



The Mitchell Forum

A Shifting Puzzle: Understanding and Countering Russian Hybrid Warfare

By Cadet Courtney Kunselman, US Air Force Academy

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.#

Abstract

In the contemporary strategic operating environment facing the United States, so-called “hybrid warfare” use is growing more prevalent. Hybrid warfare combines conventional and unconventional means in order to produce strategically destabilizing effects and often involves an actor’s use of all diplomatic, information, military, and economic means, making this form of war a whole-of-government endeavor. If conducted properly, this model has the potential to effectively cripple an adversarial state, and facilitate the achievement of strategic goals without necessarily showing any obvious signs of aggression.

Through its use of a hybrid strategy, Russia now poses an alarming security threat to NATO, specifically on the Alliance’s eastern periphery and towards the Baltic States. In order to effectively counter Russia’s aggressive posture, NATO must rethink its outdated doctrines and defense strategy, prioritize military capacity building, and quickly develop a plan for stabilizing targeted regions. The United States can assist in this endeavor by fully cooperating with NATO counter-hybrid initiatives, and through implementing counter-hybrid initiatives of its own.

It is likely that regional powers other than Russia, such as Iran with its close ties to non-state actors like Hezbollah, and China with its cyber and disinformation capabilities, will learn from Russia’s success and the west’s inability to respond to hybrid strategies effectively. In order to ensure the US and its allies have the capability to meet the challenges this form of warfare poses, NATO and the United States must commit to developing and adopting an effective all-of-government counter-hybrid warfare strategy.

Introduction: The Problem of Hybrid War

The contemporary strategic operating environment facing the United States often resembles a jigsaw puzzle, where pieces are constantly warping while the picture remains the same. This often renders old solutions obsolete, while simultaneously prompting political and military decision-makers to swiftly and effectively react before a picture becomes unrecognizable.

This “warping” is simply a result of shifting balances of power and influence in geopolitics due to technological and intellectual advances, the formation and dissolution of alliances and partnerships, ideological uprisings, and other events. One of the puzzle’s pieces that have warped drastically in recent history is the ratio of conflicts that fall under the categories of conventional, unconventional, and hybrid warfare.

While none of these categorizations of using political ways and means to achieve desired ends are especially novel or radical, until recently the prevalence of solely conventional or unconventional conflicts far outweighed the appearance of conflicts that combined elements of these categories. However, in a world with a sole military superpower, an assortment of conflicting ideologies, and a healthy dispersal of nuclear weapons, hybrid conflicts are on their way to becoming the dominant component in modern warfare, especially in cases where forces that are weaker conventionally are pitted against a military superpower (the United States) or its partners. This paper will discuss the implications of this shift, focusing on the significance of the security threat Russia poses to the United States and its allies and partners through its successful utilization of hybrid strategy and how these nations should go about responding to these threats.

Before the specifics of Russian strategy can be discussed, a referential framework needs to be built for this often-cloudy concept. As evidenced by its name, hybrid warfare combines conventional and unconventional means in order to produce strategically destabilizing effects. Hybrid war often involves the actor’s use of all diplomatic,

informational, military, and economic means, making it a whole-of-government endeavor.¹ It is a model of waging war that, if conducted properly, has the potential to effectively cripple an adversarial state and facilitate the achievement of strategic goals without showing any obvious signs of aggression.²

The general framework for the employment of hybrid war in its modern form can be illustrated in the following notional example. The adversarial state starts off by seeking to create an environment of public uncertainty, fanning elements of dissent through methods such as information operations, propaganda campaigns, economic coercion, and sponsorship of political protests. Once problems begin to emerge in the form of unrest or social upheaval, the aggressor seeks acceptance into the conflict by painting itself as a concerned party instead of an influencing power. As this access is gained, existing internal dissent can be encouraged through covert denial and deception operations using special operations forces, which create an operating front within an adversarial state.

