russian forces. No date was set for the action to start, rather the Kremlin believed that an inciting incident would take place, allowing the plan to come together. On 1 December 2020, that event takes place.

The 'Attack'

The winter of 2020 has been particularly cold in the eastern parts of Estonia and Latvia, with temperatures averaging -30° C. On 1 December, a massive snowstorm[460] hits both Estonia and

Latvia, leaving thousands, especially in the poorer eastern provinces, without electricity or access to the transportation networks connecting them to the rest of the country. The Kremlin has been looking for an entry point and the weather brought it to them.

The storm has knocked out the ability for the Estonian and Latvian governments to respond to cries of help from their citizens in the east. Moreover, what is later identified as a computer virus originating from a Russian IP address has altered both countries' abilities to remotely track power outages, as well as their phone lines for citizens to self-report outages. As a result, while the Russian-dominated areas of both countries suffer in darkness, it appears to their governments as if nothing is amiss until the damage is already done. Unaware that their governments have no way of knowing of their suffering, the Russian-speaking populations come to believe that their national governments are unable or unwilling to help them. Therefore, the first call for help comes, not from a co-opted local politician, but from the Harmony party government in Riga. Without the ability to get severely needed food and medicine to the remote areas in the east, they have turned to the Russian government for help. The Russians are only too willing to support the request and quickly deploy military convoys, along with paratroopers, to get to the most remote locations. Two days after the call for support, Russian military forces are firmly ensconced in Rēzekne and Daugavpils, nominally running the eastern part of Latvia.

The call for help in Estonia comes from a different source, the mayor of Narva. Using local security forces, with the help of Spetsnaz operators, the mayor relieves the border guards on the bridge connecting Narva with Russia. Minutes later, Russian military convoys begin crossing the border, bringing diesel generators, fuel, and food with them. They spread out quickly from the center of the city and head toward the more remote parts of Narva province. Since they were pulled out of the province after the 2018 incident, there are no Estonian Defence League forces to impede their progress. In less than two days, the Russian military has administrative control over Narva province. Despite this seemingly quick and easy victory, Russian forces in both Estonia and Latvia stop there and maintain their limited territorial aims. Holding to the plan is essential in order to ensure that further expansion does not risk accomplishing the goal of the "attack."

The Response

As Russian forces flow over the Narva-Ivangorod bridge, Estonia immediately calls an emergency session of NATO and asks for Article 5 consultations. They also contact the government in Riga asking for their support and interest in joining their call to activate NATO Article 5; they receive no response. During the emergency meeting, Lithuania, Poland, Norway, and the U.S. quickly come to the rhetorical aid of Estonia, calling on the alliance to do its duty and push out the Russian military using force, but there is opposition. Germany and France, both hurt severely by the economic situation in Europe, call for calm and a focus on a diplomatic solution; they cannot afford the fight, much less the likely cutoff of Russian natural gas to their countries. Additionally, Russia has worked for years to essentially buy NATO countries using aid packages and cheap energy exports. For example, Greece and Portugal[461] will not vote for Article 5.

By the end of the debate it is clear what the result will be; NATO will not come to the aid of Estonia using military forces. Instead, the alliance turns to the tried-and-true method of many international institutions—they announce that NATO is condemning the action and call on the Russian military forces to remove themselves from Estonian territory. The U.S., along with Poland and Lithuania, choose to go it alone and inform the Estonians that they will come to their aid using forces already in place in Poland and Germany. However, they will not risk open war with Russia.

The two U.S. brigades put in northern Poland in 2017 begin to mobilize with the decision to support Estonia. The idea is to combine these forces with two Polish brigades and travel through the Suwalki Gap and up to Estonia via Latvia. The troops have been on alert for several years, so they mobilize quickly and, within two days of the decision, are ready to move forward. In the meantime, U.S. rapid reaction forces from Germany have been flown in on C-17s to Tallinn; however, with the first flyover of the Baltic Sea, they receive a warning from anti-aircraft batteries in Kaliningrad: "Do not overfly this area, this airspace is under the control of the Russian military. We will fire on any overflight." Instead of risking the shoot down, U.S. forces begin to transit from Germany to Tallinn by overflying the Scandinavian Peninsula, adding a significant amount of time to the transit schedule.

As the main force of U.S. and Polish brigades begin to move through the Suwalki Gap, strange things begin to occur. At some points, they find downed trees across the roads, and at others, burning cars; then the attacks come from the forests. Russian operators using insurgent tactics and anti-tank weapons launch devastating assaults on the CF and their supply lines as they move through the Gap. Lithuanian Special Forces with USSOF teams attached attempt to root out the Russian operators, but years of Russian preparation and infiltration make it even more difficult to fight these troops. Moreover, the lack of secure communications equipment on the part of the Baltic forces has caused USSOF teams essentially to scatter amongst the Baltic teams to serve largely in communications roles, preventing them from directing their efforts toward combatting the invasion. In the meantime, Russian forces solidify their lines in Narva province, and the Latvian government remains quiet on the topic.

On the international stage, the U.S. and their Western allies fully condemn the moves by Russia as an attack on the Baltic states, but are slow to intervene due to domestic politics. On the one hand, Cold Warriors in Congress are calling for decisive and immediate intervention to prevent Russian expansion. But, following the election in November, the president has entered a lame duck period in which the executive branch is attempting to take only necessary actions and defer the expansion of the response to the future administration. And, crippling national debt and a general lack of desire to intervene in what appears to be another regional conflict have led younger members of Congress on both sides of the aisle to actively caution against intervention. Russia counters that it had a responsibility to ethnic Russians no matter where they reside to ensure their safety and wellbeing in the event of a crisis. They continue by saying that the Baltic governments could not or would not provide the needed support to their citizens, so the Russian Federation had a legal and moral responsibility to intervene. Additionally, they note that the Latvian government invited their troops into the country to support their efforts.

Freezing the Conflict

With the tepid response coming from all corners of the NATO alliance, the Kremlin knows that they have an opportunity to not only accomplish their goal of fragmenting the alliance, but also the opportunity to de facto annex the Russian majority province of Narva in Estonia, as well as bring Latvia officially under its sphere of influence.

On 15 December, Latvia officially halts the U.S., Lithuanian, and Polish brigades from crossing the border from Lithuania into Latvia. They will not be able to come to the aid of the Estonians over land. When asked to clarify their position by the NATO Secretariat, the Latvian government replies that, given the current state of emergency, they could not support the movement of such a large number of troops through their territory. Many, especially in the U.S.

government, see this as the beginning of the end for Latvia in the NATO alliance. The brigades are effectively stranded until air assets can be diverted to support lifting the combined manpower and equipment.

On 27 December, Putin flies to Riga to nominally negotiate with the government on the eventual withdrawal of Russian troops from the eastern portion of the country. Instead, he comes with an offer that will be difficult for the Harmony party to turn down: leave NATO, maintain its connection with the EU, but also join the Eurasian Economic Union in exchange for military protection and economic assistance. This will effectively bring Latvia into the Russian sphere and territorially isolate Estonia. The next day, at the signing ceremony to announce the economic assistance package, the Latvian president announces the country's unilateral withdrawal from NATO. Under Putin's instruction, the president cites the lack of support and confidence in the alliance as the primary reasons for his decision to leave NATO. During the same press conference, Putin makes the stunning announcement that Russia is officially recognizing the province of Narva as an independent nation. He also announces that Russia will support its newest neighbor both economically and militarily, and calls on all patriotic Russians in Estonia to move to the new country. Since the beginning of the occupation, U.S., Estonian, Polish, and Lithuanian troops have all stopped at the provincial border. Putin states that this is a clear indication that the West has no interest in the welfare of the Russian people in the province and that the Estonian government has forfeited its right to control over the territory.

On 29 December, the Estonian president privately calls on the U.S. president asking for assistance to expel the Russian forces. After a long night of briefings from the military and the State Department, the president responds that it will be difficult to accomplish this without bringing the U.S. into an impossible war with Russia. With such limited access to Estonia because of Russian A2/AD capabilities in Kaliningrad and Latvia's move to withdraw from NATO, the U.S. cannot risk conflict on such poor terms. However, the U.S. will still support Estonia as it adjusts to the new normal. It will be an island in a sea of Russian influence.

The Aftermath

The events in the winter of 2020 serve as a death knell for the NATO alliance. The alliance's refusal to act to protect Estonia leads many of the members most threatened by Russia, including Lithuania, Poland, Finland, Sweden, and Norway, to reevaluate the alliance and their futures as members. They all cite the threat from Russia and the unwillingness of the alliance to combat that threat as the key reason for their reevaluation and potential withdrawal. The U.S. maintains the alliance, but significantly decreases its commitment by removing its forces from NATO command and control. The U.S. redoubles its commitment to the states most threatened by Russia, but still refuses to permanently base a large number of forces in those countries.

The event also reveals deep divides within the NATO alliance, pitting the U.S. against France and Germany over intervention. To make matters worse, the U.S. ultimately decides to go back on its interventionist position. Rumblings begin among the allies that perhaps U.S. leadership is waning.

The Russians accomplish their goal of fragmenting NATO by calling their Article 5 bluff. They also add a few benefits through the de facto annexation of Narva and the inclusion of Latvia into Russia's sphere of influence.

Analysis of Key Components Used

Economic Warfare

As with other Russian hybrid campaigns, economic warfare featured prominently in the notional case. The Baltic states are all economically dependent on Russia to varying degrees, with Latvia as the most dependent of the three. Russia's decision to shut down rail transport to Riga was key in drawing Latvia closer to Russia, which was necessary to produce the desired result of its defection from NATO. The suspension of the rail transport industry not only weakened the economy as a whole, but also targeted the Russian minority population in Latvia, as the majority of those employed by the railroad and shipping companies who use it are members of the Russian minority. Although it was Russia's decision to stop the transport, it was able to use its control over Russian-language media content in the region to spin the story as the fault of the EU, fostering a sense of discontent and alienation among the Russian-minority population.

In addition, Russia capitalized on its control of the European oil and gas market by essentially buying votes in NATO. They combined their diplomatic and economic actions to negotiate low-cost energy deals with NATO members like Germany and France. This move tied those countries to Russia both diplomatically and financially. As a result, when an Article 5 vote came to stop Russia in the Baltics, NATO was unable to reach a consensus.

Diplomatic Action

Outside of the Baltics, Russia capitalized on Greece's and Portugal's precarious financial situations to build stronger relationships with those countries, making them more and more dependent on Russia's goodwill. As a consensus-based organization, NATO depends on the strong leadership of the U.S. and the maintenance of common interests and values across its member states for effective decision-making. Knowing this, Russia was then able to use that leverage to undermine NATO's decision-making process with regards to Article 5 and deal a blow to the credibility of the organization as a whole.

Within the Baltics, Russia's strongest diplomatic move came in the form of its relationship with the Harmony party–led Latvia. Through historical ties, early support for the party, and actions taken throughout the attack, Russia was able to strengthen its relationship with the party and ultimately encourage Latvia as a whole to leave NATO. Latvia's decision to leave the alliance proved the death knell for Baltic unity and had long-lasting effects on NATO as a whole and American leadership within it. Therefore, Russia's diplomatic action and its results were the cornerstone of the hybrid attack and proved vital to achieving Russia's goal of fracturing NATO.

Political Action

Russia's political action largely focused on fostering Russian-minority parties and divisions within the national governments of Estonia and Latvia. In Estonia, the rise of the Russian minority party and its transition from a regional power within Estonia to a real player on the national stage brought the fracture in Estonian society between the ethnic Russians and ethnic Estonians to the fore. This undermined the legitimacy of the Estonian state and left it more vulnerable to other advances.

In Latvia, the effect was compounded in that the pro-Russia Harmony party was able to take power in the country and act as the key decision-maker in the crisis. It is likely that this

campaign in the Baltics would have gone differently if the Harmony party had not been in power, as a non-Russian-minority government would not have had the existing relationship with Russia. It was the relationship with Russia that precipitated the government's decision to stop the movement of NATO forces through its borders, effectively ending the conventional conflict and leading to its withdrawal from the NATO alliance. Russia's political action in helping the Harmony party take power in Latvia was a long-term plan, but one that paved the way for the hybrid campaign to come. Ultimately, by supporting the rise of Russian-minority parties, Russia was able to foster disunity within Estonia's government and ultimately create a puppet state in Latvia.

Lawfare

Russia's use of lawfare in this campaign focused more on capitalizing on existing norms and decision-making processes to justify the actions of others, than to support its own actions. Most prominently, it exploited the consensus decision-making in NATO to expose the ineffectiveness of the process. Rather than attacking the process itself, it was able to manipulate members of the alliance into undermining the ability of the alliance to agree that collective defensive measures should be taken under Article 5.

Moreover, Russia capitalized on the international norm of respecting state sovereignty. Russia knew that the U.S. depended on Latvia's consent to move troops through its borders into Estonia and that the U.S. would have to pull out, should that consent be withdrawn. Therefore, it used its leverage in Latvia to encourage the Harmony party government to do just that. Because state sovereignty is a well-established international norm, the U.S. had no choice but to comply, and the conflict was frozen as a result.

Cyber Action

Russia's use of cyber action in this campaign was particularly interesting in that the cyberattack was not intended to be an attack in and of itself. Rather, it was meant to prevent the Estonian and Latvian governments from acting in the way that they would have otherwise, namely supporting the populations on their eastern frontiers as quickly and effectively as possible, given resource constraints. However, by preventing the appropriate authorities within the Estonian and Latvian governments from fully grasping the extent of the power outages and damage inflicted by the storm in the eastern regions of their countries, the Russians were able to play up the narrative they have perpetuated that these governments do not care about the Russian-minority populations. This not only gave them an excuse to move into the countries, but also exacerbated the existing fractures in Estonian and Latvian societies between the majority and minority populations.

Military Operations: Conventional Forces

Russia's CF were used in two broad functions: to support power projection, which will be discussed in a later section, and in an A2/AD strategy. The A2/AD actions based in Kaliningrad were key in controlling the U.S.-led conventional counterattack once it had decided to intervene, as it forced the U.S. to move through the Suwalki Gap. By funneling forces through the gap, it concentrated them in such a way as to make it easier for Russian SOF to harass them and slow their advance. Moreover, it made the U.S. dependent on the consent of Lithuania and Latvia to aid Estonia, which proved less reliable than previously anticipated. Once Latvia decided to stop all forces moving through its borders, the U.S. was unable to support Estonia with CF, effectively freezing the conflict.

