University of Ottawa

Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization

API 6999 – Major Research Paper
Katie Abbott (7844363)
Supervisor: Professor Roland Paris
March 23, 2016

Abstract

The Russian annexation of Ukraine's Crimea and subsequent destabilization of Eastern Ukraine was kinetically executed through special forces in conjunction with a series of synchronized, layered, well planned and coordinated diplomatic, cyber, economic, informational, and psychological tactics. This form of warfare is referred to as "hybrid warfare". Hybrid warfare is a form of war fighting that includes a range of multi-modal activities that can be conducted by state or non-state actors. Emphasis is placed on simultaneous and unprecedented fusion of a variety of means such as political, military, economic/financial, social and informational using conventional, irregular, catastrophic, terrorist and disruptive/criminal methods to achieve political objectives. In the case of the Crimea, the Russian intervention involved the rapid deployment of a range of complex, multi-modal, and highly integrated set of activities in a way that was novel, and which posed a historically unique set of challenges to the North Atlantic Treaty Organization (NATO). This research paper will explore the concept hybrid warfare, identify the political and military limitations NATO has faced as a result of hybrid warfare in Ukraine, evaluate NATO's efforts to date to adapt, and provide recommendations for NATO and Canada in adapting to this form of aggression.

Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization

1.0 Introduction[1]

The Russian annexation of Ukraine's Crimea and subsequent destabilization of Eastern Ukraine was kinetically executed through special (unconventional) forces in conjunction with a series of synchronized, layered, well planned and coordinated diplomatic, cyber, economic, informational, and psychological tactics. This form of warfare is referred to as "hybrid warfare". As this paper will illustrate, the term hybrid warfare lacks a precise universally accepted definition.[2] However, this paper concludes that a well-rounded definition of hybrid warfare

[1] I would like to express my gratitude and appreciation to the Government of Canada officials at the Departments of Defence and Global Affairs Canada, who graciously facilitated meetings and/or spoke with me regarding this research project and provided unique and insightful perspective.

[2] It is important to note that is beyond the scope of this paper to thoroughly debate the operationalization of the term hybrid warfare. A brief summary of the concept's central milestones of its theoretical and definitional origins will be provided in order to facilitate the contextualization of Russia's use of hybrid warfare in Ukraine. This paper acknowledges that the novelty and usefulness of the concept hybrid warfare is challenged and debated. However, this paper is based on the theoretical assumption that because NATO has defined, identified and securitized "hybrid warfare" as an existential threat, and has devoted significant amounts of resources and efforts in constructing strategic, policy and operational counter-measures aimed exclusively at hybrid warfare, it is of importance in and of itself to discuss and

would incorporate and acknowledge the various definitions of the concept and describe it as a form of warfare that includes a range of multi-modal activities that can be conducted by state or non-state actors. Emphasis is placed on simultaneous and unprecedented fusion of a variety of means such as political, military, economic/financial, social and informational using conventional, irregular, catastrophic, terrorist and disruptive/criminal methods to achieve political objectives. The hybrid actor fuses these means and methods in a way that is specific to and tailored-made to the context at hand. Importantly, this paper notes that when conceptualizing the term, is "not the 'one time' precision in defining hybrid warfare but instead perpetuation of an active dialogue on a new and expanding universe of complex defence-relevant challenges." [3]

In the case of the Crimea, the Russian intervention involved the rapid deployment of a range of complex, multi-modal, and highly integrated set of activities in a way that was novel, and which posed a historically unique set of challenges to the North Atlantic Treaty Organization (NATO). By its own admission, Russia's hybrid warfare exposed political and military limitations within NATO - an organization primarily designed to respond to state conventional kinetic threats.

This research paper will first provide a brief summary of the concept of hybrid warfare and explore the central milestones of its theoretical and definitional origins in order to facilitate the contextualization of Russia's use of hybrid warfare in Ukraine. It will then outline the various aspects of hybrid warfare deployed by Russia in Ukraine. After doing so, it will then move on to the paper's three goals: (1) to show how Russia's hybrid warfare exposed, and exploited, gaps in NATO's doctrine and methods of operation, (2) to review NATO's attempts to date, to adapt its doctrines and methods of operation in response to Russia's hybrid warfare, (3) to identify and evaluate additional ways in which NATO could adjust to this form of aggression, and (4) to consider ways in which Canada has and could contribute to these efforts.

In conclusion, this paper argues that Russia's use of hybrid warfare has indeed exposed gaps within current NATO doctrine and methods of operation in the following ways: 1) hybrid warfare does not easily lend itself in all cases to fit squarely within the key NATO articles (V and VI), as it largely operates below the threshold of attribution, and therefore cannot provoke or allow for a collective military response or defence; 2) NATO lacks nimbleness and flexibility in responding to this new form of aggression, both operationally as well as within the North Atlantic Council decision making structure; 3) NATO defence spending does not necessarily match what is required for a hybrid warfare defence strategy; 4) hybrid warfare actors knowingly

explore. Some examples of the academic literature that debates and challenges the novelty and/or usefulness include, but are not limited to: Kofman, and Rojansky.. "A Closer look at Russia's Hybrid War". *Kennan Cable.* April 2015; Popsecu, Nicu. "Hybrid tactics: neither new nor only Russia." *European Union Institute for Security Studies*. January 2015; Deep, Alex. "Hybrid war: old concept, new techniques." Small Wars Journal. March 2015; Charap, Samuel. "The Ghost of Hybrid Warfare." *Global Politics and Strategy.* November 23 2015; Biscop, Sven. "Hybrid Hysteria." *Security Policy Brief*. No. 64. June 2015.

[3] Frier, Nathan. "Hybrid Threats and Challenges: Describe… Don't Define." *Small Wars Journal.* December 2009.

and strategically uses non-violent civilian means and methods of operation, thus reducing NATO's ability to have a full and successful defence or deterrence against it.

This paper will recommend that the Alliance must not only focus on reassurance measures for Allies (as was set out at the 2014 Wales Summit), but also focus on deterrence and resilience measures to this form of aggression. The areas in which NATO should continue and/or improve its strategic, policy and/or operational counter-measures to combat hybrid warfare are the following: 1) endorse deeper and more consistent cooperation with the European Union (EU) in the promotion of good governance and social cohesion within countries and beyond the institutions borders; 2) create a joint database and early warning system with the EU to flag countries that are particularly vulnerable to hybrid warfare; 3) improve intelligence sharing and gathering within the Alliance, as well as with the EU; 4) redefine defence spending and procurement to reflect hybrid warfare threats; 5) address the lack of doctrine against hybrid warfare; and 6) improve operational and structural nimbleness.

Finally, a caveat this paper recognizes is the issue surrounding Ukraine's non-membership status within the Alliance. Although the Alliance and Ukraine share a historically important and positive strategic partnership through the Partnership for Peace Programme, the hybrid warfare attack on Ukraine and NATO's response to such a scenario would have likely been very different had it been perpetrated against an actual member state.

2.0 Defining Hybrid Warfare and the Use of Hybrid Warfare in Ukraine

Since the beginning of the conflict in Ukraine, the concept "hybrid warfare" has become somewhat of a *buzzword*, as its use has been increasingly widespread by media and news agencies, the academic community, and NATO to describe Russia's actions and methods of operation in Crimea and the Donbas area. Despite the recent popular (re)deployment of the term hybrid warfare, the concept itself is not new. Although the concept is not new, it is important to note that the exact definition of hybrid warfare has been debated among the academic and security communities. To facilitate this papers consequent discussion on Russia's use of hybrid warfare in Ukraine, this section will first define the term hybrid warfare through exploring the central milestones of its theoretical and definitional origins. This section aims to do two things: 1) demonstrate how hybrid warfare as a concept differs from and is theoretically and operationally novel compared to other commonly used terms such as, compound warfare (wars that include regular and irregular or asymmetrical components under unified direction[4]) and 2) to contextualize Russia's use of hybrid warfare in Ukraine for the remaining discussion. The second half of this section will explore the various specific aspects of hybrid warfare in the context of Russian aggression in Ukraine. This portion will attempt to narrow down which aspects of hybrid warfare have been of particular importance or significance in relation to the situation in Ukraine.

2.1 - Defining the concept hybrid warfare

Hybrid warfare, hybrid threats, and hybrid aggression have been concepts used to describe the unprecedentedly complex and tailored integration of a whole-of-spectrum approach to warfare in the 21st century. Mark Galeotti, a leading expert of Russian security issues and

[4] Hoffman, Frank. "Hybrid Warfare and Challenges." JFQ issue 52 (1). 2009. ; Hoffman, Frank. "Hybrid vs. Compound." *Armed Forces Journal*. October 2009.

hybrid warfare studies has stated it may be "less of a new way of war so much as a way of fighting war in the new world – it is the world that has changed, not so much the ideas and tactics". [5] This form of warfare places military operations "back in the toolkit" and instead allows aggressors to fuse a combination of diplomatic, intelligence, militaristic, economic and humanitarian means, in a battle space that is no longer limited to the direct immediate physical area (i.e., the home front, the regional, the international, and the cyber).[6] As the discussion below will show, hybrid warfare is about the blending and blurring of multi-modal war forms in a combination of increasing frequency and lethality that concepts such as, compound wars, cannot fully and deeply grasp under their definition.[7]

To discuss hybrid warfare is to revert to the roots of Clausewitz notions of war. Clausewitz importantly reminds us "war is merely the continuation of policy by other means"[8] – war is a means to an end, not an end in and of itself, it is a tool upon which the act of force can compel one's enemy to do as is desired of them. Clausewitz distinguishes between two types of warfare: the first maintains the objective to defeat an enemy army and conquer its territory, the second maintains the objective to achieve desired political goals by exhausting the enemy's forces, but without intending for a conclusive military victory and/or the conquest of territory. [9] This second type of warfare, the type that is more indirect, can be viewed as the fundamental logics to modern day hybrid warfare.