When this front is established, influence can continue by the aggressor until the adversarial state becomes so destabilized that the aggressing state appears justified in sending in conventional forces to provide stability. When conventional forces become involved, the aggressor has the power to unduly influence governing structures in the adversarial state. The aggressor maintains a “low signature state involvement” so that early acts are deniable, an aspect of hybrid war which is key to its success. Uncertainty causes the adversarial state’s governing apparatus to become paralyzed and unable to attribute the source of the instability, while simultaneously discouraging other interested parties from intervening.³

The History of Hybrid War

While the general idea of a hybrid approach has been used throughout history, its methods have evolved over time. Its first recognized use was during the Peloponnesian War when the town of Mytilene rose up against the Athenian Empire in order to encourage the unification of the island of Lesbos. To achieve this goal, ambassadors were sent to both Sparta in order to seek clandestine support, and to Athens in order

The adversarial state starts off by seeking to create an environment of public uncertainty, fanning elements such as dissent through methods such as information operations, propaganda campaigns, economic coercion, and sponsorship of political protests.

...the Kremlin has augmented its hybrid warfighting capabilities since 2008 and is now relying on them to achieve strategic military and political goals.

to negotiate a settlement. The conflict did not end well for the Mytilenians, but the idea of combining conventional and unconventional means in order to achieve strategic effects through disorientation was a key feature of the conflict.⁴

In the Jewish Rebellion of 66 CE, a hybrid force of bandits, trained soldiers, and unregulated fighters which used tactics ranging from roadside ambushes to fixed battles sought to overcome a stronger conventional Roman force through asymmetric means.⁵ In the American Revolutionary War, the Continental Army was supported by irregular militia forces which employed guerrilla tactics against the superior British forces. Similarly, in 1806 during the Napoleonic Wars in Spain, Spanish guerrillas disrupted French lines of communication in order to allow British regular troops to have a fighting chance against the French forces.⁶ More recent examples, which have enjoyed higher levels of success, include Iran's support and resupply of Hezbollah in its war with Israel in 2006, and Russia's invasion of Georgia in 2008 which involved escalation of tensions through information operations in order to allow Russia to enter under the guise of preventing a humanitarian crisis.^{7,8}

Unfortunately, as evidenced by recently published military doctrine and its successful employment in Ukraine, the Kremlin has augmented its hybrid warfighting capabilities since 2008 and is now relying on them to achieve strategic military and political goals. In February of 2013, General Valery Gerasimov, chief of the Russian General Staff, published a piece entitled "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." This article, which articulates what has come to be known as the Gerasimov Doctrine, proposes "a new Russian way of warfare that blends conventional and unconventional warfare with aspects of national power."⁹ He advocates for Russia to see war as something beyond the scope of a military conflict, and argues that war should be fought by a four to one ratio of non-military to military measures.¹⁰ Russia certainly showcased the power of these non-

military instruments in Ukraine by employing economic tools to pressure political elites, utilizing media to spread pro-Russian propaganda, building bonds between Russian organized crime and local criminal organizations, and coordinating massive cyber attacks on non-military targets to cause internal strife and political paralysis.¹¹

For the Western world, the Russian success in Ukraine is certainly cause for concern. In building this model of conducting war, Gerasimov was no fool. Recognizing conventional military capabilities as a strength of his own but an even greater strength of the friends of his enemies, Gerasimov designed a method of aggression which stays below the threshold of conventional conflict while still wreaking enough havoc to make the targeted state susceptible to an arguably justified conventional intervention.¹² This strategy also assists the Kremlin in battling the occasional flare up of political instability by providing Putin with the option to boost national pride through aggressive action to support ethnic Russians living outside of Russia, without facing any negative consequences from intervening outside powers. If Putin starts to feel his power slip, Baltic States such as Latvia (26 percent ethnic Russians) and Estonia (25 percent ethnic Russians) are rightly perceived as the potential next victims of Russian hybrid aggression. Thus, if NATO wishes to protect its members from Russian aggression, without having to worry about invoking Article V and igniting World War III, it must develop an effective response to this hybrid strategy. Furthermore, to assist in this undertaking and to protect its own interests, the United States, the most influential member of NATO, should lead the charge and prioritize the development of its own counter-hybrid warfare response.¹³

The importance of expending the time and resources to develop a strategy tailored to countering the hybrid threat cannot be overlooked. Indeed, according to the British House of Commons Defense Committee, "NATO is currently not well-prepared for a Russian threat against a NATO Member State" because the asymmetric beginnings of hybrid operations are below NATO's response threshold and because its doctrine and subsequent training does not address the blending of conventional and unconventional means.¹⁴