Military Operations: SOF

Russian SOF were largely focused in Lithuania to secure the Suwalki Gap and mobilize small pockets of Russian-speaking populations within the country. Because of the A2/AD strategy employed by Russia in Kaliningrad, U.S. forces were forced to move through the Suwalki Gap to reach Latvia and Estonia. This left them open to Russian SOF insurgent tactics, which had devastating effects on the U.S.'s supply lines and CF as a whole. Although USSOF attempted to counter these efforts, Russian forces had years of preparation, making them difficult to root out of sympathetic Russian-speaking populations. Moreover, USSOF were largely scattered amongst Baltic nation SOF to support communications between the Baltic operators and the U.S. forces, because of the limitations in secure communications equipment among those nations.

Power Projection

Russia's power projection efforts were focused on the period leading up to the conflict. In the months leading up to the beginning of open hostility, Putin ordered snap exercises along Russia's western border, complimented by increased flyovers and submarine traffic in NATO territorial waters. While this did not have a direct impact on the conflict to come, it served to ratchet up tensions in the period leading up to the outbreak of fighting. Moreover, it demonstrated the power of Russia's military to both Russian-speaking minorities, who have been feeling increasingly abandoned by their national governments, and the national governments themselves, who were feeling increasingly encircled by Russia and isolated from their NATO allies. Finally, it demonstrated to the U.S. Russia's level of commitment to defending its western frontier, forcing decision-makers to think carefully about whether defending the Baltics would be worth the losses the U.S. would likely incur in a conventional conflict. All of this served to prepare the battlespace for the wider campaign to come.

IO

Russia employed a two-pronged strategy with regards to the information warfare aspect of the campaign. The first was traditional propaganda directed at the Russian-minority populations of the Baltic states in support of the campaign. These efforts capitalized on Russia's near complete control over Russian-language media in the Baltics. Because Russian-sponsored news sources are typically the only ones the average Russian-speaking citizen in the Baltics follows, Russia is able to spin any story the way that is most in line with its strategy. Therefore, it was able to prepare the battlespace incredibly effectively for any number of the hybrid components it used in the wider campaign. For example, as previously mentioned, although it was Russia who shut down rail transport to Riga and thus severely damaged the economic situation of the Russian minority in Latvia, Russia was able to redirect that anger and frustration against the EU. Therefore, the IO in the Baltics were foundational for the wider campaign, as it paved the way for the political, economic, diplomatic, and cyber activities that followed.

The second was a wider campaign to spin its actions in the Baltics and their outcome for both its domestic population and those of the Western nations. In essence, if the goal of the engagement was to discredit NATO and fracture its eastern flank, the entire campaign was an IO. Every move Russia took in the conflict was carefully chosen to demonstrate the ineffectiveness of the NATO alliance and its inability to protect its member states. Those choices culminated in Latvia deciding to leave the alliance and ally itself more closely with Russia. Latvia's actions sent a strong message that other states may be better off looking to Russia for protection, rather than

relying on a U.S.-led NATO alliance. By spinning the conflict through its IO structure, Russia was able to translate its victory in the Baltics into a wider victory against the West, showing both its own population, and that of the Western states, that Russia is still a superpower and will not stand for incursions into its sphere of influence.

The Analysis: How Hybrid Warfare Was Used in this Case

When mapped as a network, shown in Figure 13, Russia's hypothetical campaign against the Baltics is a highly complex set of components and actors, many of which reinforce each other. One of the more interesting aspects of the attack, which becomes visible in Figure 13, is the variety of targets involved in the campaign and their use in activities against each other. The people of each country are often targeted separately from their governments, fracturing the relationships between the states and their constituents. This contributes to Russia's strategic goal to destabilize NATO's eastern flank and undermine the alliance as a whole. Similarly, the West in general, NATO in particular, and the U.S. as NATO's leader are all approached slightly differently in the attack, complicating the place of each within the other.

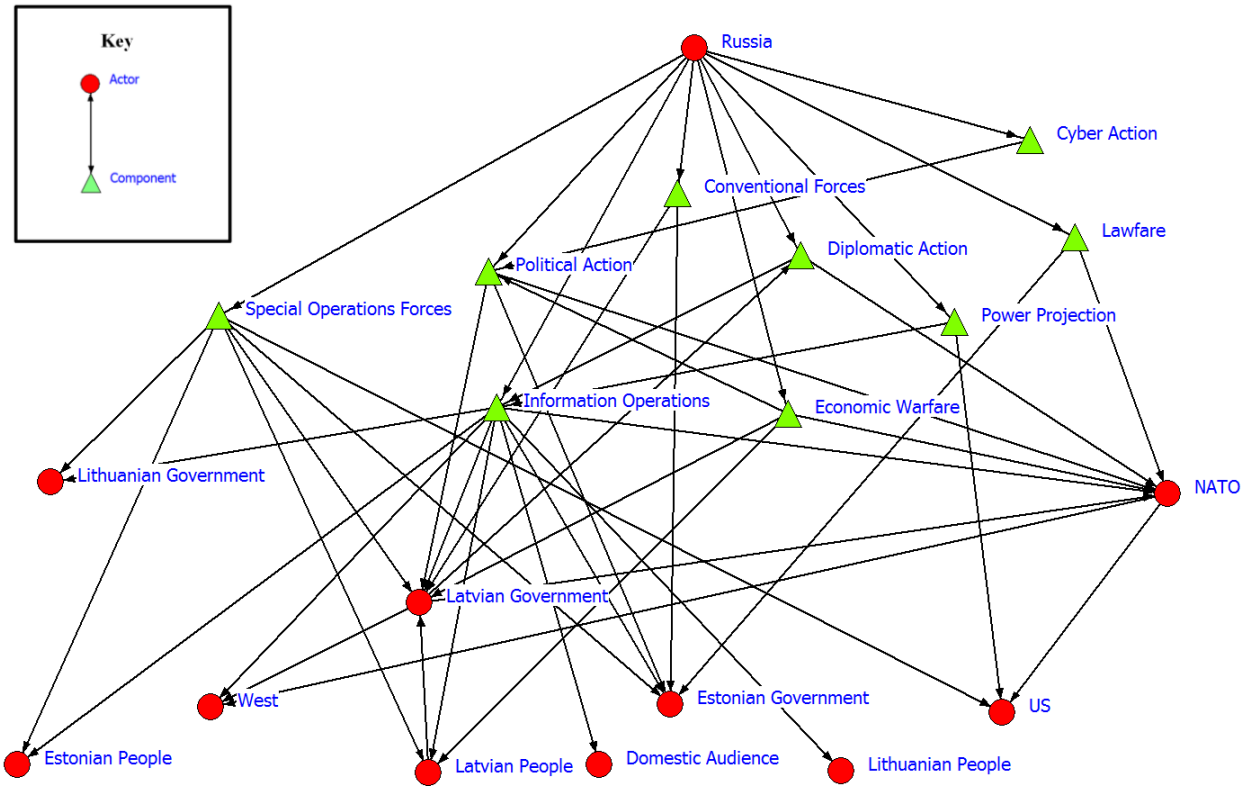

Figure 13: Baltics 2020 Network Map

To further elucidate these relationships, this analysis will turn to one specific action within the case: the Latvian government's decision to leave NATO, shown in Figure 14.

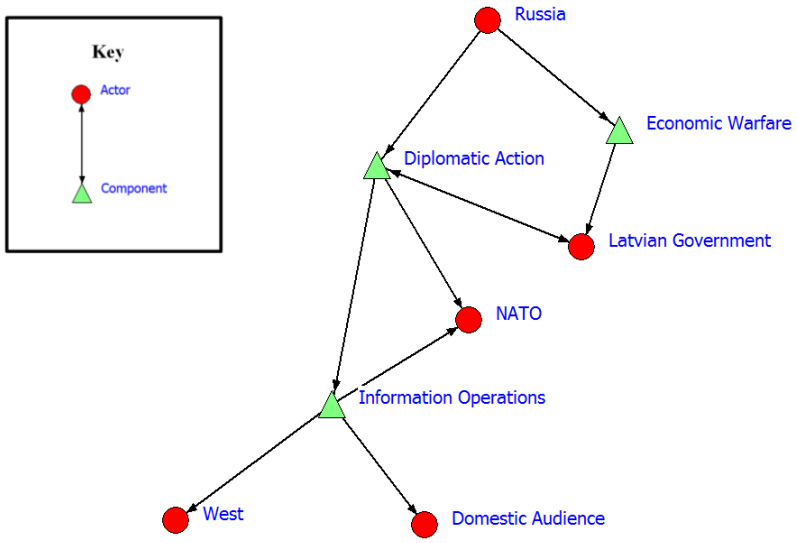

Figure 14: Baltics 2020 Latvian Exit Network Map

Initially, Russia used its economic leverage and its diplomatic ties to Latvia to push the state into the decision. From there, Latvia's action was, in itself, a diplomatic attack against NATO, signaling the potential breakdown of the alliance. It also served within a larger IO with largely the same message, namely that NATO is not the strong, cohesive alliance that its members want the world to believe. Interestingly enough, this message is directed at both the Russian domestic audience, serving to further demonstrate the strength of the Russian leadership and the weakness of its historical enemies, and the West, calling into question the continued relevance of the NATO alliance.

In short, the Latvian government's decision to leave NATO had deep origins and far-reaching consequences. Although potentially devastating in the long run, the networked approach does offer some hope for more effective intervention. The relationships between the components and actors mean that an intervention meant to counter the move could focus solely on Latvia's decision-making, rather than trying to combat the fallout. If the Latvian government's actions are taken out of the network, the rest of the relationships in Figure 14 disappear.

Conclusion

Despite their geographic proximity and shared history of Soviet occupation, the Baltic states have very different histories, cultures, and political situations. As such, any intervention coming from Russia would necessarily be complex and tailored to each state. To successfully counter such an attack, interventions must take into consideration the nuance of the Baltic states and the interconnectivity of the hybrid attack.

Part III

Lessons Learned and Recommendations

Introduction

While parts I and II were focused generally on hybrid warfare, Part III of this project focuses specifically on Russian hybrid warfare and ways to counter it. Part III is focused on lessons learned that have been gathered through both academic and on-the-ground research. Our team has taken these lessons learned and used them to develop a set of recommendations for each actor that we see having a role in countering Russian hybrid warfare.

Lessons Learned

For anyone charged with dealing with the threat of hybrid warfare, we believe there are several lessons learned that transcend the context of the particular geo-political situation.

1. *Do Not Fight Your Adversary at Its Strength.* In the example of Russia, the Russians clearly hold an advantage in the IO field. Thus soft-power interventions, particularly those focused on IO, should not attempt to meet Russia at its strength. These interventions are less likely to succeed and may have the unintended consequence of reinforcing Russia's perceived dominance in the arena.
2. *Treat Hybrid Warfare as a Network.* Countering each component individually is inefficient and ignores the nuance of a hybrid campaign. Instead, interventions should view a campaign as a network and target countermeasures toward particular actors and components in order to disrupt the campaign as a whole with minimum investment.
3. *Hybrid Campaigns Are Complex and Customized.* A hybrid campaign is highly customized for the population at which it is directed. Therefore, a counter-campaign must show the same level of understanding of both military and civilian actors within the battlespace, as well as cultural and linguistic elements that affect the views and activities of that society.
4. *Each Hybrid Campaign Is Different.* No hybrid campaign is the same. While similar components may be used against different targets, the network and method for creating the campaign will change every time. Therefore, those planning countermeasures should avoid assuming similarities with previous campaigns to avoid fighting the last war.

Recommendations

European Union

The EU is a vital part of any counter–hybrid warfare strategy in Europe. The organization not only has the resources to provide assistance, but also has the mandate to assist on soft security aspects in which it would be inappropriate for NATO or the U.S. military to partner with host countries. The following are recommendations for the EU:

1. *Integrate Ethnic Russian Minority Populations.* The EU must do more to provide support to governments with significant ethnic Russian populations by helping those governments better integrate minority populations. The EU itself should not focus on building national

identities, but can help support individual governments. The EU can play a part through financing integration programs, education programs, and media content, but the tastes and preferences of Russian-speakers must be carefully considered when developing these programs.

2. *Build a European Identity for Russian Minorities.* In the Baltic states, there is already a fledgling European identity among the ethnic Russian population, however the EU could do more to build a more robust identity for Russian minorities within the broader European community. This could be accomplished through funding for professional education, educational exchanges, internships, educational stipends, support to business ventures, and other forms of financial assistance to these populations.
3. *Increase Border Security*. Because of the current refugee crisis, the EU is focused on its southern borders; however, the eastern border must also be at the top of the organization's priority list. Hybrid strategy calls for the infiltration of agents through porous borders. Once inside the EU, these agents can move freely. Therefore, the EU should support increased border security and training for border patrol officers along the eastern border. Additionally, the EU should work with individual countries to finance and provide training for electronic sensors to better enable border security. By ensuring a high standard of professionalism and supporting contingency planning efforts in the case of overt or covert border infiltration, this will allow the Baltic states, as well as other Eastern European members of the EU, to be better prepared to keep out malevolent actors.
4. *Support Russian Language Media.* The EU should support the development and/or financing of Russian-language television channels targeting Russian-speaking populations in the EU. Despite Estonia's efforts to provide alternative Russian-language media through their own channel, ETV+, it is severely under-financed and could benefit from support. However, as mentioned previously, the content must match the aesthetic and format that the audience is familiar with, otherwise it will have limited impact. Particularly, these programs should be geared primarily toward entertainment and not politics to avoid the implication of Western propaganda.
5. *Increase Economic and Energy Security.* Economic and energy vulnerabilities pose a significant threat in the Baltic states, and in other Eastern European EU members threatened by Russia. The EU should pursue trade and energy security policies to mitigate this dependence on Russia. Specifically, the EU should provide financing to encourage the construction of additional liquid natural gas import terminals in its eastern members. As in the case of Lithuania, these terminals can be significant bargaining chips against extreme Russian energy policies. These policies, and the freedom that would be provided through them, could be used as a leverage point against Russia in the future.