In 2002, Major William Nemeth was one of the first to use the term hybrid warfare, as a way of outlining a "society-specific way of warfare".[10] He did so in the context of the 1994-1996 Chechen war, to which he referred to as the "flexible, half regular, half irregular warfare" that relied on conventional arms, methods of terrorism and organized crime, and irregular warfare. [11] Nemeth argued that the Chechens successfully deployed systematic and focused fusion of elements of Western and Soviet military doctrines, with decentralized operational guerrilla tactics (that included psychological and informational operations) and the use of modern communications technology to closely coordinate themselves in real-time. [12]

Nathan Frier, senior associate, in the International Security Program at the Centre of Strategic and International Studies, has also contributed to defining the term hybrid warfare. In the 2005 National Defence Strategy, Frier introduced the 'quad chart' to examine what he termed the new "hybrid norm". [13] This quad chart includes four threats or challenges: traditional,

[5] Manea, Octavian. "Hybrid War as a War on Governance: Interview with Mark Galeotti". *Small Wars Journal*. August 19 2015.

[6] Manea, 2015; Hoffman, Frank. "Hybrid vs. Compound." *Armed Forces Journal*. October 2009.

[7] Hoffman, Frank. "Hybrid Warfare and Challenges." JFQ issue 52 (1). 2009. ; Hoffman, Frank. "Hybrid vs. Compound." *Armed Forces Journal*. October 2009.

[8] Clausewitz, *On War*.

[9] Clausewitz, *On War*.

[10] W. J. Nemeth, "Future War and Chechnya: A Case for Hybrid Warfare". *Naval Postgraduate School California*. June 2002; Racz, Andras, "Russia's Hybrid War in Ukraine". *The Finnish Institute of International Affairs*. 2015.

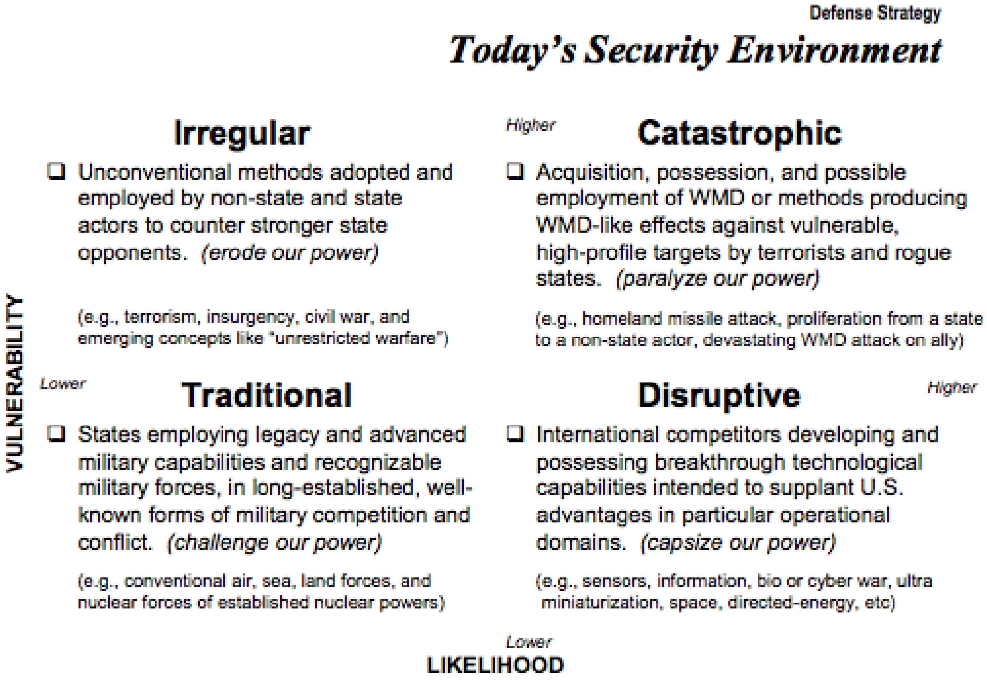
[11] Nemeth, 2002., Racz, 2015.

[12] Ibid.

[13] The National Defense Strategy of the United States of America. March 2005.

irregular, catastrophic terrorism and disruptive. [14] According to Frier, a hybrid actor would have to deploy a combination of two or more of these threats, allowing them to negate a traditional military superiority. Frier's quad chart is extremely useful when exploring the definition of hybrid warfare. As mentioned, the novelty of the term is contested and debated, and Frier's concrete definitions of each of the four threats allow the examination of differences between irregular warfare and hybrid warfare (Figure 1). This further clarifies that hybrid warfare is not simply another name for irregular warfare. Indeed, irregular warfare tactics may be one component of hybrid warfare but they are most certainly not the sole component.

FIGURE 1: Frier's Quad Chart[15]



Defense Strategy

Today's Security Environment

Irregular

❑ Unconventional methods adopted and employed by non-state and state actors to counter stronger state opponents. *(erode our power)*

(e.g., terrorism, insurgency, civil war, and emerging concepts like "unrestricted warfare")

Catastrophic

❑ Acquisition, possession, and possible employment of WMD or methods producing WMD-like effects against vulnerable, high-profile targets by terrorists and rogue states. *(paralyze our power)*

(e.g., homeland missile attack, proliferation from a state to a non-state actor, devastating WMD attack on ally)

Traditional

❑ States employing legacy and advanced military capabilities and recognizable military forces, in long-established, well-known forms of military competition and conflict. *(challenge our power)*

(e.g., conventional air, sea, land forces, and nuclear forces of established nuclear powers)

Disruptive

❑ International competitors developing and possessing breakthrough technological capabilities intended to supplant U.S. advantages in particular operational domains. *(capsize our power)*

(e.g., sensors, information, bio or cyber war, ultra miniaturization, space, directed-energy, etc)

Retired U.S. Colonel Jack McCuen further developed Nemeth's theory and concept of hybrid warfare in 2008. McCuen defines hybrid warfare as:

> *"full spectrum wars with both physical and conceptual dimensions: the former, a struggle against an armed enemy and the latter, a wider struggle for, control and support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community."*[16]

Importantly, McCuen contributes that hybrid wars are fought on, "three decisive battlegrounds: within the conflict zone population, home front population and international community" and that hybrid warfare requires simultaneous success on all these fronts. Therefore, this is

[14] Ibid.

[15] Freier, Nathan. "Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context." *Strategic Studies Institute*. May 2007.

[16] McCuen, J.J. "Hybrid Wars". *Military Review*. March-April 2008.

significantly different from conventional warfare or compound wars. Conventional warfare tactics play a large role, in that the first goal is to defeat the enemy forces, then secure control over the territory, and then start state-building exercises that include the entire society and the non-combatants.

Finally, retired Lieutenant Colonel Frank Hoffman who now is a Senior Research Fellow with the Institute for National Strategic Studies is one of the leading academic experts on hybrid warfare. His work focuses on the case study of Hezbollah as a successful hybrid actor against the Israel Defence Forces and Iraq's *Fedayeen* in 2003. His definition of hybrid warfare is currently the most widely accepted and quoted definition of the term:

> *"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 battle space to achieve synergistic effects in the physical and psychological dimensions of the conflict. These effects can be gained at all levels of war"*[17]

Hoffman argues that the term "hybrid" captures both the organization and the means (form and application), allowing the demonstration of fused multi-modal and context specific tactics. In addition, much of Hoffman's work is valuable because it explores how hybrid warfare differs from compound warfare, which combine "regular and irregular components and fight simultaneously under unified direction". [18] The degree of difference between the concepts of hybrid warfare and compound warfare is highly debated among academics, and is one of the more frequently used points to challenge the assertion that the concept of hybrid warfare is useful or novel. Hoffman argues that the regular and irregular components of compound wars occur in different theatres or in different formations. The irregular components usually facilitate the ability of victory for the regular forces in a decisive battle. In this sense, in a compound war, there is a sort of division of labour between the irregular forces/tactics and regular forces/tactics. In contrast, hybrid wars use components that can become blurred into one force in the same battle space, creating a layering of threats. The multi-modal activities used in hybrid warfare can be conducted by separate units or by the same unit – they do not have to be conducted solely by irregular forces. Hybrid actors seek victory by the fusion of a multitude of political, military, economic, social and informational means using conventional, irregular, catastrophic, terrorist and disruptive/criminal methods to achieve their political objectives. When looking back to the definition of irregular and regular war as defined under Frier's quad chart (which are also commonly accepted definitions of the terms), they are limited to violent means. Consequently, another difference between compound wars and hybrid wars is that, unlike compound wars, which emphasize and use violent means of war forms, hybrid warfare importantly includes violent, non-violent, and civilian means to achieve their ends. In conclusion, Hoffman argues,

[17] Hoffmann, Frank. "Conflict in the 21st Century: The Rise of Hybrid Wars", *Potomac Institute for Policy Studies, Virginia*, Dec 2007.
[18] Hoffman, 2007.

compound wars (or any other current definitions of warfare) do not grasp the low-level synergistic blurring, complexity, fusion and fluidity of modes of war as the definition of hybrid warfare does.