Similarly, as claimed by the United States Army Special Operations Command's recent white paper on countering unconventional warfare, "the joint and interagency community [of the United States] has yet to present a credible strategic-level ability to interdict and roll back external sponsorship of insurgent and separatist movements."¹⁵ These deficiencies most likely stem from the fact that counter-hybrid methods differ significantly from the counter-terrorism and counter-insurgency operations that the West has been focused on conducting for more than the past decade. While the West is surely capable of adapting to this new style of conflict, the major differences between these types of operations must first be recognized. As an analysis from the Indian think tank Centre for Land Warfare Studies explains:

[w]hile [counterinsurgency] ops are designed to contain and defeat an insurgency and often have a tendency to generate a very large footprint, [counter-hybrid operations] on the other hand can be executed by a smaller force and hence project a smaller footprint. Being specifically designed to deny an adversary the ability to use proxy war as a path to strategic success, [counter-hybrid operations] are narrowly scoped with a low signature. Unlike [counter-terrorism operations] which tend to be short-term, time-sensitive operations with instant visible results, [counter-hybrid operations] by contrast are visualised to become prolonged and proactive.¹⁶

Thus, in order for NATO and the United States to effectively counter this new form of Russian aggression, they must develop distinct and cohesive counter-hybrid warfighting responses instead of relying on a conglomeration of methods for countering other types of irregular conflict.

In order to develop this effective response, NATO must first re-examine and re-engineer some current doctrine and defense strategy. As described above, NATO's recent focus on counterinsurgency and counter-terrorism operations "has introduced force profiles, training, exercises, logistics systems, equipment, and priorities quite different... to those which would be required to meet a Russian

threat to a Baltic state," according to an analysis from the defense committee of the British House of Commons.¹⁷ To counter these established force profiles and priorities, NATO should establish an "Opposing Force Office" through which it can gather intelligence, and strategic and technological experts from all member states to conduct research into opponents' advances in order to recommend new policies or courses of action necessary to tackle the most pressing threats.¹⁸ Once decision makers are convinced of the pressing danger and dynamism of the Russian hybrid threat, steps can be taken to alter priorities and policy to defend against it. One such step would be to re-invigorate large-scale conventional military exercises. Indeed, since the second phase of the hybrid threat involves swift and decisive conventional action, NATO must have a large, well-trained conventional force at its disposal. Vast improvements have occurred with regards to NATO military capability since the Crimea crisis, as seen in the organization and implementation of exercises such as Trident Juncture in 2016, the largest Alliance training exercise since the end of the Cold War, involving 36,000 troops. But Russian exercises continue to occur on a larger scale. In September 2015, the Russian "Centr-15" exercise consisted of 95,000 troops, with the Russian general staff bragging the "Kavkaz-16" exercise involved some 120,000 personnel, though analysts said this claim is somewhat suspect as it conflated separate activities together.¹⁹

A second step would be to re-examine the wording of Article 5 of NATO's founding treaty in light of threats specifically designed to stay beneath the Alliance's response threshold. Currently, Article 5 necessitates an armed attack against a NATO member in order to warrant a collective response. Unfortunately, this is ill suited to hybrid threats, since the integrity of the victim state is generally compromised before any type of armed attack that can be attributed commences. Thus, NATO should seriously consider removing the word "armed" from Article 5 in order to allow a collective response for asymmetrical acts of aggression, such as cyber attacks and information/psychological operations.²⁰ Of course, these responses would be proportional in order to avoid the unnecessary escalation of the conflict.

While this Opposing Force Office would surely come up with more policy and doctrinal changes than recommended here, one last step would be to take deliberate action to synchronize and streamline processes across government agencies as well as in public and private sector decision-making approaches to improve situational awareness, threat recognition, and response time. This will assist the coordination and implementation of both military and nonmilitary tools to answer hybrid threats.²¹ The only way to effectively counter an all-of-government approach is with an all-of-government approach, and the key to success in this endeavor is closer cooperation between all civilian and military elements. Indeed, the hybrid threat

relies upon disrupting the Observe, Orient, Decide, and Act Loop of the adversary in order to paralyze decision-making and response time. Thus, if NATO can fortify its own OODA Loop through greater cooperation between decision-making elements, the Alliance will be at a much lower risk of falling victim to response paralysis.