NATO

NATO remains the security guarantor in the Western world and continues to serve as the primary adversary—whether perceived or actual—of the Russian Federation. Maintaining NATO in this role is key to ensuring peace remains the de facto state of international relations on the European continent. Thus, NATO must continue, and expand its role in the Baltic states and in other Eastern European member states. We recommend that NATO pursue the following general recommendations to ensure that it continues to serve as a counter to Russian aggression in its near-abroad:

1. *Continue Conventional Rotations, Exercises, and Training.* The continuation of rotations, exercises, and trainings conducted by conventional NATO forces is vital to the maintenance of security in the Baltic and in Eastern Europe. Particularly, NATO should make an effort to include local volunteer defense forces, like the Estonian Defence League, in their training and exercise efforts. The continued presence of NATO forces on NATO's Eastern border, as well as the efforts to train host country forces, is vital to the sense of security for the member states who border Russia or feel threatened by Russian activities. Additionally, the continuation of exercises to prepare host country militaries for various contingencies is vital. Even if these conventional-force activities do not actually increase security against an invasion, the perception of their value from host country citizens and NATO member-state audiences is just as important and increases NATOs perceived internal and external legitimacy.
2. *Increase Public Affairs Efforts.* Contact between member-state civil affairs and public affairs teams and NATO HQ should be increased. This effort would also include providing more Russian-language content on the NATO website and other resources sponsored by NATO. Many Russian-speakers seek out a variety of news sources (both Western and Russian). While Russian-speakers may be wary of the information broadcast through the NATO website because of perceived bias, it is still important that Russian-language information is freely provided for them by NATO to educate Russian-speakers about the alliance without opening NATO to accusations of propaganda or bias.
3. *Expand Presence in Ethnic Russian Majority Areas.* Increase the presence of NATO non-combat personnel in Russian-speaking minority areas in countries with significant minorities. For example, we would recommend that NATO work closely with the Estonian government to do outreach programs in Narva, such as visiting schools, contributing to construction projects, meeting with local leaders and Russian-speaking journalists, and participating in cultural exchanges and other events that are not military in nature. By increasing its representation in these areas, NATO can show Russian-speaking minorities that NATO is not coming to threaten them or destroy their way of life, as many believe. Expanded presence can also show that NATO is a force for good by performing activities to better communities in these areas. Finally, an expanded presence shows strength, which has traditionally commanded respect and support among ethnic Russians.
4. *Expand Cyber Defense Capabilities.* NATO needs to take more steps to understand and proactively prevent cyber attacks. There also needs to be a clearer understanding within NATO of how cyber attacks fit into the collective self-defense framework. This conversation began at the Wales Summit and was clarified at the Warsaw Summit. Ambiguity in the invocation of Article 5 should remain the standard in order to not limit NATO's ability to respond; however, NATO must have clear guidelines on how it would react to a cyber attack that does warrant an Article 5 consultation.
5. *Ensure that Article 3 Is Followed.* NATO leadership must do more to ensure that member states abide by Article 3 of The North Atlantic Treaty. The two percent threshold is an important marker, but a balanced scorecard of effectiveness in judging members on their preparedness would be valuable. While a more robust outline should be pursued for a new scorecard, the approach should focus on military spending, military preparedness, societal preparedness for military conflict, political preparedness for military conflict, preparedness for national and regional crises, and other related metrics. This scorecard should be created by an independent organization or consultancy similar to an audit for corporations.

6. *Streamline Crisis Response Processes.* NATO needs to further streamline its internal processes for crisis response. While some steps have been taken, the alliance needs to understand exactly how decisions will be made in case a quick response is required. The principle of consensus decision-making may be challenged by changing these processes, so, where possible, consensus should be pre-approved to allow for rapid action in particular situations that might evolve from a hybrid threat. If pre-approval is not possible, NATO should consider other options, such as continuing simulations focused on joint military and political decision-making and the creation of detailed protocols to be followed in case of crisis, accompanied by required training for those involved at all levels.
7. *Limit Prepositioning of Equipment.* We recommend that there should be limited prepositioning of equipment in the Baltic states. As has been shown through war games, NATO will not be able to adequately counter a Russian conventional attack on the Baltic. Prepositioning significant amounts of heavy equipment will not improve NATO's ability to hold the countries and would only serve to provide Russian forces with NATO equipment, should they occupy the region.
8. *Monitor for Overextension and Provocations.* The alliance risks becoming overextended with some of the recommendations being pushed by outside parties and members of the alliance. NATO leadership must monitor for signs of overextension of the alliance. Additionally, NATO must ensure that their activities are not seen as provocations by Russia. While Russia routinely calls all NATO activities provocative, there are clearly some activities that would require more than a rhetorical response from Russia. These activities would include a significantly larger, permanently based NATO force in the Baltics or larger exercises along the Russian border. These provocations would do little to increase preparedness of the alliance for an attack, but would do significant damage to the NATO-Russian relationship.

United States Government

The USG continues to be the Baltic states' primary ally in preparing to counter Russian conventional and hybrid activities. The USG has the resources, technology, and know-how to provide governments who feel threatened by Russian hybrid activities with support. Additionally, because the USG does not have the same multinational consensus-based constraints of NATO and the EU, it can provide a far wider range of support, not only to NATO or EU members, but also to allies outside of these circles.

1. *Improve Interagency Preparedness.* The USG must do more to prepare the interagency and National Security Council processes for reacting to rapid Russian hybrid actions. The process is optimized for a series of consultations, but in the event of the deployment of a hybrid tactic against one of America's allies, the interagency and the National Security Council staff are going to have to marshal the national resources more rapidly than is currently possible within the constraints of the process.
2. *Improved Communications Connections Among Agencies.* Push the Baltic governments, and those of other countries threatened by Russian actions, to establish communications links between their ministries of Defense and Interior. Additionally, the USG should encourage expansion of interagency collaboration among Baltic governments beyond those already in place among the militaries.

3. *Provide Secure and Interoperable Communications Technology.* Support the Baltic states in acquiring communications technology that is secure and interoperable with U.S. and NATO forces and that can survive a Russian attack. This will allow them to communicate with NATO and the U.S. without depending upon the communication capabilities of USSOF or relying on non-secure channels, which is the current capability of the Baltic CF.
4. *Continue Embassy-Sponsored Events in Minority Areas.* The embassies in at risk countries should prioritize programs including English-language classes, cultural events, sponsored trips for Russian-language journalists, and sponsored meetings between U.S. persons and local leaders. Local NGOs are a great partner for these activities. A success story of this type of programming can be seen in the value of meetings between Narva, Estonia, and their "sister city" in the U.S.
5. *Support Social Welfare Programming.* The USG should support development programming in impoverished regions in the Baltic states, many of which have large Russian-speaking minorities. These programs should be implemented through USAID where possible. Additionally, the USG, through the embassies, should work with U.S. companies and the U.S. Trade Representative to find ways to develop business connections between these areas and the U.S. This will further tie the regions to the West and make their residents less vulnerable to Russian media sources and efforts to foment social unrest. There is a great deal of interest in creating entertainment programming aimed at educating populations about national history and identity in these states, particularly in Lithuania. However, they lack the resources to produce the high-quality programming they envision (e.g., a historical drama about the Grand Duchy), which is where American businesses could step in.
6. *Develop Public Resistance to Russian Media Sources.* Support public diplomacy programming oriented toward countering Russian media sources while ensuring that it is tailored to the audience to which it is directed. However, in order to avoid countering Russia at its strength, we do not recommend the creation of a USG-sponsored television station. This station, like ETV+, would be seen as biased and could never compete in terms of financing or programing with Russian television. Instead, we recommend innovative, Internet-based public diplomacy initiatives aimed at these groups, as well as a further increase in funding for Voice of America.
7. *Encourage Alliance Cohesion.* Undertake diplomatic efforts to ensure that U.S. allies, especially those in the NATO alliance, share the American commitment to ensuring the sovereignty of the Baltic states. These actions should specifically target nations that have become closer to Russia in recent years out of necessity and that might cause a divide within NATO's 28 countries were a vote for the invocation of Article 5 against Russia to be called (e.g., Greece following Russian support during the financial crisis). The USG could further support this recommendation by expanding its support to the Transatlantic Capability Enhancement and Training initiative and pushing NATO member countries currently not assisting with the initiative to put their support behind its goals along NATO's eastern border.

United States Special Operations Command

SOF are some of the best-positioned forces to both prevent large-scale hybrid warfare from being waged against the Baltics and increase the ability of the Baltic populations and governments to resist, should a hybrid campaign come. To accomplish this, SOF efforts should be concentrated on supporting the Baltic governments in engaging with ethnic Russian minorities and developing capacity to resist hybrid attacks.

1. *Support Underground Resistance Capabilities.* SOF should encourage the development of an underground network throughout the region to prepare for Russian aggression. The three Baltic states have a tradition of underground, partisan networks that remains incredibly important to them. The legend of the Forest Brothers informs a lot of what the Baltic states believe they can do against a Russian occupation. While the SOF community has already focused on establishing these networks in Lithuania, more can be done in Estonia and Latvia through SOF-on-SOF interactions.
2. *Increase Civil Resistance Capabilities.* Develop a civil resistance capacity within each of the Baltic nations, using the Lithuanian program as a model. Lithuania has released a manual to all of its citizens detailing how to resist in the case of a Russian occupation. All three countries have a recent history of civil resistance, both against the Nazis and against the Soviet Union. They came out of occupation through a civil resistance program. SOF might consider coordination with NGOs (e.g., the International Center on Nonviolent Conflict in the United States) to implement programs on nonviolent resistance in these countries. Additionally, SOF may use their already well-developed connections with Baltic SOF to develop a nonviolent competency within those forces so that they can train members of the government and the civilian population.
3. *Increase Capacity of Ministries of Interior.* SOF teams should spread their engagement to the Ministries of the Interior of the Baltic states, which are currently under-resourced and unprepared for the threat. As these border control and police officers will likely be the first line of defense in a hybrid attack, it is crucial that they are prepared to combat hybrid tactics. Border guards and police should be included in counter–hybrid warfare planning and training. Similarly, SOF should work with the ministries to secure national communications technologies and crisis protocols to allow for effective planning and communication in the event of a crisis.
4. *Continue Baltic SOF Development.* Continue to assist in the development of SOF in Estonia, Latvia, Lithuania, and Poland. There is already a robust relationship between U.S. SOF (USSOF) and those of the Baltic states. Preserving that relationship and continuing the training and capacity building activities already underway should be a priority.
5. *Engage with Local Security Actors Outside of Conventional Militaries.* Each Baltic state has its own volunteer security forces, with varying degrees of training and engagement with Baltic SOF and USSOF. As these forces are embedded in local populations and are therefore likely to have a large role in any resistance movement, USSOF should work with their Baltic counterparts to better integrate these volunteer forces into training and simulation exercises where possible, given proper vetting of these groups.
6. *Strengthen Relationship with Consistent SOF Liaison Staffing.* Having consistent leadership within the USSOF teams in this region both strengthens the relationship between the U.S. and our Baltic allies via personal relationships and increases the command's

understanding of the context shaping the situation in these countries. We recommend that a SOF officer at the O5 rank serve as a regional liaison with the special operations components of these countries' militaries. This officer should be rotated through all three Baltic states over a two-year tour. This regional liaison would be supplemented with permanent liaisons in each Baltic state at the O3 or equivalent level. We saw the effectiveness of this policy in Lithuania and believe that it should be continued and expanded to other countries under threat from Russian hybrid techniques.

7. *Strengthen Relationship through Continued Rotations.* We recommend that USSOCOM continue with the current policy of six-month rotations for SOF teams in each of the Baltic countries. Making the Baltics a location that teams frequently rotate into and out of will deepen the knowledge of individual special operators and allow them to better combat a hybrid threat, which is by nature highly tailored to its target. It will also allow the local SOF components to develop a deep understanding of USSOF procedures and tactics, which will be vital if a hybrid action is implemented by the Russians.
8. *Monitor for Burnout.* The intensity of rotations makes it more likely that host SOF teams will burn out through the continuous rotations, trainings, and exercises. The command must work with the teams and the host country to ensure that these rotations do not burn out the local SOF units.
9. *Increase Local Engagement.* Expand beyond the Joint Combined Exercise Training (JCET) focus in the Baltics to allow SOCEUR Civil Affairs teams to engage in civil-military support element (CMSE)–style missions that could support engagement with the minority populations and improve understandings of local atmospherics. Another way to improve engagement would be to encourage SOCEUR teams to coordinate with the annual schedule of tabletop and other interagency crisis response exercises in order to tailor the presence of JCETs to assisting and learning the required capabilities.

Conclusion

With these recommendations our team has attempted to provide both short-term and long-term activities that many of the actors facing the threat of Russian hybrid warfare could be pursuing. Some recommendations are high-level and others are tactical. We believe that many of these recommendations are already being pursued, either in the public eye or within classified domains, and we believe that those recommendations that are already in action be continued and strengthened. We believe all are important to the overall counter–hybrid warfare campaign and should be evaluated for potential deployment.

Endnotes

[1] Carol Morello, Will Englund, and Griff Witte, "Crimea's Parliament Votes to Join Russia," *Washington Post*, 17 March 2014, accessed 22 November 2015, https://www.washingtonpost.com/world/crimeas-parliament-votes-to-join-russia/2014/03/17/5c3b96ca-adba-11e3-9627-c65021d6d572_story.html.

[2] Steven Myers and Peter Baker, "Putin Recognizes Crimea Secession, Defying the West," *New York Times*, 17 March 2014, accessed 22 November 2015, http://www.nytimes.com/2014/03/18/world/europe/us-imposes-new-sanctions-on-russian-officials.html.

[3] Marie-Louise Gumuchian, Victoria Butenko, and Laura Smith-Spark, "Russia Lawmakers Vote to Annex Crimea; U.S. Steps Up Sanctions," CNN, 21 March 2014, accessed 22 November 2015, http://www.cnn.com/2014/03/20/world/europe/ukraine-crisis/.

[4] "Ukraine: Putin Signs Crimea Annexation," *BBC News*, 21 March 2014, accessed 22 November 2015, http://www.bbc.com/news/world-europe-26686949.

[5] The Russian Federation refers to it as 'non-linear warfare.' Others have called it fourth-generation warfare or compound warfare, although Frank Hoffman, who first used the term 'hybrid warfare,' takes issue with these designations because he believes they are different from his conception of it. Hybrid warfare has also been referred to as hybrid conflict, hybrid techniques, hybrid combat, etc.

[6] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, December 2007), 8, accessed 22 November 2015, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[7] Ibid., 23.

[8] Ibid.

[9] Ibid., 23–24.

[10] Ibid., 24.

[11] Ibid., 17.

[12] Ibid. The quote from General Krulak comes from: Robert Holzer, "Krulak Warns of Over-Reliance on Technology," *Defense News*, October 1996, 7–13.

[13] Ibid., 35. Hoffman had also researched several precursor groups, like the Irish insurgents of the early 1900s, the Mujahedeen in Afghanistan, and the Chechen rebels, but had concluded that these were simply "first generation Hybrid Warriors or the earliest prototypes."

[14] Ibid.

[15] Ibid., 36.

[16] Ibid., 9.

[17] Ibid., 20. For example, Hoffman writes the following about compound wars: "Because it is based on operationally separate forces, the compound concept did not capture the merger or blurring modes of war we had identified in recent case studies or our projections."

[18] Frank Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly*, no. 52, 2009, 34–39. From page 36: "However, despite having its roots in history, modern hybrid war has the potential to transform the strategic calculations of potential belligerents due to the rise of non-state actors, information technology, and the proliferation of advanced weapons systems."