The remainder of the discussion on defining the concept hybrid warfare will now turn to more recent work and definitions – the work done by General Valery Gerasimov, Chief of the General Staff of the Russian Federation, and NATO's current working definition of the term. In 2013, General Gerasimov published an essay on the topic of "non-linear warfare" (an interchangeable name for hybrid warfare). This essay, or as it is now referred to the Gerasimov Doctrine, has received considerable attention, especially post Russian aggression in Ukraine, from Western academics and Governments as many view it to be a key insight into the future of Russian military planning and doctrine. Gerasimov's essay refers to the Arab Spring as a key, modern example of the changing nature of warfare. He stresses that conflicts are actually means to political ends, and that non-military means (diplomatic, political, economic and other non-violent means) may actually be far more effective than military means, and thus Russia must now look to and emphasize these non-military means. General Gerasimov foresees concealed, non-open use of force, such as, paramilitary and civilian insurgent units who deploy and rely on asymmetrical and indirect means of warfare. He continues to note that relevance and importance of the information battle space, such as the use of drones, targeted attacks on critical infrastructure, and coordination of civilian insurgents in real-time, will also continue to grow. In contrast to compound wars, he argues that regular forces ought only to be used for action during later phases of the conflict and done so under the disguise of peacekeeping or humanitarian aid.

A *NATO Review* video posted on July 3 2014 was the first official NATO media release to use the term hybrid warfare in the context of the situation in Ukraine.[19] A few months later in September 2014, during the Wales Summit, the term hybrid warfare was used on several occasions to describe Russian aggression in Ukraine that had occurred earlier that year in March 2014. Although currently, there is no Alliance consensus on one single precise definition of the term and no official NATO doctrine or Strategic Concept on hybrid warfare, since the Wales Summit, NATO has used the following definition several times in public statements and practice exercises:

> *"Hybrid warfare is where a wide range of overt and covert military, paramilitary and civilian measures are employed in a highly integrated design. The adversary tries to influence influential policy-makers and key decision makers by combining kinetic operations with subversive effort. The aggressor often resorts to clandestine actions, to avoid attribution or retribution."* [20]

Although the Global Affairs Canada and the Department of Defence[21] has not yet produced

[19] North Atlantic Treaty Organization. "A hybrid war – a hybrid response?". July 2014.

[20] North Atlantic Treaty Organization, Wales Summit, September 2014.

[21] Interview with Global Affairs Canada Officials, January 12, 2016; Interviews with Officials from the Department of Defence, March 4 2016.

an official definition of hybrid warfare, the officials stated that their internal working definition of hybrid warfare is in accordance with NATO's and they maintain that the term itself is useful. Much like the above NATO definition of hybrid warfare, officials at Global Affairs Canada and the Department of Defence emphasize that hybrid actors skillfully and carefully operate on the fine line that is just below the threshold of provoking a military response from their opponent. In addition, the officials add that the Russian model of hybrid warfare operates on a much more fluid continuum from non-military, military and civilian means, that is of an unprecedented and refined level and that terms such as asymmetrical warfare or compound wars cannot grasp or fully explain.

During an interview with Global Affairs Canada[22], officials insightfully noted that while their department finds the term hybrid warfare useful, a major challenge in concluding a precise definition of the concept lies within the fact that hybrid warfare is always changing and is tailored by the hybrid actor to the context at hand. This means, that in each case or example of hybrid warfare, different means and methods of war will be deployed and in different manners and capacities – there is no one precise list of components or criteria to hybrid warfare as it is fluid and complex. Nathan Frier reiterates this awareness by suggesting it may be more helpful to describe and analyze, not define the concept – what is critical in understanding the waging of war in a modern world, he notes, is "not the 'one time' precision in defining hybrid warfare but instead perpetuation of an active dialogue on a new and expanding universe of complex defence-relevant challenges." [23] This is important to keep in mind when summarizing the above discussion to a common and concise definition of hybrid warfare.

It is also important to note that the definitions have evolved over time, beginning with Bill Nemeth's definition to NATO's current working definition of how hybrid warfare was used in Ukraine in 2014. The older academic examples of hybrid warfare (Chechnya, Hezbollah, actors in the Arab Spring, etc.) also seem to limit hybrid actors to non-state actors (although their theoretical definitions do include the state as a possible hybrid actor), whereas in the situation in Ukraine, it was a state actor who deployed hybrid tools. In addition, previous academic examples seem to imply that hybrid tactics were used against opponents who were stronger or more powerful than them, in order to maintain a tactical and strategic edge. This is certainly not the case in Ukraine, as Russia, the more powerful actor, used hybrid tools against a smaller weaker actor in comparison. The use of hybrid warfare by a powerful state actor is a significant development. The advantage for Russia in doing so was that it allows them to reduce their exposure to international political and legal attribution and shape a narrative within the context of information/psychological warfare.

Despite the slightly differing above definitions of hybrid warfare (while keeping in mind its transformation and evolution) there has still remained a broad coherency: it is a form of warfare that includes a range of multi-modal activities that can be conducted by state or non-state actors. Emphasis is placed on simultaneous and unprecedented fusion of a variety of means such as political, military, economic/financial, social and informational using conventional, irregular, catastrophic, terrorist and disruptive/criminal methods to achieve political objectives. The hybrid

[22] Interview with Global Affairs Canada Officials, January 12, 2016.

[23] Freier, Nathan. "Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context." *Strategic Studies Institute.* May 2007.

actor fuses these means and methods in a way that is tailor-made to the context at hand. As there is a blurring between war forms, there is also a blurring between combatants and non-combatants, resulting in a whole of society integration into the conflict. This section introduced the concept hybrid warfare and the evolution of the concept's definition for contextualizing Russia's use of hybrid warfare in Ukraine and to also demonstrate the degree to which the term hybrid warfare is theoretically and operationally novel and distinct from similar terms such as, compound wars.

2.2 ***Aspects of hybrid warfare in Ukraine***

The situation in Ukraine has drawn particular attention from academics and security communities, such as NATO, for the reason that the operations perpetrated against Ukraine by Russia were not designed as a simple traditional kinetic military operation. Instead, several military and non-military means and methods, discussed above, were used to achieve Russia's objectives in Crimea and Eastern Ukraine. Hence, this section will be a discussion of the various aspects of hybrid warfare that were present and deployed by Russia in Ukraine. What is interesting when examining the various sub-categories of hybrid warfare used in Ukraine is that it becomes apparent the techniques used are inextricably linked and mutually reinforcing. This is the key aspect in hybrid warfare. Isolated, these events may appear to be forms of previously defined or 'regular' types of warfare. However, their true significance and destructive power occurs when examined as a whole; the low-level detailed inter-mingling and interaction of these forms of warfare, and consequently how they come together in conjunction to form a coherent political strategy of the adversary. This section will demonstrate how, for example, cyber-attacks early on in the conflict facilitated and provided the necessary intelligence for certain military actions or for the spreading of certain pieces of disinformation. Thus, when the various elements of hybrid warfare are analysed in conjunction with one another, it deteriorates a state's domestic sovereignty (the ability of the public authority to exercise effective control within the borders of their own polity).

The following section is divided into four sub-categories or aspects of hybrid warfare found in the battle space: overt and covert military presence, information warfare, cyber warfare and economic warfare. As the conflict is still very much evolving, certain events and information are not or cannot always be corroborated or proven during the early and ongoing stages of conflict, therefore (and in the interest of this paper's scope), this section will only explore the most compelling and widely accepted pieces of evidence supporting each category.

Overt and Covert Russian Military Presence

The situation in Ukraine is especially interesting from a military perspective because of events that occurred during the initial phases of conflict (circa late February until early-mid March 2014). During these events foreign unmarked military units using high-tech Russian uniforms and equipment took over key Ukrainian political targets: army bases, administration and government buildings (such as the Parliament building, the Supreme Council of Crimea, mayoral offices, etc.), police stations, and airfields, with overwhelming success and largely without a single shot fired.[24] The operation was highly sophisticated in terms of the way it was

[24] Weiss, Michael, et al. "An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine" *The Institute of Modern Russia*. 2015.; International Centre for Defence Studies. "Background Paper: Russia's Actions against Ukraine." June 10 2014.

planned and executed. By doing so, as part of its strategy Russia was able to exploit popular pro-Russian support and by mobilizing this support it was able to erode Kyiv's influence and power through limited non-kinetic attacks on these key political targets. The political, cultural and social context of Crimea led itself well to the application of hybrid warfare. In addition, the fact that the attackers were dressed without insignia or in civilian clothing, severely limited the potential of the Ukrainian government to use force against them.[25] After this initial take-over was accomplished, alleged "self-defence" Russian forces "stood behind" Ukrainian separatist forces, allowing them to take over the more traditionally kinetic aspects in the conflict. [26] Together, these strategies enabled avoiding early and immediate attribution from Ukrainian (or international) forces, thus contributing to the success of the Russian hybrid offensive. This sub-section will explore the heavily documented evidence of the presence of Russian troops, often called "polite people" or "little green men", and the presence of Russian grade military equipment used by these unmarked troops.