These changes logically lead to concrete actions in capacity building, deterring Russian aggression, and countering asymmetric attacks that are even currently taking place. Regarding

capacity building, NATO has recently taken steps to augment its rapid-reaction forces, but it is still lacking in sufficient counter-electronic warfare and cyber capabilities, and an ability to function in denied environments. The deficiencies of NATO's older response force structures stem from a scarcity of credibility. This is largely due to an inability to agree on response force deployment practices, depleted command and control structures, and a lack of exercises and training at the divisional and corps level.²² In response to recognizing the vulnerabilities resulting from such deficiencies, the Alliance has bolstered the NATO Response Force to 30,000 troops and created the Very High Readiness Joint Task Force (VJTF) in 2015. This task force, consisting of 5,000 troops from land, air, sea, and special operations forces, is designed and equipped to effectively respond to emerging

threats within 48 hours. Both exercise Noble Jump (in June 2015) and Trident Juncture (in fall 2015, and a smaller iteration in 2016) showcased NATO's ability and willingness to employ these newly-enhanced rapid response forces. In addition, the decision-making process leading to NRF and VJTF employment has been streamlined through the establishment and empowerment of six small headquarters elements in Bulgaria, Estonia, Latvia, Lithuania, Poland, and Romania.²³ However, in order to maintain this level of readiness, NATO members must be committed to spending an agreed upon two percent of GDP on defense measures so they can build and maintain capabilities to contribute to the collective defense of the organization.

Another capacity NATO needs to build up is its counter-electronic warfare and cyber capabilities. NATO has fallen far behind its potential adversaries (especially those engaging in unconventional practices) in resources committed to electronic warfare, some analyses suggest, and this lack of investment has made command, control, communication and intelligence (known as C3I) assets and tools vulnerable to Russian asymmetric methods.²⁴ Every Russian military district "houses an independent [electronic warfare] brigade, supplemented by strategic battalions with specialized [electronic warfare] equipment," and these capabilities caused devastating effect in the Ukrainian conflict, when they supported Russian special operators.²⁵

In order to at least mitigate the impact of this threat, NATO must ensure that all of its C3I capabilities are sufficiently redundant to survive electronic defense breaches. Similarly, assessments show that cyber space constitutes one of NATO's greatest vulnerabilities. Forming adequate reactions is difficult in NATO's consensus-driven structure, and determining the source of an attack is almost impossible to do in this sort of construct rapidly.²⁶ Since cyber defense and responding to cyber attacks is so difficult, NATO must also ensure the redundancy of its cyber systems and build offensive cyber capabilities. If NATO intelligence platforms gain evidence pointing to an impending cyber attack, the Alliance can preemptively attack the threat. However, in case redundant systems are not enough to counter Russian electronic warfare

Another capacity NATO needs to build up is its counter-electronic warfare and cyber capabilities. NATO has fallen far behind its potential adversaries (especially those engaging in unconventional practices) in resources committed to electronic warfare...

Countering propaganda campaigns, as well as information and psychological operations, is key to stunting the growth of instability. The more educated the target population is, the more likely it is that Russian operations will be seen for the deceptions that they are.

and cyber threats, NATO forces must be prepared to operate in network-denied environments. Once again, preparing for this scenario would entail large-scale exercises simulating the loss of communications, navigational, or other electronic systems which modern combat operations have come to rely upon.