[19] Lieutenant General Riho Terras, chief of defense for Estonia, interview by Andrew Nathaniel Koch, 18 November 2015. Lieutenant General Terras spoke on the record with a member of the Fletcher School team during a meeting prior to his speech to the school's International Security Studies program on 18 November 2015.

[20] Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO," The German Marshall Fund of the United States, 12 February 2015, 2, accessed 22 November 2015, http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato.

[21] Julio Miranda Calha, "Hybrid Warfare: NATO's New Strategic Challenge?" Draft General Report (Brussels, Belgium: NATO Parliamentary Assembly, 7 April 2015), accessed 22 November 2015, http://www.nato-pa.int/default.asp?SHORTCUT=3778.

[22] Ibid.

[23] Michael Kofman and Matthew Rojansky, "Kennan Cable No. 7: A Closer Look at Russia's 'Hybrid War,'" Kennan Institute of the Woodrow Wilson International Center for Scholars, April 2015, accessed 22 November 2015, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

[24] Ibid.

[25] Alex Deep, "Hybrid War: Old Concept, New Techniques," *Small Wars Journal*, 2 March 2015, http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques.

[26] Frank Hoffman, "Hybrid Warfare and Challenges," 36. Hoffman writes specifically about how the techniques and enabling technology of hybrid warfare is what makes hybrid warfare different from other types of warfare, like compound warfare. "These hybrid wars blend the lethality of state conflict with the fanatical and protracted fervor of irregular warfare. In such conflicts, future adversaries (states, state-sponsored groups, or self-funded actors) will exploit access to modern military capabilities, including encrypted command systems, man-portable air-to-surface missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosive devices (IEDs), and coercive assassinations. This could include states blending high-tech capabilities such as antisatellite weapons with terrorism and cyber warfare directed against financial targets."

[27] Daniel Drezner, "Hybrid Warfare, Cyberwarfare, and Covert Action" (lecture, Fletcher School of Law and Diplomacy, Tufts University, Medford, Massachusetts, 9 November 2015).

[28] Ibid.

[29] Ibid.

[30] Steven Pinker and Andrew Mack, "The World Is Not Falling Apart," *Slate*, 22 December 2014, accessed 22 November 2015, http://www.slate.com/articles/news_and_politics/foreigners/2014/12/the_world_is_not_falling_apart_the_trend_lines_reveal_an_increasingly_peaceful.2.html.

[31] Daniel Drezner, "Hybrid Warfare, Cyberwarfare, and Covert Action."

[32] Ibid.

[33] Ibid.

[34] *National Security Act of 1947*, amended 18 December 2015, codified at 50 USC §3093 (e), http://uscode.house.gov/view.xhtml?path=/prelim@title50&edition=prelim.

[35] Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: Congressional Quarterly Press, 2006), 157.

[36] Ibid., 166.

[37] Bruce D. Berkowitz, and Allan E. Goodman, "The Logic of Covert Action," *The National Interest*, Spring 1998, 39; Lowenthal, *Intelligence: From Secrets to Policy*, 162–164.

[38] Lowenthal, *Intelligence: From Secrets to Policy*, 157.

[39] Roy Godson, *Dirty Tricks or Trump Cards* (Washington, D.C.: Brassey's, 1995), 134.

[40] Ibid., 121.

[41] Ibid.

[42] Ibid.

[43] Ibid., 122–123.

[44] Ibid., 123–124.

[45] Ibid., 124.

[46] Ibid., 122.

[47] Ibid.

[48] Ibid., 145.

[49] Ibid., 145–146.

[50] CNN, F. Mark Wyatt interview in *Cold War* "Episode 3: Marshall Plan, 1947–1952," original airing 11 October 1998, https://youtu.be/JQHEMG6zt8I.

[51] Ibid.

[52] Tim Weiner, "F. Mark Wyatt, 86, C.I.A. Officer, Is Dead," *New York Times*, 6 July 2006, accessed 22 November 2015, http://www.nytimes.com/2006/07/06/us/06wyatt.html.

[53] Ibid.

[54] CNN, F. Mark Wyatt interview. Wyatt said: "The communist party of Italy was funded, in the first place, by black bags of money directly out of the Soviet compound in Rome; and the Italian services were aware of this. As the elections approached, the amounts grew, and the estimates [are] that $8 million to $10 million a month actually went into the coffers of communism."

[55] Godson, *Dirty Tricks or Trump Cards*, 147. This advice can be political in nature, as mentioned above, or it could be technical in nature.

[56] Ibid., 135.

[57] Ibid., 136. Godson writes: "In the sixteenth century, ambassadors from Italian city-states…were unable to act covertly. Such circumstance furthered the adoption of a variety of diplomatic agents, ranging from the *mandatario*, usually a man of lesser social status than an ambassador with either a limited or full mandate, to a friend at court (*amico*)…. All of these men could be employed with greater secrecy than an ambassador and with less risk of offense to a susceptible ally." He goes on to add from a modern perspective that. "[a]fter World War II, many CIA chiefs of station in Arab, Latin American, and Asian countries became trusted advisers to foreign leaders…."

[58] Ibid., 135.

[59] Ibid., 139. The term 'seeding' can be used when countries identify "political agents of influence at an early stage and then [act] to advance their careers."

[60] Ibid., 137.

[61] Ibid., 137.

[62] Ibid., 141. "These individuals were sent for training to the USSR, where they were assessed by informants in training school. Upon their return home, Moscow sometimes continued to subsidize individual leaders secretly. Some of those employed by local Communist parties and their labor and media fronts rose to key positions…. Thus, Moscow—'the Center'—set up reliable channels of influence in local Communist parties outside of normal interparty channels, and was often able to dominate the institutions."

[63] Bernard Reich, *Political Leaders of the Contemporary Middle East and North Africa: A Biographical Dictionary* (Westport: Greenwood Press, Inc., 1990), 53.

[64] Ibid., 52.

[65] Serhy Yekelchyk, "The Ukrainian Crisis: In Russia's Long Shadow," *Origins: Current Events in Historical Perspective*, 7, No. 9, June 2014, http://origins.osu.edu/article/ukrainian-crisis-russias-long-shadow/page/0/1.

[66] Ibid.

[67] "Pro-Moscow Yanukovych 'to Win Ukraine Election,'" *BBC News*, 8 February 2010, accessed 22 November 2015, http://news.bbc.co.uk/2/hi/world/europe/8503177.stm.

[68] Luke Harding, "Yanukovych Set to Become President as Observers Say Ukraine Election Was Fair," *The Guardian*, 8 February 2010, accessed 22 November 2015, https://www.theguardian.com/world/2010/feb/08/viktor-yanukovych-ukraine-president-election. While the vote was fair in 2010, according to the Organization for Security and Co-operation in Europe, Yanukovych's actions in the 2012 parliamentary elections were deemed unfair. "Unfair Fight: Ukrainian Election Criticized as Votes Counted," *Spiegel Online*, 29 October 2012, accessed 22 November 2015, http://www.spiegel.de/international/europe/osce-criticizes-ukrainian-election-early-results- show-yanukovich-ahead-a-864085.html.

[69] Yekelchyk, "The Ukrainian Crisis: In Russia's Long Shadow."

[70] "Why Is Ukraine in Turmoil?" *BBC News*, 22 February 2014, accessed 22 November 2015, http://www.bbc.com/news/world-europe-25182823.

[71] Will Englund and Kathy Lally. "Ukraine, Under Pressure from Russia, Puts Brakes on E.U. Deal," *Washington Post*, 21 November 2013, accessed 22 November 2015, https://www.washingtonpost.com/world/europe/ukraine-under-pressure-from-russia-puts-brakes-on-eu-deal/2013/11/21/46c50796-52c9-11e3-9ee6-2580086d8254_story.html. "Russia bullied Ukraine all summer long, with threats, customs slowdowns at the border and sanitation-related sanctions on chocolates and other imports—all of which at the time seemed to strengthen Ukraine's resolve to turn westward to its European neighbors. But more recently, top Russian officials have quietly made it clear that doing so would cost the fragile Ukrainian economy dearly. Ukraine conducts a large part of its trade with Russia, and the consequences of Russian obstruction would be painful. Ukraine has said it could make do without Russian natural gas, but a moratorium on gas purchases that it implemented last week quickly crumbled."

[72] "Russia Maintains Supply Flow to Ukrainian Separatists," Stratfor, 7 November 2014, accessed 22 November 2015, https://www.stratfor.com/analysis/russia-maintains-supply-flow-ukrainian- separatists. In addition to the large supply of weapons and military equipment crossing the border between Russia and Eastern Ukraine, there also has been a significant amount of non-lethal aid. Both amount to financial support to the separatists.

[73] Matthew Weaver and Alec Luhn, "Ukraine Ceasefire Agreed at Belarus Talks," The Guardian, 12 February 2015, accessed 22 November 2015,https://www.theguardian.com/world/2015/feb/12/ukraine-crisis-reports-emerge-of-agreement-in-minsk-talks. Evidence of political and technical advice is harder to find than equipment because it cannot be counted, however there is clear evidence of this advice taking place. At the Minsk peace talks, President Putin clearly was providing the separatists with political advice and eventually pressured the separatists to sign the accord. Roman Olearchyk, "Tensions Ease as Ukraine Rebels Agree to Scrap Election," Financial Times, 6 October 2015, accessed 22 November 2015, https://www.ft.com/content/67a5bc68-6c3e-11e5-aca9-d87542bf8673. Russian political advisors were likely significantly involved in the decision by the separatists not to hold planned elections in October and November, which would have caused major problems with the government in Kiev.

[74] Weaver and Luhn, "Ukraine ceasefire agreed at Belarus talks."

[75] Robert Morgus, "NATO Tries to Define Cyber War," *Real Clear World*, 20 October 2014, accessed 22 November 2015, http://www.realclearworld.com/articles/2014/10/20/nato_tries_to_define_cyber_war_110755.html.

[76] Nuala O'Connor, "Why the OPM Data Breach Is Unlike Any Other," *Center for Democracy & Technology*, 22 June 2015, accessed 22 November 2015, https://cdt.org/blog/why-the-opm-data-breach-is-unlike-any-other/.

[77] David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries –Pentagon," Reuters, June 2013, accessed 22 November 2015, http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619#049F8zHhLpXFH84z.97.

[78] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks," *The Internet Protocol Journal*, 2004, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7- 4/dos_attacks.html.

[79] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 16 May 2007, accessed 22 November 2015, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

[80] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, 19 November 2013, accessed 22 November 2015, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

[81] Morgus, "NATO Tries to Define Cyber War."

[82] Thomas Rid, "Cyberwar and Peace," Foreign Affairs, December 2013, accessed 22 November 2015, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

[83] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S," *New York Times*, 11 October 2012, accessed 22 November 2015, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

[84] House Subcommittee on Technology and Competitiveness of the Committee on Science, Space, and Technology, *Computer Security Hearing*, 102nd Cong., 1st session, 27 June 1991, 10, https://babel.hathitrust.org/cgi/pt?id=pst.000018472172;view=1up;seq=3. While this concept of a 'cyber Pearl Harbor' is often credited to Leon Panetta, it actually dates back even farther to the 1991 testimony to Congress of Winn Schwartau, executive director of the International Partnership Against Computer Terrorism, where he expressed concern about an "electronic Pearl Harbor." More than two decades later, this concern and corresponding analogy still stands and continues to concern government officials and security experts,

[85] Lee Rainie, Janna Anderson, and Jennifer Connolly, *Cyber Attacks Likely to Increase* (Washington, D.C.: Pew Research Center, 29 October 2014), 7, accessed 22 November 2015, http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to- increase/.

[86] NATO, "Wales Summit Declaration," news release, 5 September 2014, accessed 22 November 2015, http://www.nato.int/cps/en/natohq/official_texts_112964.htm. Article 5 (also known as the collective defense clause) of the Washington Treaty, establishing the NATO alliance, states: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

[87] Ibid.

[88] Adrian Chen, "The Agency," *New York Times Magazine*, 7 June 2015, MM57, accessed 22 November 2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[89] Jarno Limnell, "Russia Playing the Long Game in Global Cyberwar Campaign," *International Business Times*, 24 March 2015, accessed 22 November 2015, http://www.ibtimes.co.uk/russia-playing-long-game-global-cyberwar-campaign-1493342.

[90] Andrew Roth, "Russia and China Sign Cooperation Pacts," *New York Times*, 8 May 2015, accessed 22 November 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation- pacts.html.

[91] Patrik Maldre. *Global Connections, Regional Implications: An Overview of the Baltic Cyber Threat Landscape* (Tallinn, Estonia: International Centre for Defence and Security, October 2015).

[92] "VOA History," Voice of America, accessed 22 November 2015, http://www.insidevoa.com/p/5829.html.

[93] Ibid.

[94] Some refer to information operations as influence operations, but we chose to keep the broader phrase information operations to encompass the various aspects of these activities.

[95] RAND Corporation, "Research Topics: Information Operations," accessed 22 November 2015, http://www.rand.org/topics/information-operations.html.

[96] Our example above of the VOA clearly falls into the category of propaganda based on the definitions provided above. Propaganda carries a negative connotation because of its use by authoritarian regimes and bad political actors

around the world. However, generally, the term is good for defining IO-focused dissemination of information designed to deceive or influence.

[97] Harold Lasswell, "Propaganda," in *Propaganda*, ed. Robert Jackall, 13-26 (New York, NY: New York University Press, 1995). Lasswell states that the history of propaganda goes back millennia: "The walls of Pompeii were found to be covered with election appeals. Frederick the Great was ever anxious to influence European public opinion. Napoleon subsidized a London newspaper, Metternich and the Rothschilds employed Friedrich von Gentz and Bismarck used Moritz Busch to spread favorable press comment. In the American Revolution committees of correspondence fostered anti-English sentiment."

[98] Ibid.

[99] Lowenthal, *Intelligence: From Secrets to Policy*, 162.

[100] Tom Dreisbach, "Germany to Close Last American Cold War Era Cultural House," *PRI's The World*, 13 September 2011 accessed 22 November 2015, http://www.pri.org/stories/2011-09-13/germany-close-last-american-cold-war-era-cultural-house. During the Cold War, the United States established "Amerika Hauses" throughout Germany to teach Germans and other Europeans about culture and life in the United States and to counter the spread of communism.

[101] Office of Information Resources, "American Corners - Quick Info for Partners," United States Department of State, accessed 22 November 2015, http://photos.state.gov/libraries/171414/acworkshop/0920-handout-AC-Quick-Info-Sheet-Partners.pdf. United States embassies around the world have established official information centers called American corners.

[102] Godson, *Dirty Tricks or Trump Cards*, 151.

[103] Ibid.

[104] Ibid., 154. Godson makes the point that: "The black propagandist, unlike the gray, takes extreme care to cover his tracks, making it difficult for any foreign intelligence service to identify him with a particular project."