On February 22, 2014, it is documented that *Spetsnaz* forces (Russian Special Forces Units) from the 45th Guards Separate Reconnaissance Regiment of Russian Airborne Unit, were put on high-alert, and within five days were deployed to the 810th Independent Naval Infantry Brigade Russia's Black Sea naval base in Sevastapol.[27] On February 27, 2014, footage shows unmarked military units using high-tech uniforms and equipment, which Finnish intelligence later concluded to be the 45th Regiment, to capture the Crimean Supreme Council. [28] In the following days, and with aid from the 810th Brigade, other *Spetsnaz* units (431st naval *Spetsnaz*, the 10th Brigade, the 25th Brigade, the 3rd Brigade, the 16th Brigade, and the 25th Brigade), and pro-Russian private security firms, the Simerfopol airport and other key political buildings were captured. [29]

In addition to the footage and intelligence gathered on these forces, NATO Supreme Allied Commander General Breedlove noted the units that targeted key Ukrainian government buildings in coordinated systematic strikes (quickly surrounding the area with roadblocks and barricades, acted under direction from a few key group leaders), handled weapons and military equipment (coordinated use of tear gas and stun grenades) in a disciplined and professional behaviour that is consistent with an organized, trained military force under a strong chain of

[25] Racz, 2015.

[26] Reuters. "Putin Press Conference with Vladimir Putin". March 2014.; Weiss, Michael, et al. "An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine" The institute of Modern Russia. 2015: International Centre for Defence Studies. "Background Paper: Russia's Actions Against Ukraine."

[27] Perry, Bret. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations." *Small Wars Journal.* August 14 2015.

[28] International Centre for Defence Studies. "Background Paper: Russia's Actions against Ukraine."; https://www.youtube.com/watch?feature=player_detailpage&v=ztuHuSw_4zw and http://www.youtube.com/watch?v=qPHNiTZe_wI; Russian Special Troops Enter Inside in Crimea Parliament, https://www.youtube.com/watch?v=DUH-A3IF3h0. Rogin, Josh, "Exclusive: Russian 'Blackwater' Takes Over Ukraine Airport". *The Daily Beast Company*. February 2014; Alexey Nikolsky, "Little, Green, and Polite: The Creation of Russian Special Operations Forces," in *Brothers Armed: Military Aspects of the Crisis in Ukraine*. 2014.

[29] Perry, 2015.; Rogin, 2014; Galeotti, Mark. "The rising influence of Russian special forces" *IHS Janes Intelligence Review. 2014.*

command (rifle muzzles were pointed down, fingers were not on triggers), and did not exhibit behaviour of a recently formed spontaneous militia.[30] This is especially apparent when compared in a side-by-side analysis of video footage of Ukrainian separatist forces conducting sieges of government buildings on their own, who appear "incompetent and undisciplined" – a common trademark of quickly trained, unorganized irregular forces operating under a loose command system.[31] In addition, expert analysis of the actual equipment used by the troops appearing in Crimea and Eastern Ukraine were of Russian military grade. The forces carried a modified SVD-S sniper rifle that is used only by Russian and Armenia troops; the forces wore elements of the modern Russian Ratnik Future Solider System (which include specific types of protective goggles, body armour and unique communication systems); signature Russian weapons such as grenade launchers.[32]

The mysterious Vostok Battalion[33], another unit of elite special forces, was also frequently sighted during the earliest battles in Ukraine.[34] Notably, they were present during the siege of the Donestk Sergey Prokovfiev International Airport in Eastern Ukraine on May 26, 2014.[35] Prior to this Battalion's sightings, Ramzan Kadyrov, the leader of Chechnya and one of Putin's strongest allies threatened to send tens of thousands of "volunteers" to Ukraine to help the pro-separatist forces against the "junta" in Kyiv.[36] It was then, when men who claimed to be Chechen started to appear in these early frontline battles.[37] There is video evidence of members from this Battalion fighting in early battles in Donestk as well as rallies there, and acknowledging they had previously fought alongside other Chechens in Ukraine. [38] In addition, there were local Chechen reports that document the return of their fighter's bodies from Ukraine. [39] Once again, Russia's use of the Vostok Battalion as a proxy to fight on their behalf awards Russia the plausible deniability, or difficulties relating to attribution, that is a core element of hybrid warfare.[40]

[30] International Centre for Defence Studies, 2014;
North Atlantic Treaty Organization. "Who are the Men Behind the Masks?". *Supreme Headquarters of the Allied Powers Europe: General Breedlove's Blog*. April 2014.

[31] The Firearm Blog. "Comparative Weapon Analysis of Crimea Troops and Eastern Ukraine Militias." April 2014.

[32] International Centre for Defence Studies, 2014; Firearm Blog, 2014.

[33] Which suspiciously shares its name with another infamous GRU (the Russian Intelligence Service) controlled Special Forces group that was disbanded in 2008. This Battalion was made up of mainly Chechen fighters who played a key role in the past 15 years in South Ossetia and the Caucauses. Weiss, 2015.

[34] Weiss, 2015.

[35] Perry, 2015.

[36] Weiss, 2015.

[37] Ibid.

[38] Weiss, 2015; "Ukraine Liveblog Day 104: Klitschko Receives Cool Reception on Maidan". *The Interpreter*. June 1 2014; Backzynska, Gabreila. "More foreign fighters break cover among Ukraine separatists". *Reuters*. June 1 2014.

[39] Weiss, 2015; Perry, 2015

[40] Galeotti, Mark. "The rising influence of Russian special forces" *IHS Janes Intelligence Review*. 2014; Rosen, Armin. "The Ukraine Crisis is entering a dangerous new phase." *Business Insider*. June 2014.

There has also been documented evidence that verifies the presence of Russian tanks in Donestk, Makiivka and Slavyanks, at the hands of pro-Russian separatists beginning in early June.[41] NATO analysed the video footage of these tanks and determined them to be Russian grade.[42] NATO noted that the vehicles were stripped of all identifiable symbols and numbers (a tactic used in Crimea and then used in Eastern Ukraine) and the camouflage the tanks were painted with was not consistent with the camouflage used by the Ukrainian army (therefore voiding the argument that all tanks were simply captured from Ukrainian military stockpiles or from attacks on military bases). NATO satellite imagery also shows Russian tanks on the border of Ukraine, and a few days later shows three out of eight of those tanks being loaded onto transporters (trucks normally used to move tanks) on the Russian side of the border, likely "indicating their imminent movement".[43] One day later Ukrainian officials reported that 3 main battle tanks and several armoured vehicles crossed the border at Dovzhanskyy, which at the time was under the control of pro-Russian separatists. [44]

Cyber Warfare

While jamming communication and radio signals has been a long-standing practice in warfare, cyber space has opened up a vast number of alternative possibilities to influence a conflict's outcome, often in a manner that can be easily covered up to avoid attribution. Cyber attacks are a key element in the contribution of waging hybrid warfare. They are being used at an increasingly unprecedented level to attack critical infrastructure in order to disrupt communication and information flows, and to gain intelligence on the adversary's intentions and actions. NATO has identified cyber warfare (and information warfare) as key and new highly devastating components. [45] However, the issue with cyber warfare is that it can be extremely difficult, if not sometimes impossible, to confirm who the attacker is (referred to in the literature as problems of "attribution"). As stated, this is highly beneficial and works in favour for a hybrid actor (as Russian cyber operations in Georgia and Estonia have previously shown), as it allows them to operate below the threshold of attribution, which, as discussed in the previous section, is an important element when defining hybrid warfare as a concept. This section will explore the incidents of cyber warfare that can more concretely place Russian or pro-Russian forces as the attacker(s). The significance of these cyber attack examples is that they operate in conjunction with other elements of warfare, providing an important intelligence advantage to the military component and/or the information warfare component of Russia's hybrid warfare strategy.

Beginning in November 2013, before the build-up of troops on the Crimean border, Russian hacker groups (pro-Russian hacker group CyberBerkut claimed responsibility for the

[41] The Interpreter. "T-64s Appear Between June 12 and June 18."

[42] Supreme Allied Headquarters of the Allied Powers of Europe. "NATO Releases Imagery: Raises Questions on Russia's Role in Providing Tanks to Ukraine." *North Atlantic Treaty Organization.* June 14 2014; The Interpreter. "T-64s Appear Between June 12 and June 18."

[43] Supreme Allied Headquarters of the Allied Powers of Europe. "NATO Releases Imagery: Raises Questions on Russia's Role in Providing Tanks to Ukraine." *North Atlantic Treaty Organization*. June 14 2014.

[44] Ibid.

[45] North Atlantic Treaty Organization. "Cyber Defence" February 16 2016; North Atlantic Treaty Organization. "Hybrid War – does it even exist." *NATO Review Magazine*; McCaney, Kevin. "Russia's Hybrid warfare tactics gain upper hand in Ukraine." *Defense Systems*. March 24, 2015.

attacks) began to execute Distributed Denial of Service attacks (DDoS) on critical government websites, rendering them unusable or destroying or changing their content.[46] This was seen to be the beginning of the mounting disinformation campaign against Ukraine perpetrated by Russia.[47]

In February 2014, the telecoms firm Ukrtelecom stated that armed, unmarked and highly skilled men, as described in the above sub-section "overt and covert Russian military presence" to be Russian Special Forces Units, broke into Ukrainian telecommunications facilities in Crimea and tampered with fibre optic cabling.[48] As mentioned, these actions also facilitated a first step on the front of information warfare, as Ukrainian television channels were shut down and then replaced by Russian ones. The tampering with the fibre optic cables also shut down local telephone services, Internet systems, and vital communication services such as, first aid, fire and rescue, and law enforcement.[49] This hindered the ability for the Ukrainian government to communicate to the people in Crimea regarding the unfolding situation and hindered their ability to effectively communicate with and/or mobilize Ukrainian troops in that area.[50]

The pro-Russian hacker group CyberBerkut launched another "prolonged" DDoS attack against NATO and Ukrainian media outlets in March 2014. [51] Also in March 2014, only 72 hours after Russian troops entered Crimea and tampered with telecommunications towers and fibre optic cables, up to 700 mobile phones of Ukrainian members of parliament and government officials were disrupted.[52] At this point, the head of the Ukraine's Security Services stated that the country had been facing a serious cyber attack over the last few days. [53] During this time, security experts stated that they believed these cyber attacks were part of a wider strategy that would allow Russian military forces to isolate the region, which in fact later turned out to be true. [54] As mentioned in the introduction to this section, it is apparent that cyber attacks were used in conjunction with information warfare and covert and overt military presence to achieve Russia's political objectives of securing the peninsula of Crimea back into the Russian federation.