Once the capacity-building process is under way, NATO should take steps to utilize these new capabilities to deter Russian aggression in the Baltics. Nuclear deterrence is only credible in the face of the most egregious and easily attributable attacks since employing such a weapon has the potential to cause massive devastation on both sides. In order to deter a threat that is designed to stay below response thresholds and which is often difficult to attribute, NATO must improve upon its conventional deterrence structure.²⁷

One way of doing so would be to raise the cost of invading a Baltic state far above any potential benefits Russia would receive from such an act. To do so, NATO should continue and expand its efforts to pre-position heavy conventional equipment in the Baltics while simultaneously maintaining a continuous presence with a significant force of troops. This presence is expanding, through the implementation of large-scale training exercises, such as Trident Juncture and Poland's Anaconda-2016, and by the US' effort to move more troops into Europe to partner with allies.²⁸ According to Edward Lucas of *The Economist*, it would actually be cheaper to base troops in Eastern Europe than in Western Europe. This move would both help NATO to be fiscally responsible, and raise the cost of an invasion, while at the same time, significantly reducing NATO response time.

NATO could further raise the cost of invasion by encouraging at-risk Baltic states to follow the Swiss model of a total defense program. If a greater proportion of the population is trained to fight and has a better understanding of military operations, the price of occupation by Russian forces would skyrocket (that is, as long as Russian propaganda campaigns were successfully countered, so that ethnic Russians in these states

would not utilize this training to become more effective insurgents).²⁹ Furthermore, encouraging the augmentation of interior ministries and law enforcement agencies in these countries would assist in rendering asymmetric attacks such as propaganda campaigns and home-grown separatist militias much less effective and result in reduced internal ethnic Russian support.³⁰ In implementing any deterrence action, it is important to remember that Russia is engaging in hybrid methods because it wishes to avoid direct conventional confrontation. Thus, any repositioning or augmentation of capabilities which raise the probability that an asymmetric attack would involve Russia in a large-scale conventional conflict is certainly a credible deterrent against this type of aggression.

Unfortunately, the steps outlined above will not be successful in deterring all hybrid aggression from Russia. Thus, NATO must have some strategy in place to counter asymmetric means before the victim state becomes too unstable. Countering propaganda campaigns, as well as information and psychological operations, is key to stunting the growth of instability. The more educated the target population is, the more likely it is that Russian operations will be seen for the deceptions that they are.

One way in which NATO can counter this disinformation is with information campaigns of its own. Indeed, countering unconventional means often entails employing asymmetric tactics in response. However, it is important to note that "unilateral information broadcast from NATO itself would not be accepted in all parts of society and could be perceived as NATO propaganda, as the reception of Russian media disinformation has shown."³¹ Instead, NATO should start funding and empowering international networks of anti-corruption non-government organizations (NGOs) to operate in at-risk states to disseminate objective, truthful information.³² These organizations would be able to debunk Russian deceptions at both the local and the international levels, resulting in a clearer picture of Russian actions to base decisions on. Ultimately, as NATO Secretary General Jens Stoltenberg explains, "[our] best weapon against disinformation is information based on our values of democracy, freedom of speech, and open societies."³³

Other non-military means, such as economic tools, can also be used to counter Russian asymmetric aggression. As James Sherr of Chatham House explains, it is important to understand that, economically, Russia is more dependent on the West than any states in the West are on Russia.³⁴ Thus, economic sanctions could have huge impacts on Russia's ability to fight wars. Furthermore, Russia would be hard pressed to respond since countering with sanctions of its own would only further isolate its struggling economy from the rest of the world. However, the fact that many Eastern European countries, including some NATO allies, are reliant on Russian gas cannot be overlooked because there is the chance that Russia would respond to such sanctions by cutting off desperately needed energy to these countries. If

NATO were to pursue economic sanctions, it would first need to greatly encourage the Western European states to expedite the construction of the gas pipeline between Germany and Lithuania, as well as invest in a Trans-Adriatic Pipeline in order to avoid potential instability in the states it is ultimately trying to protect.³⁵

Of course, many of these recommended changes and actions will only work with support from individual member states. This implies there are actions that the United States can take specifically to support the

collective fight against Russian hybrid aggression. If the United States could lead by example and fill all of its senior command positions, keep defense spending at or above two percent of GDP, and leverage its law enforcement assets to train and assist partner organizations in at-risk states, other NATO members would likely be encouraged to follow suit. However, in a state governed by popular opinion, this task can be difficult if the population is not properly educated on both the graveness of the Russian hybrid warfare threat and the importance of NATO taking action to counter it. Thus, political leaders must make greater efforts to educate the American (and European) populace on these issues. If the United States does not appear

to be fully behind the counter-hybrid mission, NATO's deterrent posture could be somewhat discredited due to a perceived lack of unity.³⁶