[105] Ibid., 152. Godson says, "Gray propaganda hides its source from the uninitiated public, but not from sophisticated observers."

[106] Ibid., 151.

[107] Ibid.

[108] Ibid., 155.

[109] Hoffman, *Conflict in the 21st Century*, 38.

[110] Marvin Kalb and Carol Saivetz, *The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict* (Washington, D.C.: The Brookings Institution, 2007), https://www.brookings.edu/wp-content/uploads/2012/04/2007islamforum_israel-hezb-war.pdf.

[111] Hoffman, *Conflict in the 21st Century*, 38.

[112] United States Joint Chiefs of Staff, *Joint Publication 3-13.1, Electronic Warfare*, 25 January 2007, 1–2.

[113] Ibid., 1–3.

[114] Ibid.

[115] Ryskeldi Satke, "Russian Intelligence in Kyrgyzstan, Cold War Redux," *The Diplomat*, 7 December 2014., accessed 22 November 2015, http://thediplomat.com/2014/12/russian-intelligence-in-kyrgyzstan-cold-war-redux/.

[116] Andrew E. Kramer, "Before Kyrgyz Uprising, Dose of Russian Soft Power," *New York Times*, 18 April 2010, accessed 22 November 2015, http://www.nytimes.com/2010/04/19/world/asia/19kyrgyz.html?_r=1.

[117] Ibid.

[118] Ibid. In fact, according to the *New York Times*: "In March, Roza Otunbayeva, now the head of the interim government traveled to Moscow to attend a conference of former Soviet political parties and to meet Sergei M.

Mironov, speaker of the upper chamber of the Russian Parliament and a close ally of Prime Minister Vladimir V. Putin."

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] John Vandiver, "SACEUR: Allies Must Prepare for Russia 'Hybrid War,'" *Stars and Stripes*, 4 September 2014, accessed 22 November 2015, http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

[124] United States Joint Chiefs of Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 February 2016), 50.

[125] United States Joint Chiefs of Staff, *Joint Publication 1-02*, 221.

[126] Lowenthal, *Intelligence: From Secrets to Policy*, 163–164.

[127] United States Joint Chiefs of Staff, *Joint Publication 1-02*, 221.

[128] Capt Gregory Ball, "Operation Eagle Claw," Air Force Historical Support Division, 8 October 2015, accessed 22 November 2015, http://www.afhistory.af.mil/FAQs/FactSheets/tabid/3323/Article/458949/operation-eagle-claw.aspx. Operation Eagle Claw was a joint operation prepared by the U.S. military to recover the hostages taken by the Iranian regime during the storming of the U.S. Embassy in Tehran. The operation ended in tragedy when a helicopter collided with an EC-130 that was full of fuel. Both the helicopter and the aircraft exploded, killing eight personnel. While the operation had previously been aborted because of mechanical issues, the exploration and the subsequent abandoning of the other equipment led to the mission being found out by the Iranian regime and, thus, the world. This was a huge blow to Carter and made the U.S. military appear incompetent.

[129] Lowenthal, *Intelligence: From Secrets to Policy*, 163.

[130] Ibid.

[131] United States Joint Chiefs of Staff, *Joint Publication 1-02*, 249.

[132] Lowenthal, *Intelligence: From Secrets to Policy*, 163.

[133] Ibid.

[134] Ibid.

[135] *Antiterrorism Act of 1990*, 18 U.S. Code § 2331, accessed 22 November 2015, https://www.law.cornell.edu/uscode/text/18/2331.

[136] Godson, *Dirty Tricks or Trump Cards*, 161.

[137] Mark Wheelis, "Biological Warfare at the 1346 Siege of Caffa," *Emerging Infectious Diseases*, 8, no. 9 (September 2002): 971–975, http://wwwnc.cdc.gov/eid/article/8/9/01-0536_article. In 1346, the Crimean city of Caffa was brought under siege by an invading Mongol army. During the siege, "the Mongol army hurled plague-infected cadavers into the besieged Crimean city of Caffa." This was a clear use of terrorism by the Mongols against the people of Caffa. Incidentally, it was perhaps also the first use of biological warfare. According to accounts, the cadavers "thereby transmit[ed] the disease to the inhabitants [causing] fleeing survivors of the siege [to] spread plague from Caffa to the Mediterranean Basin."

[138] "FLASHBACK: April 18, 1983: U.S. Embassy Attacked in Beirut," Central Intelligence Agency, News & Information, modified 10 July 2014, accessed 22 November 2015, https://www.cia.gov/news-information/featured-story-archive/2014-featured-story-archive/flashback-april-18-1983-u-s-embassy-bombed-in-beirut.html.

[139] Ibid.

[140] CNN Library, "Beirut Marine Barracks Bombing Fast Facts," CNN, 19 October 2015, accessed 22 November 2015, http://www.cnn.com/2013/06/13/world/meast/beirut-marine-barracks-bombing-fast-facts/.

[141] Alan Cullison and Andrey Ostroukh, "Russia Plans Deep Budget Cuts as Revenues Drop," *Wall Street Journal*, 14 January 2015, accessed 22 November 2015, http://www.wsj.com/articles/russia-facing-budget-cuts-on-oil-price-western-sanctions-1421223776?alg=y.

[142] "Russia Targets NATO With Military Exercises," Stratfor, 19 March 2015, accessed 22 November 2015, https://www.stratfor.com/analysis/russia-targets-nato-military-exercises.

[143] "MH17 Ukraine Plane Crash: What We Know," *BBC News*, 14 October 2015, accessed 22 November 2015, http://www.bbc.com/news/world-europe-28357880.

[144] Ibid.

[145] Office of the Historian, Bureau of Public Affairs, "Mahan's The Influence of Sea Power upon History: Securing International Markets in the 1890s," U.S. Department of State, accessed 22 November 2015, https://history.state.gov/milestones/1866-1898/mahan.

[146] David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *New York Times*, 25 October 2015, accessed 22 November 2015, http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0.

[147] Reuters, "Russia Will Add 80 New Warships To Black Sea Fleet," *Business Insider*, 23 September 2014, accessed 22 November 2015, http://www.businessinsider.com/r-russia-will-add-80-new-warships-to-black-sea-fleet-fleet-commander-2014-9.

[148] Christoper P. Cavas, "US: Russia Building 'Arc Of Steel' From Arctic To Med," *Defense News*, 6 October 2015, accessed 22 November 2015, http://www.defensenews.com/story/defense/naval/2015/10/06/russia-military-naval-power-shipbuilding-submarine-warships-baltic-mediterranean-black-sea-arctic-syria-estonia-latvia-lithuania-crimea-ukraine/73480280/.

[149] Jim Garamone, "NATO Leader Says Russia Building 'Arc of Steel' in Europe," DOD News, U.S. Department of Defense, 6 October 2015, accessed 22 November 2015, http://www.defense.gov/News-Article-View/Article/622080/nato-leader-says-russia-building-arc-of-steel-in-europe.

[150] Andrew E. Kramer, "Russian Warships Said to Be Going to Naval Base in Syria," *New York Times*, 18 June 2012, accessed 22 November 2015, http://www.nytimes.com/2012/06/19/world/europe/russian-warships-said-to-be-going-to-naval-base-in-syria.html?_r=1.

[151] Trude Pettersen, "Arctic Training for Strategic Nuclear Submarines," *Barents Observer*, 30 July 2015, accessed 22 November 2015, http://barentsobserver.com/en/security/2015/07/arctic-training-strategic-nuclear-submarines-30-07.

[152] Kristine Brunmark, "Frykter Russisk Hybridkrig Mot Norge," *ABC Nyheter*, 11 February 2015, accessed 22 November 2015, http://www.abcnyheter.no/nyheter/2015/02/11/217651/frykter-russisk-hybridkrig-mot-norge.

[153] "Russia Submarine Capabilities," Nuclear Threat Initiative, 10 June 2014, accessed 22 November 2015, http://www.nti.org/analysis/articles/russia-submarine-capabilities/.

[154] "Russia Reveals Giant Nuclear Torpedo in State TV 'Leak,'" *BBC News*, 12 November 2015, accessed 22 November 2015, http://www.bbc.com/news/world-europe-34797252.

[155] Jeffrey Lewis, "US Concerned About Russian Submarines with Nuclear Armed Cruise Missiles Near Washington," *Atlantic Council: NATOSource* blog, 6 January 2015, accessed 22 November 2015, http://www.atlanticcouncil.org/blogs/natosource/us-concerned-about-russian-submarines-with-nuclear-armed-cruise-missiles-near-washington.

[156] Garamone, "NATO Leader Says Russia Building 'Arc of Steel' in Europe."

[157] Ibid.

[158] Stephen J. Blank, "Imperial Ambitions: Russia's Military Buildup," *World Affairs*, May/June 2015, accessed 22 November 2015, http://www.worldaffairsjournal.org/article/imperial-ambitions-russia%E2%80%99s-military-buildup.

[159] Sanger and Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort."

[160] Ibid.

[161] Richard Weitz, "Hybrid Power: The Limits of Russia's Military Resurgence," *World Politics Review*, 7 April 2015, accessed 22 November 2015, http://www.worldpoliticsreview.com/articles/15470/hybrid-power-the-limits-of-russia-s-military-resurgence

[162] BertilDunér, 1981. "Proxy Intervention in Civil Wars," *Journal of Peace Research* 18, no. 4 (1981): 353–61, http://www.jstor.org/stable/423538.

[163] Michael Graham Fry, Erik Goldstein, and Richard Langhorne, eds., *Guide to International Relations and Diplomacy* (New York, NY: Bloomsbury Continuum, 2004), 9.

[164] Mark Galeotti, "An Unusual Friendship: Bikers and the Kremlin (Op-Ed)," *Moscow Times*, 19 May 2015, accessed 22 November 2015. http://www.themoscowtimes.com/opinion/article/an-unusual-friendship-bikers-and-the-kremlin-op-ed/521763.html.

[165] Ibid.

[166] "Russia's Night Wolves Wrap Up Epic WWII Victory Ride to Berlin," Sputnik, 9 May 2015, accessed 22 November 2015. http://sputniknews.com/europe/20150509/1021920453.html.

[167] Valery Gerasimov, "The Value of Science in Anticipation" (translated from orginial Russian), *BNK*, 27 February 2013, accessed 22 November 2015, http://www.vpk-news.ru/articles/14632.

[168] Charles Krauthammer, "Democratic Realism," *American Enterprise Institute*, 10 February 2004, accessed 22 November 2015, https://www.aei.org/publication/democratic-realism/.

[169] Bradley S. Klein, "Hegemony and Strategic Culture: American Power Projection and Alliance Defence Politics," *Review of International Studies* 14, no. 2 (April 1988): 133–148, http://www.jstor.org/stable/20097137.

[170] Klein, "Hegemony and Strategic Culture."

[171] Stephen Blank, "After Afghanistan: Reassessing Soviet Capabilities and Policies for Power Projection," *Comparative Strategy* 9, no. 2 (1990): 117–136, http://dx.doi.org/10.1080/01495939008402804.

[172] Klein, "Hegemony and Strategic Culture."

[173] Cullison and Ostroukh, "Russia Plans Deep Budget Cuts as Revenues Drop."

[174] Dmitry Gorenburg and Ryan Evans, "The State of Russian Strategy: Ukraine, Syria, and Beyond," *War on the Rocks*, 22 September 2015, accessed 22 November 2015, http://warontherocks.com/2015/09/the-state-of-russian-strategy-ukraine-syria-and-beyond/.

[175] "Russia Reveals Giant Nuclear Torpedo in State TV 'Leak,'" *BBC News*.

[176] Matthew Bodner, "Russia's Bombers Over Europe Are Scary, But Not in the Way You Think," *Moscow Times*, 3 April 2015, accessed 22 November 2015, http://www.themoscowtimes.com/business/article/russia-s-bombers-over-europe-are-scary-but-not-in-the-way-you-think/518600.html.

[177] "Russia Reveals Giant Nuclear Torpedo in State TV 'Leak,'" *BBC News*.

[178] Matthew Bodner, "Russia's Bombers Over Europe Are Scary."

[179] Cullison and Ostroukh, "Russia Plans Deep Budget Cuts as Revenues Drop."

[180] Tor Egil Førland, "'Economic Warfare' and 'Strategic Goods': A Conceptual Framework for Analyzing COCOM," *Journal of Peace Research* 28, no. 2 (1 May 1991): 192–194, http://www.jstor.org/stable/424388.

[181] Ibid., 193.

[182] Ibid., 191–194.; Lowell M. Pumphrey, "Economic Warfare Tactics," *Military Affairs* 6, no. 1 (Spring 1942): 8–9, http://www.jstor.org/stable/1983173.

[183] Tor Egil Førland, "The History of Economic Warfare: International Law, Effectiveness, Strategies," *Journal of Peace Research* 30, no. 2 (1 May 1993): 156–157, http://www.jstor.org/stable/425196.

[184] Lowenthal, *Intelligence: From Secrets to Policy*, 162–163.

[185] "Iran Sanctions: Joint Comprehensive Plan of Action," U.S. Department of State, accessed 22 November 2015, http://www.state.gov/e/eb/tfs/spi/iran/jcpoa/.

[186] Førland, "The History of Economic Warfare," 158–159.

[187] Pumphrey, "Economic Warfare Tactics," 8.

[188] Førland, "'Economic Warfare' and 'Strategic Goods,'" 192.

[189] Paul Sonne and Anton Troianovski, "Russia Bans Food Imports in Retaliation for Western Sanctions," *Wall Street Journal*, 7 August 2014, accessed 22 November 2015, http://www.wsj.com/articles/russia-bans-food-imports-in-retaliation-to-western-sanctions-1407403035?alg=y.

[190] "Russia Destroys Tonnes of Foreign Food Imports," *BBC News*, 6 August 2015, accessed 22 November 2015, http://www.bbc.com/news/business-33814362.

[191] Sonne and Troianovski, "Russia Bans Food Imports in Retaliation for Western Sanctions."

[192] "Russia Destroys Tonnes of Foreign Food Imports," *BBC News*.

[193] Lieutenant General Riho Terras, interview by Andrew Nathaniel Koch. During an interview, LTG Terras emphasized efforts that the Estonians have made to reduce their economic dependence on Russia. These include creating an electricity link between Estonia, Sweden, and Finland, as well as working to create a liquefied natural gas import facility. The General acknowledged that Estonia is currently reliant on Russian natural gas imports, but emphasized that, because of Estonian efforts, natural gas only accounts for 6% of Estonian energy needs.

[194]. "Baltic States Join Forces to Resist Russia," *Jane's Intelligence Review*, February 2015, 28–33.