[46]Maurer, Tim and Janz, Scott. "The Russian-Ukraine Conflict: Cyber and Information Warfare in a Regional Context." *The International Relations and Security Network*. October 17 2014; "Hromadske.tv under DDoS-attack." Ukrainian non-governmental Organization: Institute of Mass Information. November 26 2013; Stone, Jeff. "Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyber warfare Against Ukraine." *International Business.* December 17 2015.

[47] Maurer and Scott, 2014.

[48] Vegue-Martin, Tony. "Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it". *CSO Online*. April 24, 2015; Finkle, Jim, and Polityuk, Pavel. "Ukraine says communications hit, MPs phones blocked." *Reuters*. March 4 2014

[49] "Ukrtelecom's Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea." *Ukrtelecom*. February 28 2014.

[50] Vegue-Martin, 2015.

[51]"DDoS Attacks Hit NATO, Ukrainian Media Outlets". Information Week: Dark Reading. March 17 2014; Tweet from Oana Lungescu, NATO Spokesperson.

[52] Finkle and Polityuk, 2014.

[53] "Crimean – the Russian Cyber Strategy to Hit Ukraine." *InfoSec Institute.*

[54] Ibid.

Later in the year, during the Ukrainian elections in October 2014, Ukraine's Security Services discovered the presence of Russian malware in the Central Election Commission computer systems. The goal of this malware was to tamper with data collected on the results of the election. This was a shocking and frightening moment for Ukrainians as it revealed how close Russian hackers had come to sabotaging the election results and eventually lead to the erosion of public trust in voting mechanisms.[55]

Throughout the conflict, updates from the both the Organization of Security and Co-Operation Europe (OSCE) and IHS Jane's 360, reported that Russian special forces units used high-powered microwave systems to jam the communications and reconnaissance assets of the Ukrainian armed forces and disabled the surveillance unmanned aerial vehicles operated by ceasefire monitoring teams from the OSCE in Eastern Ukraine.[56]

Finally, in January 2016, it was revealed that a massive cyber attack had occurred on Ukraine's largest airport (Boryspil). [57] Authorities stated that the control centre of the malware found in the IT network of Kyiv's main airport was in Russia. This malware was also similar to that found in another cyber attack in December 2015 when three major power firms lost power, causing outages across the country. A US cyber intelligence firm found that this malware could be traced back to Moscow and was part of a "Russian group's ongoing hacking campaign".[58]

Information/Psychological Warfare

A key element in Russia's hybrid warfare toolkit is the "weaponization" of information, or use of information warfare (the management of information and communication technology). By successfully mastering the weaponization of information, the actor is allowing for a "qualitatively more intense and powerful non-material", non-military form of warfare – thus a psychological component of warfare.[59] Information warfare operations include a mix of propaganda, disinformation, diplomatic duplicity, media manipulation, or disseminating outright falsehoods designed to confuse and divide opinion within the targeted state and other adversaries.[60] Together, they create and contribute a powerful psychological component to the conflict.[61] It has been argued that Russia's current use of information warfare/psychological warfare within the context of Ukraine surpasses the limits drawn during the Cold War.[62]

[55] Maurer, Tim. "Cyber Proxies and the Crisis in Ukraine." *NATO CCD COE Publications*, Talinn, 2015; Vegue-Martin, 2015.

[56] "Latest from OSCE Special Monitoring Mission (SMM) to Ukraine based on information received as of 18:00 (Kyiv time), 3 November 2014" Organization for Security and Co-Operation in Europe. November 4 2014. ; "OSCE drone jammed over eastern Ukraine." *Ukraine Today*. November 6 2014.

[57] Bolton, Doug. "Ukraine says major cyberattack on Kiev's Boryspil airport was launched from Russia" *The Independent*. January 18 2016.

[58] Bolton, 2016.

[59] Weiss, 2015.

[60] Weitz, Richard. "Countering Russia's Hybrid Threats". *Diplomaatia*. November 2014.

[61] Gosu, Armand, and Manea, Octavian. "Russian Pyschological Warfare." *Black Sea in Access Denial Age*. September 11 2015.

[62] Gosu, and Manea, 2015. This is important to note because it contributes to the novelty of hybrid warfare in the 21st century as used by Russia. Opponents of hybrid warfare argue the means and methods

For Moscow, controlling the means of mass communication so that their narrative went unchallenged was crucial in constructing and furthering an appearance of legitimacy both at home and abroad. Russia's disinformation and propaganda campaign as well as control over information allows for several key aspects of plausible deniability and psychological interference to be realized: it concealed Russia's true objectives; it confused the enemy and the average media consumer/viewer; it made it more difficult for analysts to estimate the actual size of Russia's military presence in the battle space; it allowed for a range of flexibility when choosing methods to exacerbate the conflict; and created diplomatic cover and solutions for Russia's covert military and foreign policy activities. [63] Within Ukraine, Russia effectively conducted information operations by leveraging television stations, newspapers and the Internet to spread Russian approved narratives. NATO Supreme Allied Commander of Europe stated that the most impressive and newest addition to hybrid warfare, in the context of Ukraine, was the use of information tools to create an extremely powerful and influential false narrative. [64] This section will look at the most prevalent occurrences of information/psychological warfare (propaganda, disinformation, diplomatic duplicity, media manipulation, or disseminating outright falsehoods designed to confuse and divide opinion within the targeted state and other adversaries) conducted by Russia viewed as a contributing element within the wider scheme of hybrid warfare.

Television is the most popular source of information within Russia. There are three television channels: Channel One, Russia One, and NTV, that maintain a nationwide and regional reach. Channel One and Russia One are owned by the Government, and NTV is owned by the state-controlled energy giant Gazprom. [65]As mentioned in the "cyber warfare" sub-section, Ukrainian news outlets in Crimea were shut down early on in the crisis and television transmitters seized by the pro-Russian Crimean administration and replaced by Russian state-owned broadcasts. [66] An Organization for Security and Cooperation representative from the Freedom of Media department spoke out against the closure of the Ukrainian news outlets and the attacks on journalists in Crimea, stating that these actions "paved the way for the worst kind of propaganda". [67] A prominent news anchor for the Kremlin funded RT channel, resigned after it became apparent Russia was using the media as a means of information warfare against Ukraine and the West. She disagreed with RT's support for "military intervention in Ukraine" and the network's "whitewashing of Putin's actions" there. [68]

Thus, it is hardly a surprise that since the Ukraine crisis began, Russian state media has intensified the pro-Kremlin and nationalistic/anti-Western attitudes of their broadcast content. Much of the rhetoric found on these broadcasts dispels those in power in Kyiv as fascists, Nazi

of war fighting are not new – which this essay does not contest. However, what is novel is the speed, intensity and integration that the means and methods of hybrid warfare are now currently being used.

[63] Lasconjarisa, Guillaume, and Larsen, Jeffery. "NATO's Response to Hybrid Threats." *NATO Defense College*. 2015.

[64] McCaney, 2015.

[65] Ennis, Stephen. "How Russian TV Changed during Ukraine Crisis." *BBC News*. June 26 2015.

[66]Sukhov, Oleg. "The Media War Behind the Ukraine Crisis." *The Moscow Times.* March 11 2014.; Ostrovksy, Arkady. "Putin's Ukraine Unreality Show." *The Wall Street Journal.* July 28 2014.

[67] Sukhov, 2014.

[68] Ibid.

sympathizers illegitimate, and anarchic.[69] These media outlets argued that the Russian military intervention in Crimea was justified because Russian speakers were being persecuted and their protection was required.[70] BBC has reported that Russian controlled television coverage of the conflict in Ukraine employed "techniques of psychological conditioning designed to excite extreme emotions of aggression and hatred in the viewer".[71] A tactic often used by Russian controlled media is the fabrication or exaggeration of events for the cameras. One notable example of this was of a story run by Channel One, which reported an interview of a woman who claimed she had seen Ukrainian soldiers crucify a three-year-old boy on a billboard. The story was quickly exposed as false and was widely criticised, resulting in the eventual reluctant admission by Channel One that the story was indeed fictional.[72]

In addition, there has been a clear focus on the Ukraine conflict and other domestic Russian issues have been ignored because of this. An EU funded study found that Russia One's main news bulletin devoted over 35 percent of its airtime to Ukraine and only 1.3 percent to Russian social issues and health care. The study reports that Channel One's bulletins follow a similar form. [73]

Another prominent example of the disinformation campaign the Kremlin waged during the conflict in Ukraine was the spread of colourful conspiracy theories of the downing of the Malaysian airliner MH17 by the state-owned news agencies and Russian Defence officials. Some of the more popular Russian theories and explanations included: the flight MH17 was shot down by a Ukrainian Su-25 fighter jet; the flight MH17 was shot down in a botched attempt to assassinate President Putin whose Presidential plane had just passed the crash site a few hours earlier; and finally, pro Ukrainian forces launched a missile downing the plane. [74] A Dutch report on the investigation of the crash of the flight MH17 concluded the airplane was shot down by Russian-built anti-aircraft missiles launched from a 120 square mile radius south of the town of Snizhne (an area controlled by Russian-backed separatists at the time). However, a few hours before this Dutch report was released, a Russian state-owned company released their own report on the investigation that diverted all blame from Russia and asserted the plane was shot down by Ukrainian forces.