However, the United States is not limited to only countering Russian hybrid aggression through its support of NATO. The United States can engage in political warfare activities of its own against Russia, outside of the Alliance structure. Of course, since these measures would be taken to counter the unconventional aspects of Russian aggression, they would be asymmetric in nature themselves, and they would also be much different in character than the irregular methods that have been successfully employed in counter terrorism and counterinsurgency operations. Thus, according to a recently published United States Army paper on countering unconventional warfare, the Council on Foreign Relations believes that it would be prudent to assign a political warfare coordinator to the National Security Council staff. Once this advisor is sufficiently entrenched, progress can be made toward establishing effective political warfare strategies involving the entire gamut of nonmilitary instruments, including economic sanctions against groups and individuals, support for friendly governments and foreign political actors opposing Russian hybrid actions, and strategic communications and information operations focused on exposing Russian activity.³⁷

Unfortunately, it must be understood that these recommended policy changes and courses of action for both NATO and the United States come with significant challenges. The most glaring challenge this proposed model for counter-hybrid warfare poses is that it requires a very coordinated all-of-government approach over a prolonged period of time. For the United States, this implies better relations between civilian and military organizations as well as continuity of policy over multiple administrations.

Since the end of the Cold War, it has been rare for the United States to invest in developing long-lead options like the type required to counter hybrid warfare strategies. Consequently, the United States has not displayed much enthusiasm for a strategic whole-of-government capacity beyond operations such as counter-terrorism, and due to the lack of metrics which counter-hybrid methods produce in comparison to counter-terrorism

...the fact that many Eastern European countries, including some NATO allies, are reliant on Russian gas cannot be overlooked because there is the chance that Russia would respond to such sanctions by cutting off desperately needed energy to these countries.

operations, it is likely that new legislation in the US Congress may even be necessary to create an enduring capacity.³⁸ As for NATO, the problems described for the United States are multiplied because a protracted policy which all members agree on has to be maintained and executed by civilian and military organizations from the Alliance's member states. Furthermore, any more proposed large-scale exercises would most likely incur increases in defense spending, prompting member states to contribute more to the collective good of the Alliance. This aspect could be a long term issue, considering there is currently a lack of political will in many NATO member states to support collective responses to asymmetric attacks.³⁹

Before the West loses sight of the present strategic operating environment, it must ensure that it is fitting the newly sized puzzle pieces together with a comprehensive counter-hybrid warfare

approach. While hybrid methods are certainly not new, their prevalence is on the rise, especially by states wanting to achieve strategic goals without participating in a large-scale conventional conflict with the West. As evidenced by its recent actions in Ukraine, Russia is certainly one of the most effective employers of this method of warfare, and if NATO does not adapt, the Baltics could soon be in danger.

However, it is likely that other regional powers, such as Iran with its close ties to non-state actors such as Hezbollah, and China with its cyber and disinformation capabilities, will learn from Russia's success and the West's inability to respond and become more aggressive in their own hybrid campaigns. In order to ensure that we have the capability to successfully counter this form of warfare, NATO and the United States must commit to developing and adopting an effective all-of-government counter-hybrid warfare strategy. 🌟