[195] "Pipe Dreams—Europe Wrestles with Russian Energy Dependency," *Jane's Intelligence Review*, 2014.

[196] Ibid.

[197] Andrew Hess, "Turkey and the Geopolitics of Eurasian Energy Exports" (lecture, The Fletcher School of Law and Diplomacy, Tufts University, Medford, MA, 24 September 2015).

[198] "Baltic States Join Forces to Resist Russia," *Jane's Intelligence Review*.

[199] James Sherr, *Hard Diplomacy and Soft Coercion: Russia's Influence Abroad* (London: Chatham House, 2013).

[200] Lieutenant Commander Cindy Hurst, U.S. Navy Reserve, "The Militarization of Gazprom," *Military Review* 90, no. 5 (September/October 2010): 59–67.

[201] Adam Stulberg, *Well-Oiled Diplomacy: Strategic Manipulation and Russia's Energy Statecraft in Eurasia* (Albany: State University of New York Press, 2007).

[202] Kristina Peterson, "Congressional Republicans Signal Deep Resistance to Iran Nuclear Deal," *Wall Street Journal*, 14 July 2015, accessed 22 November 2015, http://www.wsj.com/articles/iran-deal-faces-u-s-lawmakers-scrutiny-1436868209.

[203] Daniel Drezner, "Will Congress Approve the Trans-Pacific Partnership?" *Washington Post*, 6 October 2015, accessed 22 November 2015, https://www.washingtonpost.com/posteverything/wp/2015/10/06/will-congress-approve-the-trans-pacific-partnership/.

[204] Michelle Kosinski, "Inside the Obama-Putin Power Huddle," CNN, 16 November 2015, accessed 22 November 2015, http://www.cnn.com/2015/11/15/politics/obama-putin-g20-meeting/.

[205] Charles J. Dunlap, Jr., "Lawfare: A Decisive Element of 21st-Centry Conflicts," *Joint Forces Quarterly* 54 (July 2009): 34–39, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=6034&context=faculty_scholarship.

[206] Ibid.

[207] Ibid.

[208] Andru E. Wall, "Was the 2003 Invasion of Iraq Legal?" *International Law Studies* 86 (2010): 69–80, http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1097&context=ils.

[209] Jonathan Cook, "'Lawfare', Israel's Continuation of War by Other Means," Global Research, 17 April 2015, accessed 22 November 2015, http://www.globalresearch.ca/lawfare-israels-continuation-of-war-by-other-means/5443491.

[210] Valerie Pacer, "Vladimir Putin's Justification for Russian Action in Crimea Undermines His Previous Arguments Over Syria, Libya and Iraq," The London School of Economics and Political Science, 11 March 2014, accessed 22 November 2015, http://blogs.lse.ac.uk/europpblog/2014/03/11/vladimir-putins-justification-for-russian-action-in-crimea-undermines-his-previous-arguments-over-syria-libya-and-iraq/.

[211] Jasper Eitze and Michael Gleichmann, "Ten Myths Used to Justify Russian Policy in the Ukraine Crisis," *Facts & Findings* 149 (May 2014): 1–7, http://www.kas.de/wf/doc/kas_37844-544-2-30.pdf?140612145651. The Ukraine case study is explained in further detail later in this report. The Ten Myths listed in this article are as follows: 1. The West has meddled in Ukraine's internal affairs, organised and orchestrated the Euromaidan protests with the help of fascist groups; 2. The transitional government in Kiev came to power through a coup and therefore has no legitimacy; 3. The transitional government in Kiev and fascist groups discriminate and threaten ethnic Russians who mostly live in southern and eastern Ukraine; 4. The armed separatists in the south and east of Ukraine are self-defence forces of the Russian-descent population in that region, the majority of whom hope to become a part of the Russian Federation; 5. The government in Kiev is waging a war against its own people by deploying the military in the east of the country and is repressing peaceful protests; 6. Due to their common history and ethno-cultural ties, Ukraine is under Russia's natural sphere of influence and therefore has limited sovereignty; 7.The self-determination of the people and the referenda held legitimise the secession and accession of Crimea and other regions in the Russian Federation; 8. The West is using double standards with the secession of Crimea because of what it did in the case of Kosovo's independence; 9. The West has pursued a systematic policy of exclusion and weakening of Russia since the fall of the Soviet Union; 10. Despite previous assurances, NATO has expanded into the former Soviet region, seeks the inclusion of Ukraine and, in doing so, affects Russian security interests.

[212] Ibid.

[213] Ibid.

[214] Peter Roudik, "Russian Federation: Legal Aspects of War in Georgia," Law Library of Congress, August 2008, accessed 22 November 2015, http://www.loc.gov/law/help/russian-georgia-war.php.

[215] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND Corporation, 2001).

[216] Ibid.

[217] Jen Wieczner, "Report: Russians Hacked Dow Jones for Stock Tips," *Fortune*, 16 October 2015, accessed 22 November 2015, http://fortune.com/2015/10/16/report-russians-hacked-dow-jones-for-stock-tips/. In this attack, Russian hackers gained access to the Dow Jones system (which owns several major financial news sources, including the *Wall Street Journal*), to gain insider trading information before it was published. It is as yet unclear whether the hackers were able to make any money from this operation.

[218] Arquilla and Ronfeldt, *Networks and Netwars*, 6.

[219] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* blog, 6 July 2014, accessed 22 November 2015, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[220] Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *World Post*, 2 November 2014, accessed 22 November 2015, http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

[221] Arquilla and Ronfeldt, *Networks and Netwars*.

[222] "Timeline: Ukraine's Political Crisis," Al Jazeera, 20 September 2014, accessed 30 January 2016, http://www.aljazeera.com/news/europe/2014/03/timeline-ukraine-political-crisis-201431143722854652.html.

[223] Ibid.

[224] Ibid.

[225] Ibid..

[226] Ibid.

[227] Ibid.

[228] Ibid.

[229] Ibid.

[230] Ibid.

[231] Ibid.

[232] Ibid.

[233] Fred Weir, "Russia's Naval Base in Ukraine: Critical Asset or Point of Pride?" *Christian Science Monitor*, 27 February 2014, accessed 20 February 2016, http://www.csmonitor.com/World/Security-Watch/2014/0227/Russia-s-naval-base-in-Ukraine-Critical-asset-or-point-of-pride.

[234] "Timeline: Ukraine's Political Crisis," Al Jazeera.

[235] Ibid.

[236] Ibid.

[237] Ibid.

[238] Ibid.

[239] Ibid.

[240] It is important to note that Crimea operated as a semi-autonomous region of Ukraine with its own parliament and government functions. However, Kiev maintained overall control over the peninsula.

[241] "The Ukraine Crisis Timeline," Center for Strategic and International Studies, accessed 30 January 2016, http://ukraine.csis.org/crimea.htm. However, many Crimean politicians called into question the legitimacy of the vote because some parliamentarians were barred from voting.

[242] Ibid.

[243] Ibid.

[244] Ibid.

[245] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, D.C.: Institute for the Study of War, September 2015), 13, http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

[246] Ibid., 7.

[247] Referring to Ukrainian pro-Nazi World War II independence movement leader Stepan Bandera.

[248] Dunlap, Jr., "Lawfare: A Decisive Element of 21st-Century Conflicts."

[249] Jean-Dominique Giuliani, "Russia, Ukraine and International Law," *Fondation Robert Schuman* 344 (17 February 2015), accessed 30 January 2016, http://www.robert-schuman.eu/en/doc/questions-d-europe/qe-344-en.pdf.

[250] Ilya Somin, "Why the Kosovo 'Precedent' Does Not Justify Russia's Annexation of Crimea," *Washington Post*, 24 March 2014, accessed 30 January 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/03/24/crimea-kosovo-and-false-moral-equivalency/.

[251] Lukas I. Alpert, "5 Reasons Putin Gave for Annexing Crimea," *Wall Street Journal*, 18 March 2014, accessed 30 January 2016, http://blogs.wsj.com/briefly/2014/03/18/5-reasons-vladimir-putin-gave-for-annexing-crimea/.

[252] Ibid.

[253] "Russia Turns the Screws on Ukraine with Gas Supply Threat," *Time*, 8 March 2014, accessed 30 January 2016, http://time.com/16915/russia-turns-the-screws-on-ukraine-with-gas-supply-threat/.

[254] Simon Shuster, "Putin's Man in Crimea Is Ukraine's Worst Nightmare," *Time*, 10 March 2014, accessed 30 January 2016, http://time.com/19097/putin-crimea-russia-ukraine-aksyonov/.

[255] Ibid.

[256] Ibid.

[257] Ibid.

[258] Ibid.

[259] Ibid.

[260] Ibid.

[261] Steven Rosenberg, "Ukraine Crisis: Meeting the Little Green Men," *BBC News*, 30 April 2014, accessed 30 January 2016, http://www.bbc.com/news/world-europe-27231649.

[262] Ibid.

[263] Ibid..

[264] Steven Pifer, "Op-Ed: Watch Out for Little Green Men," Brookings Institution, 7 July 2014, accessed 30 January 2016, http://www.brookings.edu/research/opinions/2014/07/07-watch-out-little-green-men-pifer.

[265] "Timeline: Ukraine's Political Crisis," Al Jazeera.

[266] Ibid.

[267] "Ukraine Accuses Russia of Invading Crimea," Al Jazeera, 28 February 2014, accessed 30 January 2016, http://www.aljazeera.com/news/europe/2014/02/ukraine-accuses-russia-invading-crimea-201422820136126248.html.

[268] Dalton Bennett and David McHugh. "Putin Moves Russian Troops Into Crimea," *Huffington Post*, 1 March 2014, accessed 30 January 2016, http://www.huffingtonpost.com/2014/03/01/putin-russian-troops-crimea_n_4880076.html. Don Mackay and Nick Sommerlad, "Russia Invades Crimea to 'Protect Its Black Sea Naval Fleet' as Ukraine Tensions Soar," *Daily Mirror*, 1 March 2014, accessed 30 January 2016, http://www.mirror.co.uk/news/world-news/ukraine-news-russia-invades-crimea-3194129.

[269] "Russian Troops Storm Crimea Airbase," Al Jazeera, 22 March 2014, accessed 30 January 2016, http://www.aljazeera.com/news/europe/2014/03/russian-troops-enter-crimea-airbase-2014322152544870658.html.

[270] "Russia Turns the Screws on Ukraine with Gas Supply Threat," *Time*.

[271] Jeffrey Tayler, "Russia Raises Natural Gas Threat Against Ukraine," *National Geographic*, 3 March 2014, accessed 30 January 2016, http://news.nationalgeographic.com/news/energy/2014/03/140303-russia-natural-gas-threat-against-ukraine/.

[272] "Ukraine Accuses Russia of Invading Crimea," Al Jazeera.

[273] Shaun Walker, Harriet Salem, and Ewen MacAskill, "Russian 'Invasion' of Crimea Fuels Fear of Ukraine Conflict," *The Guardian*, 28 February 2014, accessed 30 January 2016, http://www.theguardian.com/world/2014/feb/28/russia-crimea-white-house.

[274] Matt Smith and Alla Eshchenko, "Ukraine Cries 'Robbery' as Russia Annexes Crimea," CNN, 18 March 2014, accessed 30 January 2016, http://www.cnn.com/2014/03/18/world/europe/ukraine-crisis/.

[275] Maksym Bugriy, "Economic Warfare in the Russian-Ukrainian Conflict: Crimea," *Eurasia Daily Monitor*, 3 November 2014, accessed 30 January 2016, https://jamestown.org/program/economic-warfare-in-the-russian-ukrainian-conflict-crimea/.

[276] Ibid.

[277] Ibid.

[278] Ibid.

[279] "Timeline: Ukraine's Political Crisis," Al Jazeera.

[280] Javier Jarrin, "International Response to Annexation of Crimea," *EuroMaidan Press*, 24 March 2014, accessed 30 January 2016, http://euromaidanpress.com/2014/03/24/international-response-to-annexation-of-crimea/#arvlbdata.

[281] European External Action Service, "EU Sanctions Against Russia Over Ukraine Crisis," *EU Newsroom*, accessed 20 February 2016, http://europa.eu/newsroom/highlights/special-coverage/eu_sanctions/index_en.htm#5.

[282] Christian Oliver, James Fontanella-Khan, George Parker, and Stefan Wagstyl, "EU Sanctions Push on Russia Falters Amid Big Business Lobbying," *Financial Times*, 16 April 2014, accessed 20 February 2016, http://www.ft.com/intl/cms/s/0/352f4f5c-c57c-11e3-97e4-00144feabdc0.html?siteedition=uk#slide0.

[283] European Commission Public Affairs, "European Commission's Support to Ukraine," news release, 5 March 2014, accessed 20 February 2016, http://europa.eu/rapid/press-release_MEMO-14-159_en.htm.

[284] Ibid. European Commission Public Affairs, "An 'Economic Life-Line for Ukraine': Temporary Tariff Cuts for Ukrainian Exports to the EU," press release, 11 March 2014, accessed 20 February 2016, http://europa.eu/rapid/press-release_STATEMENT-14-63_en.htm.

[285] "Sixes and Sevens," *The Economist*, 8 March 2014, accessed 30 January 2016, http://www.economist.com/news/briefing/21598743-europe-and-america-are-outraged-annexation-crimea-lack-strong-response-sixes.

[286] In many ways, the Russian companies are just as reliant on the strong German customer base in order to have a reliable customer for the long term. Anna Kwiatkowska-Drożdż and Konrad Poplawski, "The German Reaction to the Russian-Ukrainian Conflict – Shock and Disbelief," Centre for Eastern Studies, 3 April 2014, accessed 30 January 2016. http://www.osw.waw.pl/en/publikacje/osw-commentary/2014-04-03/german-reaction-to-russian-ukrainian-conflict-shock-and.

[287] "Sixes and Sevens," *The Economist*.

[288] Henry Chu, "Crimea Crisis Highlights Germany's Aversion to Being in the Vanguard," *Los Angeles Times*, 2 April 2014, accessed 30 January 2016, http://articles.latimes.com/2014/apr/02/world/la-fg-germany-ukraine-20140402.

[289] Ulrich Speck, "German Power and the Ukraine Conflict," Carnegie Europe, 26 March 2015, accessed 30 January 2016, http://carnegieeurope.eu/2015/03/26/german-power-and-ukraine-conflict.

[290] Ibid.

[291] Smith and Eshchenko, "Ukraine Cries 'Robbery' as Russia Annexes Crimea."

[292] Ibid.

[293] Carl Schreck, "U.S. Takes Off the Gloves in Rhetorical Rumble with Russia," *Radio Free Europe*, 15 April 2014, accessed 30 January 2016, http://www.rferl.org/content/us-russia-rhetorical-rumble-ukraine/25333785.html.

[294] Ibid.