Finally, Russia was also waging information warfare on the Internet. A prominent example is the use of pro-Kremlin "professional trolls" (a person who deliberately posts messages and comments on Internet forums with the intent of provoking, upsetting and sowing

[69] Weitz, 2014.

[70]Sukhov, 2014.

[71] Ennis, Stephen. "How Russian TV uses psychology over Ukraine." *BBC News*. Feb 4 2015.

[72] Ennis, Stephen. "How Russian TV uses psychology over Ukraine." *BBC News.* Feb 4 2015.; "State-Run News Station Accused of Making p Child Crucifixion." *The Moscow Times*. July 14 2014

[73] Ennis, Stephen. "How Russian TV uses psychology over Ukraine." *BBC News.* Feb 4 2015.

[74] Nest, Daniel. "10 Outrageous ways the Russian Media Covered the Crash of MH17." Listverse. September 7 2015; Cullison, Alan. "Malaysia Airlines Flight MH17 Crash Illustrates Different Realities in Russia vs. West". *The Wall Street Journal.* July 22 2015.; Akkoc, Raziye. "MH17 airliner destroyed by Buk missile fired from eastern Ukraine, Dutch report confirms". *The Telegraph UK*. October 13 2015.

discord amongst readers). [75] These professional trolls were hired to post comments that further spread disinformation and confusion about the conflict in Ukraine. Recently, many of these professional trolls have come forward and have been interviewed by journals and news agencies such as, Radio Free Europe/Radio Liberty, the Telegraph, the Atlantic and the Guardian. In these interviews it was confirmed that employees were instructed each day to bombard social media sites such as, Twitter, Facebook, LiveJounral, vKontakte (the Russian equivalent to Facebook) as well as Western news agencies such as, the BBC, CNN, the New York Times and the Guardian with a given quota of pro-Russian narratives.[76] The former employees revealed the nature of some of their tasked topics: arguing there are NATO troops embedded in Ukraine; arguing the majority of Germans support Putin's policies and dislike Chancellor Merkel; conspiracies related to the death or Boris Nemstov and the Malaysia airline flight MH17; and other fake stories and events that foster a positive public image of President Putin.[77]

In his panel remarks at the 2016 Canadian Defence Association Institute's Annual Defence Conference, Former Canadian Ambassador to NATO, Yves Brodeur, noted that NATO lost control of the narrative, while Russia was extremely timely and talented at shaping it in their favour. Brodeur emphasized that the narrative during a conflict is extremely important, especially in the context of hybrid warfare. He argued that NATO must remain focused and reminded of the important of Strategic Communications in future "faceless conflicts". [78]

Economic Warfare

Deploying an economic component within a wider hybrid strategy can be particularly influential and destabilizing, especially in situations where countries rely on certain energy resources from the hybrid perpetrator, as is the case with Russia and Ukraine. Economic warfare can include: economic sanctions, the destabilisation of energy prices, the barring of physical access to energy resources, actions of transnational criminal organizations, and cuts in other vital commercial ties and trade.[79] As NATO notes, the annexation of Crimea and conflict in Eastern Ukraine are ultimately not about energy, but about power and achieving certain political objectives.[80] However, it is important not to overlook the role economic warfare has played in the conflict. In order to achieve its goals, Russia has utilized economic dimensions and pressures that further added to the destabilization of the situation in Ukraine – as all the components of hybrid warfare have contributed to.

[75] "Internet trolling as a hybrid warfare tool: the case of Latvia." NATO StratCom Centre of Excellence Publication.

[76] Volchek, Dmitry. "One Professional Russian Troll Tells All" *Radio Free Europe – Radio Liberty*. March 25 2015.

[77]Parfitt, Tom. "My life as a pro-Putin propagandist in Russia's secret 'troll factory'". *The Telegraph.* June 24 2015.; Volchek, 2015.; Sindelar, Daisy. "The Kremlin's Troll Army." *The Atlantic.* August 12 2014.

[78] Yves Brodeur, "Panel 3: Terrorism, Non-State Actors, and Faceless Conflict." CDAI Conference 2016.

[79] Davis, John. "Continued Evolution of Hybrid Threats." *The Three Swords Magazine*. 2015.; Weitz, 2014.

[80] North Atlantic Treaty Organization. "Russian-Ukrainian-EU gas conflict: who stands to lose most?" *NATO Review Magazine.*

Ukraine has suffered large economic losses as a result of Russia's aggression in the country. There has been roughly a seven percent loss in production since the occupation of Eastern Ukraine, 3 percent loss from foreign direct investment and Russian trade sanctions, which have cut Ukrainian exports to Russia by 70 percent.[81] Over 2014 and 2015 Ukraine's GDP contracted by approximately 16 percent.[82] It can be argued that this is a result of Russian aggression – the trade war, intermitted cut off from a much needed natural gas supply and threatening financial attack have all been factors.[83]

In addition to the losses in GDP leading to a highly deteriorated economic environment, citizens in both the European Union (the EU receives about 40 percent of its natural gas from Russia, half of which passes through Ukraine[84]) and Ukraine have begun to feel the impacts of Russia's energy blockade, especially during the below-freezing winter months. Until the conflict, Ukraine relied on Russia for half of its energy supplies to fuel its heavy industry and civilian needs. During the conflict Gazprom, the state owned energy giant, has intermittently decided to increase prices of natural gas or completely cut off Ukraine's gas supply.[85] This has severely limited Ukraine's ability to maintain energy security. A lack of energy security can expose a country to vulnerabilities because it hinders the country's capacity to provide basic needs to its citizens (such as heat during winter months), as well as fulfill its energy providing requirements to heavy industries and companies – both key components to maintaining efficient and effective domestic sovereignty through the provision of public goods.

This section has demonstrated how various sub-categories of hybrid warfare – overt and covert military operations, cyber warfare, information/psychological warfare, and economic warfare – can be used in conjunction with one another and play off one another's strengths and developments in the battle space to further the political objectives of the hybrid actor. As mentioned, this is a clear tactic by the hybrid actor to limit a state's domestic sovereignty – their ability to exercise control within the borders of their own polity. By using cyber attacks and overt military operations, Crimea and Eastern Ukraine have been isolated from Kyiv, both physically and in terms of communication channels. Information and psychological warfare have confused and divided opinion with Ukraine, promoting further inner turmoil among groups of citizens and the sitting government. Finally, economic warfare has exacerbated the issue and has further driven Ukraine into collapse.

3.0 <u>How Russia has used hybrid warfare to expose gaps in NATO doctrines and methods of operations</u>

During the conflict in Ukraine, Russia has been able to expose gaps and weakness of current NATO doctrine and methods of operation by using hybrid warfare means and methods. This was acknowledged and reflected by NATO in the Wales Summit Declaration 2014, as several new initiatives and partnerships were established (this will be examined in greater detail in Section 4) as a direct means of countering and preparing for hybrid warfare in the future. A few themes

[81] Aslund, Anders. "Russia's War on Ukraine's Economy." *Project Syndicate*. July 9 2015.
[82] Ibid.
[83] Ibid.
[84] Flintoff, Corey. "A New Front In The Ukrainian Conflict: Russian Gas Imports" *NPR Radio*. March 2 2015.
[85]Stefanini, Sara, and Gurzu, Anca. "Tensions flare over Russia-Ukraine gas deal". *Politico*. November 9 2015; "Russia halts gas supplies to Ukraine after talks breakdown". *BBC News Europe*. July 1 2015.

have been particularly prevalent and recurrent when both NATO officials and academics discussed the gaps hybrid warfare has exposed within the NATO structure: the unique nature of hybrid warfare does not easily lend itself in all cases to a determination that falls within Article IV or Article V[86]; the lack of nimbleness or flexibility (both operationally and within the North Atlantic Council structure) in responding to such threats[87]; current NATO defence spending does not necessarily match what is necessary to counter hybrid warfare[88]; and finally, it goes beyond the scope of what NATO, as a military alliance, has been created and trained to respond to[89]. These themes will be discussed below to further give context to the subsequent sections, which will discuss current initiatives NATO has deployed post Russian aggression in Ukraine, as well as possible recommendations for the alliance moving forward given the acceptance that certain areas of NATO's structure have been exposed by hybrid warfare.

Hybrid Warfare and the Challenges it poses to Article IV and V of the Washington Treaty

At its point of conception, it would have been extremely difficult albeit impressive if NATO's Washington Treaty had taken into consideration the unique nature of hybrid warfare. The Treaty was designed with conventional (and the threat of nuclear) warfare, and Westphalian state versus state conflicts, in mind. However, that same unique nature of hybrid warfare has resulted in one of the most significant challenges for existing NATO doctrine when looking to counter hybrid threats, predominantly in terms of the challenges it poses to the infamous Articles IV[90] and Article V[91] of the Washington Treaty.[92] The unique nature of hybrid warfare does not easily lend itself, in all cases, to a determination that falls within Article IV or Article V.

As this paper has explored, a successful hybrid actor is able to deploy a denial strategy by using predominantly covert non-military state actions (non-military meaning that the regular

[86] NATO Parliamentary Assembly, "Hybrid warfare: NATO's new strategic challenge?" April 2015; Racz, 2015; Lucas, Edward, and Mitchell, Wess. "Central European Security After Crimea: The Case for Strengthening NATO's Eastern Defenses". *Centre for European Policy Analysis*. March 25 2014; Freedman, Lawrence, "Ukraine and the art of limited war". *War on the Rocks*. October 8 2014; Schadlow, Nadia. "The Problem with Hybrid Warfare." *War on the Rocks*. April 2 2015; "How NATO's Article 5 Works." *The Economist*. March 9 2015.