Endnotes

- 1 United States Army Special Operations Command, "Counter-Unconventional Warfare White Paper," United States Army Special Operations Command, September 26, 2014, 3.
- 2 House of Commons Defense Committee, "Towards the Next Defence and Security Review: Part Two – NATO," London, U.K. House of Commons, July 31, 2014, 14-16.
- 3 Deepak Induraj, "Countering Hybrid Warfare," Centre for Land Warfare Studies: New Delhi, India, December 16, 2015, <http://www.claws.in/1486/countering-hybrid-warfare-deepak-induraj.html> (accessed May 2017).
- 4 Induraj, "Countering Hybrid Warfare."
- 5 US Army Maj Timothy McCulloh and US Army Maj Richard Johnson, *Hybrid Warfare, JSOU Report 13-4*, (MacDill AFB, Fla.: Joint Special Operations University, August 2013), 3.
- 6 Alex Deep, "Hybrid War: Old Concept, New Techniques," *Small Wars Journal*, March 2, 2015.
- 7 Robert Newson, "Why the US Needs a Strategy To Counter 'Hybrid Warfare,'" *Defense One*, October 23, 2014, <http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybrid-warfare/97259/> (accessed May 2017).
- 8 House of Commons Defense Committee, "Towards the next Defence and Security Review," 14.
- 9 Charles Bartles, "Getting Gerasimov Right," *Military Review*, January-February, 2016, 30.
- 10 Bartles, "Getting Gerasimov Right," 34.
- 11 Ralph Thiele, "Hybrid Threats – And How to Counter Them," ISPSW Strategy Series: Focus on Defense and International Security, No. 448, September, 2016, <http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybrid-warfare/97259/> (accessed May 2017).
- 12 Dan Goure, "NATO vs. Russia: How to Counter the Hybrid Warfare Challenge," *The National Interest*, July 7, 2016.
- 13 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 28.
- 14 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 3.
- 15 United States Army Special Operations Command, "Counter-Unconventional Warfare White Paper," 5.
- 16 Induraj, "Countering Hybrid Warfare."
- 17 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 22.
- 18 Editorial Team -Atlantic-Community.org, "Future-Proofing NATO: A Forthcoming Decade of Change," *Small Wars Journal*, October 8, 2016, <http://smallwarsjournal.com/jrnl/art/future-proofing-nato-a-forthcoming-decade-of-change> (accessed May 2017).
- 19 Ian Brzezinski and Nicholas Varangis, "The NATO-Russia Exercise Gap... Then, Now, & 2017," *The Atlantic Council-NATOSource*, October 25, 2016 <http://www.atlanticcouncil.org/blogs/natosource/the-nato-russia-exercise-gap-then-now-2017> (accessed May 2017).
- 20 House of Commons Defense Committee, "Towards the next Defence and Security Review," 31.
- 21 Ralph Thiele, "Hybrid Threats – And How to Counter Them."
- 22 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 22-24.
- 23 Marc V. Schanz, "All for One in NATO," *Air Force Magazine*, October 2015, <http://www.airforcemag.com/MagazineArchive/Pages/2015/October%202015/All-for-One-in-NATO.aspx> (accessed May 2017).
- 24 Atlantic-Community.org, "Future-Proofing NATO."
- 25 Bret Perry, "How NATO Can Disrupt Russia's New Way of War," *Defense One*, March 3, 2016, <http://www.defenseone.com/ideas/2016/03/nato-russia-sof-ew-hybrid-war/126401/> (accessed May 2017).
- 26 Ralph Thiele, "Hybrid Threats – And How to Counter Them."
- 27 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 26.
- 28 Alex Duval Smith, "NATO Countries Begin Largest War Game in Eastern Europe Since Cold War," *The Guardian*, June 6, 2016; Luke Harding, "NATO and Russia Playing Dangerous Game with Military Build-up," *The Guardian*, October 27, 2016.
- 29 Atlantic-Community.org, "Future-Proofing NATO."
- 30 Ralph Thiele, "Hybrid Threats – And How to Counter Them."
- 31 Atlantic-Community.org, "Future-Proofing NATO."
- 32 Peter Pomerantsev, "How Putin Is Reinventing Warfare," *Foreign Policy*, May 5, 2014.
- 33 Jim Garamone, "NATO Focuses on Combating Hybrid Warfare," *DoD News*, May 14, 2015.
- 34 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 16.
- 35 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 29.
- 36 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 27.
- 37 United States Army Special Operations Command, "Counter-Unconventional Warfare White Paper," 12-13.
- 38 Robert Newson, "Why the US Needs a Strategy To Counter 'Hybrid Warfare.'"
- 39 House of Commons Defense Committee, "Towards the Next Defence and Security Review," 30.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Cadet Courtney J. Kunselman (United States Air Force Academy, Class of 2018) hails from DuBois, Pennsylvania. She is an applied mathematics major with a focus in materials chemistry, and aspires to work in the intelligence field upon graduation. In the future, she is also interested in continuing her studies in a masters program, focusing on materials science or policy analysis.