[295] Dan Roberts and Ian Traynor, "US and EU Impose Sanctions and Warn Russia to Relent in Ukraine Standoff," *The Guardian*, 6 March 2014. accessed 30 January 2016, http://www.theguardian.com/world/2014/mar/06/us-eu-sanctions-obama-russia-ukraine-crimea.

[296] Ibid.

[297] "Sixes and Sevens," *The Economist*.

[298] Ibid.

[299] "Ukraine Asks to Join NATO Membership Action Plan." UNIAN, 16 January 2008, accessed 30 January 2016, http://www.unian.info/world/89447-ukraine-asks-to-join-nato-membership-action-plan.html.

[300] NATO, "NATO Secretary General Condemns Moves to Incorporate Crimea into Russian Federation," press release, 18 March 2014, accessed 30 January 2016, http://www.nato.int/cps/en/natolive/news_108100.htm?selectedLocale=en.

[301] Kurt Volker, "Where's NATO's Strong Response to Russia's Invasion of Crimea?" *Foreign Policy*, 18 March 2014, accessed 30 January 2016, http://foreignpolicy.com/2014/03/18/wheres-natos-strong-response-to-russias-invasion-of-crimea/.

[302] "Timeline: Ukraine's Political Crisis," Al Jazeera.

[303] Ibid.

[304] Ibid.

[305] We hesitate to use international law, since many question the validity of international law, however we do believe that there are particular international legal norms that are universal—or near universal—that the UN would be citing in their resolution against the Crimean annexation.

[306] Raymond W. Leonard, *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918–1933* (Westport, CT: Praeger, 1999).

[307] Toivo U. Raun, *Estonia and the Estonians: Second Edition* (Stanford, CA: Hoover Institution Press, 2002).

[308] Toivo Miljan, *Historical Dictionary of Estonia* (Lanham, MD: Scarecrow Press, 2004).

[309] *Estonica: Encyclopedia about Estonia*, "An Attempted Communist Coup D'état on 1 December 1924," http://www.estonica.org/en/An_attempted_Communist_coup_d%E2%80%99%C3%A9tat_on_1_December_1924/ (accessed 20 February 2016).

[310] Ibid.

[311] Toivo Miljan, *Historical Dictionary of Estonia*.

[312] *Estonica: Encyclopedia about Estonia*, "Defence League," http://www.estonica.org/en/Defence_League/ (accessed 20 February 2016.)

[313] "Estonia" in *Freedom on the Net* 2015, Freedom House, accessed 20 February 2016, https://freedomhouse.org/report/freedom-net/2015/estonia.

[314] A.A.K.,. "How Did Estonia Become a Leader in Technology?" *The Economist*, 30 July 2013, accessed 20 February 2016, http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21.

[315] Patrick Kingsley, "How Tiny Estonia Stepped Out of USSR's Shadow to Become an Internet Titan," *The Guardian*, 15 April 2012, accessed 20 February 2016, http://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan.

[316] A.A.K.,. "How Did Estonia Become a Leader in Technology?"

[317] "Estonia Claims New E-Voting First," *BBC News*, 1 March 2007, accessed 20 February 2016, http://news.bbc.co.uk/2/hi/europe/6407269.stm.

[318] Kingsley, "How Tiny Estonia Stepped Out of USSR's Shadow."

[319] Ibid.

[320] Ibid.

[321] Urmas Loit and Andra Siibak, *Mapping Digital Media: Estonia* (New York, NY: Open Society Foundations, April 2013).

[322] Ibid.

[323] Steven Lee Myers, "Russia Rebukes Estonia for Moving Soviet Statue," *New York Times*, 27 April 2007, accessed 20 February 2016, http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html?_r=1.

[324] Ibid.

[325] Ibid.

[326] Christopher Fitzgerald Wrenn, "Strategic Cyber Deterrence" (Ph.D. Diss., The Fletcher School of Law and Diplomacy, Tufts University, July 2012), 176–238.

[327] Ibid.

[328] Ibid.

[329] Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1-2, Winter/Spring 2008, accessed 20 February 2016, http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

[330] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, 19 May 2007, accessed 20 February 2016, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

[331] R. Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," (Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, UK, July 2008), 163–168, accessed 20 February 2016, https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html.

[332] Christopher Rhoads, "Cyber Attack Vexes Estonia, Poses Debate," *Wall Street Journal*, 18 May 2007, accessed 20 February 2016, http://www.wsj.com/articles/SB117944513189906904.

[333] Ibid.

[334] Thilek, "Estonia Cyber Attacks 2007," 28 December 2009, accessed 20 February 2016, http://meeting.afrinic.net/afrinic- 11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

[335] Wrenn, "Strategic Cyber Deterrence."

[336] Ruus, "Cyber War I."

[337] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia."

[338] Jose Nazario, "Estonian DDoS Attacks – A Summary to Date," *Arbor Networks*, 17 May 2007, accessed 20 February 2016, http://www.arbornetworks.com/blog/asert/estonian-ddos-attacks-a-summary-to-date/.

[339] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review* XVIII, no. 1 (Spring 2009), accessed 20 February 2016, http://www.iar-gwu.org/node/65.

[340] Ibid.

[341] Ibid.

[342] Wrenn, "Strategic Cyber Deterrence."

[343] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007, accessed 20 Feburary 2016, http://www.wired.com/2007/08/ff-estonia/.

[344] Wrenn, "Strategic Cyber Deterrence."

[345] Ibid.

[346] Ibid.

[347] Richards, "Denial-of-Service."

[348] "Estonian Defence League's Cyber Unit," Kaitseliit, accessed 20 February 2016, http://www.kaitseliit.ee/en/cyber-unit.

[349] NATO, "Wales Summit Declaration."

[350] NATO, "Cyber Defense Pledge," news release, 08 July 2016, accessed 2 February 2017, http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[351] Christine Shelly, U.S. Department of State Daily Press Briefing for 10 May 1995, U.S. Department of State, accessed 20 February 2016, http://dosfan.lib.uic.edu/ERC/briefing/daily_briefings/1995/9505/950510db.html.

[352] Sean Mirski, "Dispute in the South China Sea: A Legal Primer," *Lawfare*, 9 June 2015, accessed 20 February 2016, https://www.lawfareblog.com/dispute-south-china-sea-legal-primer.

[353] Sean Mirski, "The South China Sea Dispute: A Brief History," *Lawfare*, 8 June 2015, accessed 20 February 2016, https://www.lawfareblog.com/south-china-sea-dispute-brief-history.

[354] Michael McDevitt, "The South China Sea: Navigating the Most Dangerous Place in the World," *War on the Rocks*, 25 November 2014, accessed 25 November 2016, http://warontherocks.com/2014/11/the-south-china-sea-u-s-policy-and-options-for-the-future/.

[355] Mirski, "The South China Sea Dispute: A Brief History."

[356] Ibid.; "CNAS Flashpoints: Timeline: 1955–Present," Center for a New American Security, 3 May 2012, accessed 20 February 2016, http://www.cnas.org/flashpoints/timeline.

[357] McDevitt, "The South China Sea."

[358] Mirski, "The South China Sea Dispute: A Brief History."

[359] Ibid.

[360] Barbara Starr, "Sub Collides with Sonar Array Towed by U.S. Navy Ship," CNN, 12 June 2009, accessed 20 February 2016, http://www.cnn.com/2009/US/06/12/china.submarine/.

[361] Peter J. Brown, "China's Navy Cruises into Pacific Ascendancy," *Asia Times*, 22 April 2010, accessed 20 February 2016, http://www.atimes.com/atimes/China/LD22Ad01.html.

[362] "CNAS Flashpoints: Timeline: 1955–Present," Center for a New American Security.

[363] Ministry of Foreign Affairs of Japan, "Protest Regarding the Issue of a Chinese Ship Approaching a Japanese Survey Ship," press release, 6 May 2010, accessed 20 February 2016. http://www.mofa.go.jp/announce/announce/2010/5/0506_01.html.

[364] Kelley Currie, "Why Is China Picking Fights with Indonesia?" *Weekly Standard*, 6 August 2010, accessed 20 February 2016, http://www.weeklystandard.com/why-is-china-picking-fights-with-indonesia/article/489430.

[365] Shannon Tiezzi, "Japan Seeks Chinese Compensation Over 2010 Boat Collision Incident," *The Diplomat*, 14 February 2014, accessed 20 February 2016, http://thediplomat.com/2014/02/japan-seeks-chinese-compensation-over-2010-boat-collision-incident/.

[366] "China Fisherman Dies in Clash with S Korea Coast Guard," *BBC News*, 18 December 2010, accessed 20 February 2016, http://www.bbc.com/news/world-asia-pacific-12026765.

[367] "U.S.-Filipino Military Exercise Draws Protests in the Philippines," *Democracy Now!* 17 April 2012, accessed 20 February 2016, http://www.democracynow.org/2012/4/17/headlines/us_filipino_military_exercise_draws_protests_in_the_philippines.

[368] Kyodo News,. "China Copter Buzzes MSDF Warship." *The Japan Times*, 9 March 2011, accessed 20 February 2016, http://www.japantimes.co.jp/news/2011/03/09/national/china-copter-buzzes-msdf-warship/#.VsjhFfkrKUk.

[369] James Hardy, "China, Japan Fated for Conflict?" *The Diplomat*, 11 March 2011, accessed 20 February 2016, http://thediplomat.com/2011/03/china-japan-destined-for-conflict/.

[370] "China's Power Thirst Underpins Sovereignty Breach," Vietnam Breaking News, 30 April 2011, accessed 20 February 2016, https://www.vietnambreakingnews.com/2011/04/chinas-power-thirst-underpins-sovereignty-breach/.

[371] Bloomberg News, "Vietnam Says Chinese Boat Harassed Survey Ship; China Disputes," *Bloomberg Business*, 9 June 2011, accessed 20 February 2016, http://www.bloomberg.com/news/articles/2011-06-05/china-reassures-its-neighbors-after-clashes-over-claims-in-south-china-sea.

[372] James Hookway, "Vietnam Plans Live-Fire Drill After China Spat," *Wall Street Journal*, 10 June 2011, accessed 20 February 2016, http://www.wsj.com/articles/SB10001424052702304259304576377090651966146.

[373] Robert Johnson, "Chinese Warship Confronts Indian Navy Vessel in the South China Sea," *Business Insider*, 1 September 2011, accessed 20 February 2016, http://www.businessinsider.com/chinese-warship-confronts-indian-navy-vessel-in-south-china-sea-2011-9.

[374] Associated Press, "Vietnam: Chinese soldiers attack fishermen," Yahoo News, 14 July 2011, accessed 20 February 2016, https://www.yahoo.com/news/vietnam-chinese-soldiers-attack-fishermen-052853883.html.

[375] Radio Netherlands Worldwide, "China Defends Boat Patrol in Disputed Waters," RNW Media, accessed 20 February 2016, https://www.rnw.org/archive/china-defends-boat-patrol-disputed-waters.

[376] "Japan Detains China Boat Captain Off Goto Islands," *BBC News*, 7 November 2011, accessed 20 February 2016, http://www.bbc.com/news/world-asia-15615705.

[377] "China Expells Japanese Survey Boats," *Xinhua*, 21 February 2012, accessed 20 February 2016, http://news.xinhuanet.com/english/china/2012-02/21/c_131423516.htm.

[378] Jeremy Page, "Beijing in Fresh Sea Row with Hanoi," *Wall Street Journal*, 1 March 2012, accessed 20 February 2016, http://www.wsj.com/articles/SB10001424052970203753704577255091639276020.

[379] AFP, "China, Taiwan Slam Japan Over Disputed Islands." Mysinchew.com, 3 March 2012, accessed 20 February 2016, http://www.mysinchew.com/node/70929.

[380] Joseph Yeh, "MOFA Reasserts Taiwan Sovereignty Over South China Sea," *China Post*, 14 March 2012, accessed 20 February 2016, http://www.chinapost.com.tw/taiwan/national/national-news/2012/03/14/334591/MOFA-reasserts.htm.

[381] Ben Blanchard, "China Detains Vietnamese Fishermen in Disputed Water," Reuters, 22 March 2012, accessed 20 February 2016, http://www.reuters.com/article/china-vietnam-idUSL3E8EM3YJ20120322.

[382] Jason Miks, "China, Philippines in Standoff," *The Diplomat*, 11 April 2012, accessed 20 February 2016, http://thediplomat.com/2012/04/china-philippines-in-standoff/.

[383] "CNAS Flashpoints: Timeline: 1955–Present," Center for a New American Security. "U.S.-Filipino Military Exercise Draws Protests in the Philippines," *Democracy Now!*

[384] Kaori Kaneko, Sui-Lee Wee, and Tomasz Janowski, "Tokyo Governor Seeks to Buy Islands Disputed with China," Reuters, 17 April 2012, accessed 20 February 2016, http://www.reuters.com/article/us-japan-china-islands-idUSBRE83G0C020120417.

[385] Jane Perlez, "China Accuses Japan of Stealing After Purchase of Group of Disputed Islands," *New York Times*, 11 September 2012, accessed 20 February 2016, http://www.nytimes.com/2012/09/12/world/asia/china-accuses-japan-of-stealing-disputed-islands.html?_r=0.

[386] Kiyoshi Takenaka and Kaori Kaneko, "Japan Fires Water Cannon to Turn Away Taiwan Boats," Reuters, 25 September 2012, accessed 20 February 2016, http://www.reuters.com/article/us-china-japan-taiwan-idUSBRE88O02C20120925.

[387] Huang Yiming and Wang Qian, "Patrols in Hainan Get More Clout," *China Daily USA*, 28 November 2012, accessed 20 February 2016, http://usa.chinadaily.com.cn/china/2012-11/28/content_15969463.htm.

[388] Hiroko Tabuchi, "Japan Scrambles Jets in Islands Dispute with China," *New York Times*, 13 December 2012, accessed 20 February 2016, http://www.nytimes.com/2012/12/14/world/asia/japan-scrambles-jets-in-island-dispute-with-china.html.

[389] J. Micheal Cole, "Japan, China Scramble Military Jets in East China Sea," *The Diplomat*, 12 January 2013, accessed 20 February 2016, http://thediplomat.com/2013/01/japan-china-scramble-military-jets-in-east-china-sea/.

[390] Mirski, "The South China Sea Dispute: A Brief History."

[391] Jethro Mullen and Yoko Wakatsuki, "China Denies Putting Radar-Lock on Japanese Warship," CNN, 9 February 2013, accessed 20 February 2016, http://www.cnn.com/2013/02/08/world/asia/china-japan-tensions/.

[392] Christopher Harress, "South China Sea Dispute Timeline: A History of Chinese and US Involvement in the Contested Region," *International Business Times*, 27 October 2015, accessed 20 February 2016, http://www.ibtimes.com/south-china-sea-dispute-timeline-history-chinese-us-involvement-contested-region-2158499.