[87] Drent, Margiret. New Threats, New EU and NATO Responses. *Netherlands Institute of International Relations*. July 2015; "NATO to counter hybrid warfare from Russia." *BBC News.* May 14 2015.

[88] Maigre, Merle. "Nothing new in hybrid warfare: the Estonian experience and recommendations for NATO". *The German Marshall fund of the United States.* February 12 2015; NATO Parliamentary Assembly 2015; Harper, Jon. "NATO Funding Shortfalls Likely to Continue." *National Defense Magazine.* September 2015; NATO, Defense expenditures of NATO countries (2008-2015).

[89] Drent, 2015; Manea, Octavian. "Hybrid War as a War on Governance: Interview with Mark Galeotti". Small Wars Journal. August 19 2015; North Atlantic Treaty Organization. "A hybrid war – a hybrid response?" July 2014.

[90] "Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened"

[91] Collective defence article: An attack on one ally, is to be considered an attack on all members of the Alliance.

[92] Interviews with Global Affairs Canada Officials, January 12 2016; Stefanescu, Daniel. "NATO strategy to defeat enemy forces in the hybrid warfare". *Air Force Academy of Romania*. May 2015; NATO Parliamentary Assembly, 2015.

conventional military does not participate outright or in plain view during the operation, but may do so under the guise of humanitarian assistance, or covertly without insignia in addition to using the various other means and methods explored in Section 2 such as economic, informational, cyber etc). NATO does not currently define these non-military actions as constituting a threat or an attack because it is an entirely new form of warfare that the drafters of the Washington Treaty did not foresee. While the North Atlantic Council (NAC) has been able to address the threat posed to itself by Al Qaeda on 9/11, hybrid warfare is different. Hybrid warfare is not applied in a uniform way and is context specific, meaning, depending on battlespace, the hybrid actor can apply a varying combination of the means and methods described in Section 2 depending on its target. This changing nature makes it even more difficult to come to a final concept or definition.[93]

Finally, as an additional layer of complexity when assessing NATO's ability, it is important to note that although Ukraine is an important and meaningful member in NATO's Partnership for Peace Programme, it is not a member of the Alliance. Consequently, any Russian aggression or use of hybrid warfare in Ukraine would not trigger a response based on Article IV or V.

Hybrid Warfare and the Challenges it poses to Operational and Structural Flexibility

A second theme that has been recurrent is the lack of nimbleness or flexibility in two areas: 1) NATO's current structure/decision making process of the North Atlantic Council (NAC), and 2) NATO's current military methods of operational in comparison to hybrid threats.[94]

In regards to the first flexibility challenge, a main issue is that the NAC is an intergovernmental institution and thus represents 28 differing interests, threat perceptions and perspectives of each individual sovereign member state.[95] For example, the Baltic States rank Russian aggression as their highest threat priority and are constantly requesting that NATO increase its reassurance and support, whereas Great Britain or France do not rank Russian aggression as their highest threat priority.[96]

NATO also operates on a consensus basis, meaning all members are equal and receive one vote each. If Article IV or Article V were to be invoked, the NAC must *unanimously agree* that

[93] Racz, 2015; Interviews with Global Affairs Canada Officials, January 12 2016; NATO Parliamentary Assembly, 2015.; Aaronson, Michael. "NATO Countering the Hybrid Threat." *Institute for National Strategic Studies*. 2011; Schadlow, 2015.

[94] Jacobs, Andreas, and Lasconjarias, Guillaume. "NATO's Hybrid Flanks". NATO Defense College Research Paper. April 2014; Davidson, Janine. "Local Capacity is the First Line of Defense Against the Hybrid Threat. *The German Marshall Fund of the United States*. September 14 2015; "Charting NATO's Future Intro and Panel 1: Introduction and NATO's New Threat Horizon." *The North Atlantic Council.* October 6 2015; McInnis, Kathleen. "NATO: Charting the Way Forward". Chatham House. July 21 2014.

[95] Williams, M.J., "NATO, Security, and Risk Management".*Sage Publications*. 2008; NATO Parliamentary Assembly, 2015; Aaronson, 2011; Drent, 2015.

[96] Lucas, 2014.; Adler, Katya. "Baltic states shiver as Russia flexes muscles". *BBC News*. March 6 2015; Griebeler, Monika. "Lithuania's deep fear of Russia". *DW Akademie*. May 24 2014; Parry-Sabet, Rayyan. "Ukraine crisis: Inhabitants of the Baltic states fear that they will be next in the firing-line." *The Independent*. February 19 2015.; Lee, Lawrence. "NATO drill aims to reassure nervous Baltic States". *Al Jazeera*. May 21 2015; Schadlow, 2015.

an intervention can occur in retaliation to an armed attack on one (or more) member(s) and to do so they must come to a unified coherent (military, legal and policy) understanding of the hybrid threat during a consultative meeting with all members.[97] It is important to note that the process of achieving a unanimous decision amongst 28 member states on whether to react and how to react to a hybrid threat could result in bureaucratic/institutional lag and rigidity in responding to a highly time-sensitive crisis.

In addition, it is important to also remember that although the NAC is structured in a way that allows each member an equal voice and vote, it is still very much a political process in which power dynamics are present and part of the decision making process. In this sense the interpretation given to Articles IV and V are more influenced by policy than legal or military considerations. The US has been the uncontested leader of the Alliance and an informal grouping of the bigger Allies (the 'big three': UK, France, US) has largely dominated crucial NATO decisions.[98] These power dynamics that are present during the political process of NAC meetings and decisions can therefore affect whether or not Article IV or V is invoked and if it is, how swiftly it is invoked and the amount or types of resources that are used. For example, PEW Global Research conducted a survey in 2015 (post Russian aggression in Ukraine), which found that many larger and more powerful NATO Allies (Great Britain and Poland in particular) would be reluctant to use force to defend Allies against an attack from Russia. [99] By contrast, smaller states, especially those along the Eastern Flank joined NATO specifically for the collective defence clause.[100]

Secondly, there is the concern of lacking military operational nimbleness and flexibility in regards to responses against hybrid warfare.[101] In 1949 NATO was created to counter conventional Westphalian state versus state threats and thus their military forces and methods of military operation included defence systems, weapons, equipment and command and control structures to counter conventional-natured threats and their timelines. However, conventional means of warfare are no longer the norm, and irregular non-military means of warfare that occur on a much faster timeline are on the rise. While the Alliance has slowly demonstrated the ability to make some operational adjustments to counter non-traditional threats such as those posed by non-state actors in Afghanistan, hybrid warfare initiated by Russia poses a new set of operational challenges. In order to effectively and efficiently challenge and counter hybrid warfare and other contemporary threats, the Alliance must have the ability to shift operations suddenly and unexpectedly and importantly, along the spectrum of hybrid warfare tactics that the adversary can put into action at any given point during the conflict. The sentiment that NATO's military forces are not entirely up to par with 21st century threats is voiced by Supreme Allied

[97] Schadlow, 2015; Stefanescu, 2015.

[98] The main themes of military strategy, retaliation, nuclear weapons, forward strategy, flexible response and enlargement decisions have been initiated or directed by 'the three big Allies' (US, UK, France). Honakanen, Karoliina. "The influence of small states on NATO making decisions". *Swedish Defence Research Agency*. November 2002.

[99] Simmons, Katie, and Stokes, Bruce, and Poushter, Jacob. "NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid." *PEW Global Research.* June 10 2015; Schadlow, 2015; "How NATO's Article 5 Works." *The Economist*. March 9 2015.

[100] Honakanen, 2002.

[101] "NATO to counter hybrid warfare from Russia." *BBC News.* May 14 2015.

Commander General Breedlove who stated, "We have to adapt our responsiveness inside the NATO Response Force so that we have a force that can respond at speed to address this new model of hybrid warfare we have seen out of Russia." [102] Section 4 will further demonstrate how NATO has taken this concern very seriously, as they have adopted several initiatives relating to the need of high readiness, agile and quickly responsive forces. [103]

Former Canadian Ambassador to NATO, Yves Brodeur, emphasized the above challenges NATO faces both operationally and within its decision-making processes during his panel remarks at the 2016 Canadian Defence Association Institute's Annual Defence Conference. He recounted the tensions he witnessed first-hand during NAC meetings when the members were attempting to define hybrid warfare, and when the members attempted to "label an aggressor".[104] He said that there were certain actors within the Alliance that were extremely reluctant or refused to label Russia as the aggressor (emphasizing the paper's above point regarding the political and power dynamics). Brodeur concluded that NATO decision-making processes and operational early warning systems were extremely slow to respond to the on-the-ground situation that was changing almost hourly, or were virtually non-existent. [105] Ultimately, Brodeur argued that this operational and decision-making rigidity failed NATO at a crucial time, and NATO is still "extremely ill-equipped to deal with faceless conflict/hybrid warfare". [106]

Hybrid Warfare and the Challenges it poses to Defence Spending

A third theme that is recurrent when discussing how hybrid warfare has exposed gaps within NATO's structure and military methods of operation is related to the defence spending budgets and the components of the defence spending and procurement. [107]While most military budgets across NATO have been declining since the end of the Cold War, they have also remained somewhat 'stuck in the past' and have failed to be organized and re-prioritized for the nature of 21st century threats.[108] Currently, some of the required resources to counter or aid a country in countering a hybrid threat do not fit within official NATO approaches to defence spending.[109] For example, there is consensus that during the initial phases of hybrid warfare, internal security services (security services, police forces and border guards) are extremely important as acting as the first line of defence until the situation can be assessed further and more assistance can be provided.[110] However, member states' individual defence spending on internal security has no agreed upon benchmark or category within the Defence Expenditures.[111] In addition, other components of defence spending, such as emphasis towards irregular or non-military equipment support systems such as communication systems, cyber deterrence systems, enhanced

[102] Sisk, Richard, and Osborn, Kris. "Breedlove: NATO needs better response force for Russian threat" *Military.com.* September 15 2014

[103] NATO Wales Summit Declaration, 2014; Davidson, 2015.