[393] Harress, "South China Sea Dispute Timeline."

[394] Mirski, "The South China Sea Dispute: A Brief History."

[395] Ibid.

[396] Edward Wong, "China Says Construction in Contested Waters Is for Maritime Purposes," *New York Times*, 9 April 2015, accessed 20 February 2016, http://www.nytimes.com/2015/04/10/world/asia/china-south-china-sea-spratly-paracel-islands.html?ref=topics&_r=0.

[397] Ibid.

[398] Jane Perlez, "Beijing, With an Eye on the South China Sea, Adds Patrol Ships," *New York Times*, 10 April 2015, accessed 20 February 2016, http://www.nytimes.com/2015/04/11/world/asia/china-is-rapidly-adding-coast-guard-ships-us-navy-says.html?ref=topics.

[399] Andrew Jacobs, "China Stands by Its Claims Over South China Sea Reefs," *New York Times*, 16 May 2015, accessed 20 February 2016, http://www.nytimes.com/2015/05/17/world/asia/china-stands-by-its-claims-over-reefs.html?ref=topics.

[400] Helene Cooper and Jane Perlez, "U.S. Flies Over a Chinese Project at Sea, and Beijing Objects," *New York Times*, 22 May 2015, accessed 20 February 2016, http://www.nytimes.com/2015/05/23/world/asia/us-flies-over-a-chinese-project-at-sea-and-beijing-objects.html?ref=topics.

[401] Andrew Jacobs, "China, Updating Military Strategy, Puts Focus on Projecting Naval Power," *New York Times*, 26 May 2015, accessed 20 February 2016, http://www.nytimes.com/2015/05/27/world/asia/china-updating-military-strategy-puts-focus-on-projecting-naval-power.html?ref=topics.

[402] Edward Wong and Jane Perlez, "As Tensions with U.S. Grow, Beijing Says It Will Stop Building Artificial Islands in South China Sea," *New York Times*, 16 June 2015, accessed 20 February 2016, http://www.nytimes.com/2015/06/17/world/asia/china-to-halt-its-building-of-islands-but-not-its-projects-on-them.html?ref=topics.

[403] Javier C. Hernández, "China Blames U.S. Military Actions for Tensions in the South China Sea," *New York Times*, 30 July 2015, accessed 20 February 2016, http://www.nytimes.com/2015/07/31/world/asia/china-blames-us-military-actions-for-tensions-in-the-south-china-sea.html?ref=topics.

[404] Jane Perlez, "China Building Airstrip on 3rd Artificial Island, Images Show," *New York Times*, 15 September 2015, accessed 20 February 2016, http://www.nytimes.com/2015/09/16/world/asia/china-building-airstrip-on-3rd-artificial-island-images-show.html?ref=topics.

[405] David E. Sanger and Julie Hirschfeld Davis, "Conflict Flavors Obama's Meeting With Chinese Leader," *New York Times*, 22 September 2015, accessed 20 February 2016, http://www.nytimes.com/2015/09/23/world/asia/conflict-flavors-obamas-meeting-with-chinese-leader.html?ref=topics.

[406] Helene Cooper, "Challenging Chinese Claims, U.S. Sends Warship Near Artificial Island Chain," *New York Times*, 26 October 2015, accessed 20 February 2016, http://www.nytimes.com/2015/10/27/world/asia/challenging-chinese-claims-us-sends-warship-near-artificial-island-chain.html?ref=topics.

[407] Jane Perlez, "In Victory for Philippines, Hague Court to Hear Dispute Over South China Sea" *New York Times*, 30 October 2015, accessed 20 February 2016, http://www.nytimes.com/2015/10/31/world/asia/south-china-sea-philippines-hague.html?login=email&ref=topics&mtrref=undefined.

[408] Associated Press, "Pentagon Chief Raises China Concerns," *New York Times*, 5 November 2015, accessed 20 February 2016, https://www.nytimes.com/2015/11/06/world/asia/pentagon-chief-raises-china-concerns.html?_r=0.

[409] Michael Shear, "Obama Calls on Beijing to Stop Construction in South China Sea," *New York Times*, 18 November 2015, accessed 20 February 2016, http://www.nytimes.com/2015/11/19/world/asia/obama-apec-summit-south-china-sea-philippines.html?ref=topics.

[410] Jane Perlez, "U.S. Navy Commander Implies China Has Eroded Safety of South China Sea," *New York Times*, 15 December 2015, accessed 20 February 2016, http://www.nytimes.com/2015/12/16/world/asia/us-navy-commander-implies-china-has-eroded-safety-of-south-china-sea.html?ref=topics.

[411] Andrew Erickson, Austin Strange, Dean Cheng, Ely Ratner, Shawn Brimley, Robert Haddick, Mira Rapp-Hooper, and Zack Cooper, "China's Menacing Sandcastles in the South China Sea," *War on the Rocks*, 2 March 2015, accessed 20 February 2016, http://warontherocks.com/2015/03/chinas-menacing-sandcastles-in-the-south-china-sea/. McDevitt, "The South China Sea."

[412]峰, 雪, "People's Daily Thinking: Embrace 'Blue Soil'" [translated], *People's Daily*, 16 February 2015, accessed 20 February 2016, http://opinion.people.com.cn/n/2015/0206/c1003-26519807.html. Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[413] Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[414] "CNAS Flashpoints: Timeline: 1955–Present," Center for a New American Security.

[415] Richard D. Fisher, "Posturing Continues in the South and East China Seas." *IHS Jane's Defence Weekly*, 4 December 2015, accessed 20 February 2016, https://janes.ihs.com/Janes/Display/1758030.

[416] Robbie Gramer and Rachel Rizzo, "China's Maginot Line," *War on the Rocks*, 11 August 2015, accessed 20 February 2016, http://warontherocks.com/2015/08/chinas-maginot-line/.

[417] Dean Cheng, "China's Bomber Flight into the Central Pacific: Wake-Up Call for the United States," *War on the Rocks*, 23 December 2015, accessed 20 February 2016, http://warontherocks.com/2015/12/chinas-bomber-flight-into-the-central-pacific-wake-up-call-for-the-united-states/.

[418] Feng Zhang, "Should Beijing Establish an Air Defense Identification Zone Over the South China Sea?" *Foreign Policy*, 4 June 2015, accessed 20 February 2016, http://foreignpolicy.com/2015/06/04/should-beijing-establish-an-air-defense-identification-zone-over-the-south-china-sea/.

[419] Ibid.

[420] Ibid.

[421] Chico Harlan, "China Creates New Air Defense Zone in East China Sea Amid Dispute with Japan." *Washington Post*, 23 November 2013, accessed 20 February 2016, https://www.washingtonpost.com/world/china-creates-new-air-defense-zone-in-east-china-sea-amid-dispute-with-japan/2013/11/23/c415f1a8-5416-11e3-9ee6-2580086d8254_story.html.

[422] Cheng, "China's Bomber Flight into the Central Pacific."

[423] Ibid.

[424] McDevitt, "The South China Sea."

[425] Julian Ku, "China's Harassment of Civilian Ships and Aircraft in the South China Sea Reminds Us Why We Need More U.S. Freedom of Navigation Operations," *Lawfare*, 16 December 2015, accessed 20 February 2016, https://www.lawfareblog.com/chinas-harassment-civilian-ships-and-aircraft-south-china-sea-reminds-us-why-we-need-more-us-freedom.

[426] Ibid.

[427] Tim Kelly, "U.S. Navy Commander Warns of Possible South China Sea Arms Race," Reuters, 15 December 2015, accessed 20 February 2016, http://www.reuters.com/article/us-southchina-usa-idUSKBN0TY03O20151215.

[428] Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[429] United Nations, *United Nations Convention on the Law of the Sea* (New York, 1982), V.A.60, 41, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

[430] Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[431] McDevitt, "The South China Sea."

[432] Kelly, "U.S. Navy Commander Warns of Possible South China Sea Arms Race."

[433] Mirski, "Dispute in the South China Sea: A Legal Primer."

[434] United Nations, *Reports of International Arbitral Awards: Island of Palmas Case* (New York, 1928).

[435] This 200-nautical-mile zone is known as the Exclusive Economic Zone (EEZ). Territorial waters only extend 12 nautical miles from the coast, and grant a state full sovereignty over the territory and allow foreign states "innocent passage" through it. Beyond the Territorial Sea is the Contiguous Zone, which is 12nm to 24nm from the shore, and provides limited sovereignty for the home state. In essence, this serves as a sort of buffer zone. Finally, the EEZ, which stretches from 24nm to 200nm from shore, grants sovereign rights over natural resources in the water column, seabed, and subsoil to the home state.

[436] United Nations, *United Nations Convention on the Law of the Sea*.

[437] McDevitt, "The South China Sea."

[438] Clark Field, "Philippines Vows Stronger Military to Back South China Sea Claim," Reuters, 21 December 2015, accessed 20 February 2016, http://www.reuters.com/article/us-southchinasea-china-philippines-idUSKBN0U40QC20151221. Wells Bennett, "Evaluating China's Jurisdictional Argument in the South China Sea Case," *Lawfare*, 24 August 2015, accessed 20 February 2016, https://www.lawfareblog.com/evaluating-chinas-jurisdictional-argument-south-china-sea-case. Ministry of Foreign Affairs, People's Republic of China, "Position Paper of the Government of the People's Republic of China on the Matter of Jurisdiction in the South China Sea Arbitration Initiated by the Republic of the Philippines," 7 December 2014, accessed 20 February 2016, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1217147.shtml.

[439] Zack Bluestone, "Water Wars: Calling for Calm Amid South China Sea Storm, Xi Unleashes Diplomatic Offensive," *Lawfare*, 13 November 2015, accessed 20 February 2016, https://www.lawfareblog.com/water-wars-calling-calm-amid-south-china-sea-storm-xi-unleashes-diplomatic-offensive.

[440] Ibid.

[441] Lauren Dickey, "Britain's Mercantile Diplomacy with China," *War on the Rocks*, 2 November 2015, accessed 20 February 2016, http://warontherocks.com/2015/11/britains-mercantile-diplomacy-with-china/.

[442] Ibid.

[443] Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[444] Mike Pietrucha, "The Economics of War with China: This Will Hurt You More Than It Hurts Me," *War on the Rocks*, 4 November 2015, accessed 20 February 2016, http://warontherocks.com/2015/11/the-economics-of-war-with-china-this-will-hurt-you-more-than-it-hurts-me/.

[445] Erickson, et al., "China's Menacing Sandcastles in the South China Sea."

[446] "Mutual Defense Treaty Between the United States and the Republic of the Philippines," 30 August 1951, *American Foreign Policy 1950–1955*, Department of State Publication 6446, accessed 20 February 2016. http://avalon.law.yale.edu/20th_century/phil001.asp.

[447] Sui-Lee Wee and Ben Blanchard, "China Angered as Filipino Protesters Visit South China Sea Island," Reuters, 28 December 2015, accessed 20 February 2016, http://www.reuters.com/article/us-southchinasea-china-philippines-idUSKBN0UB0G820151228.

[448] Andrea Shalal, "Exclusive: Another U.S. Patrol in South China Sea Unlikely This Year – Officials," Reuters, 15 December 2015, accessed 20 February 2016, http://www.reuters.com/article/us-southchinasea-china-usa-idUSKBN0TX2MJ20151215.

[449] Julian Ku, "The US Navy's 'Innocent Passage' in the South China Sea May Have Actually Strengthened China's Sketchy Territorial Claims," *Lawfare*, 4 November 2015, accessed 20 February 2016, https://www.lawfareblog.com/us-navys-innocent-passage-south-china-sea-may-have-actually-strengthened-chinas-sketchy-territorial.

[450] Kelly, "U.S. Navy Commander Warns of Possible South China Sea Arms Race."

[451] Zack Bluestone, "Water Wars: The PRC's Double Trouble in the South China Sea," *Lawfare*, 31 October 2015, accessed 20 February 2016, https://www.lawfareblog.com/water-wars-prcs-double-trouble-south-china-sea.

[452] Katie Hunt, "South China Sea: Court Rules in Favor of Philippines over China," CNN, 12 July 2016, accessed 7 February 2017, http://www.cnn.com/2016/07/12/asia/china-philippines-south-china-sea/.

[453] Kelly, "U.S. Navy Commander Warns of Possible South China Sea Arms Race."

[454] Greg Torode and Manuel Mogato, "China May Pay 'International Price' in South China Sea Legal Case, Experts Say," Reuters, 1 December 2015, accessed 20 February 2016, http://www.reuters.com/article/southchinasea-china-court-idUSL3N12Z1SB20151202.

[455] David Bosco, "Indonesia Hints at South China Sea Litigation," *Lawfare*, 12 November 2015, accessed 20 February 2016, https://www.lawfareblog.com/indonesia-hints-south-china-sea-litigation.

[456] Estonia's Social Democratic Party has become the de facto party for the Russian minority. Estonia's electoral regulations allow Russian citizens and holders of "grey passports" to vote in local elections, allowing the party to rise to prominence in areas dominated by ethnic Russians. However, as these non-citizens are not allowed to vote in national elections, the party has little power on the national stage, leading to a feeling among many ethnic Russians that their national government does not represent them or their interests.

[457] While the Harmony party had long enjoyed the highest membership of any major party in Latvia, the unwillingness of any other party to form a coalition government with it prevented it from controlling the government. However, its recent appeals to the interests of ethnic Latvians allowed it to win the majority in the country and rise to power.

[458] Of the Baltics, Lithuania has been the most successful in combatting IO through institutionalized critical thinking education and vigilante groups, colloquially called "Elves," who roam the Internet, exposing inconsistencies and untruths in Russian propaganda efforts.

[459] "Estonian Defence League," Kaitseliit, accessed 20 February 2016, http://www.kaitseliit.ee/en/edl. "The task of the Estonian Defence League is to enhance, by relying on free will and self-initiative, the nation's readiness to defend the independence of Estonia and its constitutional order. The activities of the Estonian Defence League are provided by the Estonian Defence League Act, the Statutes, which prescribe internal organisation of the Estonian Defence League more precisely, and the rules of procedure, which prescribe relations of active members of the Estonian Defence League to the codes of conduct of the Defence Forces, rules of conduct and internal administration procedure. The Statutes and rules of procedure of the Estonian Defence League are approved by the Government of the Republic. There are 15,500 members in the Estonian Defence League."

[460] This potential for the Russian use of a natural disaster to move forward with their hybrid strategy was mentioned in a variety of interviews conducted by the authors in Estonia. The interviewees chose to be anonymous for this study.

[461] Russia has been working with both countries to increase Russian tourism to their beaches, and has been able to support both countries during the latest economic crisis.