[104] Yves Brodeur, "Panel 3: Terrorism, Non-State Actors, and Faceless Conflict." CDAI Conference 2016.

[105] Ibid.

[106] Ibid.

[107] McInnis, 2014: Andreas, and Lasconjarias, 2014.

[108] NATO Parliamentary Assembly, 2015.

[109] NATO, Defense expenditures of NATO countries (2008-2015).

[110] Andreas, and Lasconjarias, 2014.; Maigre, 2015; McInnis, 2014.

[111] NATO, Defense expenditures of NATO countries (2008-2015).

intelligence collection and analysis systems, etc. should be given more attention over more traditional conventional equipment.

Hybrid Warfare and the Challenges it poses to NATO as a Military Alliance

The final challenge that hybrid warfare has exposed within NATO's structure is the simple fact that it's means and methods of operation go beyond the scope of NATO's mandate as a military alliance – meaning hybrid warfare needs hybrid solutions.[112] Hybrid warfare is a war on governance using both military and non-military means. As a military Alliance, NATO does not necessarily have at its disposal all the tools necessary to counter all aspects of hybrid warfare, such as economic or informational components. Therefore, a purely militarily response from NATO is unlikely to be wholly successful. NATO's military forces will and should no doubt continue to play a vital role in countering hybrid warfare by coordinating and supporting operations, however it is important to acknowledge that a hybrid threat requires a hybrid, comprehensive security (civilian and military) approach.[113] This challenge and its possible solutions will be explored further in Section 4 and 5.

To conclude, this section has explored a few of the more prominent and recurrent themes regarding the gaps hybrid warfare has exposed within the NATO structure. These challenges include: the fact that the unique nature of hybrid warfare does not easily lend itself in all cases to a determination that falls within Article IV or Article V; the lack of nimbleness or flexibility (both operationally and within the North Atlantic Council structure) in responding to such threats; current NATO defence spending does not necessarily match what is necessary to counter hybrid warfare; and finally, it goes beyond the scope of what NATO, as a military alliance, has been created and trained to respond to. The themes explored are reflective of the concept hybrid warfare itself – it operates below an attribution threshold and it operates on intensely flexible and context specific basis using both military and non-military means and methods of operation. The next section will build upon this section by identifying and evaluating the ways in which NATO could adjust to this form of hybrid aggression, as well as review current NATO efforts to date to adapt to Russian hybrid warfare.

4.0 A review of NATO efforts, to date, to adapt to Russian hybrid warfare

A few months after Russian aggression in Ukraine began (February-March 2014), the Wales Summit was held in September 2014. As a result of these events, the crisis in Ukraine and use of hybrid warfare was a prominent topic of discussion at the Wales Summit and was mentioned over 40 times in the official transcript.[114] NATO rhetoric clearly, firmly and repetitively stated that Russia's actions in Ukraine and the illegitimate occupation of Crimea were a breach of international law; that Russia had disrespected and disregarded Ukraine's territorial integrity and sovereignty, that Russia had "fundamentally challenged the Alliance's vision of a Europe whole, free and at peace".[115] The 2014 Wales Summit not only set the tone for the subsequent NATO rhetoric, press releases, and statements to date, but it also endorsed and set out to establish various initiatives and projects that would directly counter and adapt to Russia's use of hybrid warfare in Ukraine.

[112] North Atlantic Treaty Organization. "A hybrid war – a hybrid response?" July 2014.
[113] McInnis, 2014; Interviews with Global Affairs Canada Officials, January 12 2016.
[114] North Atlantic Treaty Organization, "Wales Summit", 2014.
[115] Ibid.

This section will review four of the most prominent and current operational initiatives that target hybrid warfare and attempt to adapt NATO's command and control structures and military operations. These initiatives and projects include: the Readiness Action Plan, an updated Defence Planning Package, a technical agreement with the European Union (EU) on cyber security, and the creation and establishment of the new NATO Strategic Communication Centre of Excellence in Riga, Latvia.

The major endorsement arising from the Wales Summit was the Alliance's creation of a Readiness Action Plan (RAP). This is NATO's most significant defence reinforcement since the end of the Cold War. The mandate of the RAP is to strengthen NATO's collective defence and to ensure the Alliance is ready to respond swiftly and firmly to new security challenges emanating from the East (Russia) and the South (Middle East and North Africa), through assurance (physical military forces) and adaption measures (long term restructuring of command and control posture and systems).[116] The RAP assurance measures are a series of continuous land, sea and air activities from all 28 NATO members (on a rotational basis) designed to reinforce member defence, reassure populations, and deter potential aggression, especially in the Central and Eastern areas of Europe. Specifically, this includes an increase from 4 to 16 fighter jets for air policing in the Baltic Region and Romania and Poland, the commencement of AWACS surveillance flights over Eastern NATO territory, the deployment of maritime forces to patrol the Baltic Sea and Eastern Mediterranean, and the increase of number of military training exercises.[117] These assurance measures can be "stepped up or reduced as necessary, depending on the security situation". [118] An example of these assurance measures put into real-time practice was during Operation Trident Juncture 2015 – NATO's largest exercise in over a decade. This training exercise brought together 36, 000 personnel, 230 units, 60 ships and submarines and over 200 aircraft.[119] This exercise simulated attacks from fictional aggressive hybrid actors, including cyber attacks and ballistic missile defence, as well as combating in Afghanistan-type scenarios.[120]

The adaptation measures are longer-term changes to the restructuring of NATO's command and control posture that will allow the Alliance to react more quickly and decisively to sudden crises.[121] These include changes to the NATO Response Force (NFR), the creation of a Very High Readiness Joint Task Force (VJTF), the establishment of six multinational NATO Force Integration Units (NFIUs), and the development of a High Readiness multinational

[116] North Atlantic Treaty Organization, "Wales Summit", 2014; North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015; North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016.

[117] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016.

[118] Ibid.

[119] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016.; Black, Christopher. "Trident Juncture: NATO's Largest Military Exercise since Cold War. The "Fictitious Target" is Russia". Global Research. October 29 2015; Weisgerber, Marcus. "Now NATO's Prepping for Hybrid War". *Defense One.* August 27 2015.

[120] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016; Black, 2015. Weisgerber, 2015.

[121] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016.

headquarters.[122] The NRF is a "highly ready and technologically advanced" multinational force of air, land, maritime and Special Operations Forces units that can be deployed quickly, to wherever needed. At the 2014 Wales Summit, the NFR increased its personnel to 40,000 from 13,000 in order to enhance and strengthen the Alliance's collective defence and readiness to respond.[123] The VJTF was created at the 2014 Wales Summit to contribute to and enhance the NRF efforts. It is a multinational "spearhead force" of around 20,000 troops consisting of air, maritime, Special Operations Forces and chemical, biological, radiological and nuclear (CBRN) units/task forces that will have the ability to deploy with 48 hours of a crisis.[124] Six multinational NFIUs were established (in Estonia, Latvia, Lithuania, Poland, Romania, and Bulgaria) as small Eastern flank command and control headquarters that will facilitate the rapid deployment of the VJTF and other follow-on forces, improve cooperation and coordination among NATO and national forces and provide support for training exercises.[125] Finally, two High Readiness multinational headquarters (Northeast and Southeast) have been developed to provide additional high-readiness support (i.e. logistical enhancements, and preposition of equipment and supplies), and control and command to forces specifically located in Poland and the Baltic states.[126]

The second initiative endorsed at the 2014 Wales Summit, in light of Russian aggression in Ukraine, was an updated version of NATO's Defence Planning Package. This new package includes updates of six key Connected Forces Initiatives (CFI) measures: a broader NATO Training Concept 2015-2020; an updated NATO Education, Training, Exercise and Evaluation Policy (ETEE); high visibility training exercise in 2015 (which was Operation Trident Juncture); a Special Operations Component Command Headquarters capability under operational command of SACEUR; and a broader and more demanding exercise programme from 2016 onwards, particularly using technological aspects of CFI.[127] The new ETEE Policy is a long-term document outlining the strategies for education, training, exercise and evaluation of individuals, units, formations and headquarters in the NATO force and command structures. It addresses the process for linking national and NATO exercises and provides a framework for non-NATO entities and partner involvement.[128] The broader NATO Training Concept 2015-2020 lays out NATO's commitment to ensure the maintenance of highly ready, interoperable, and operationally effective forces. Central elements of this broader concept include use of education

[122] Ibid.

[123] Ibid.

[124] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016; North Atlantic Treaty Organization. "NATO Response Force." Mary 11 2015. Supreme Headquarters of the Allied Powers of Europe. "NRF/VJTF News."

[125] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016; North Atlantic Treaty Organization. "NATO Force Integration Units." Fact Sheet. September 2015; Supreme Headquarters of the Allied Powers of Europe. "Six NATO Integration Units activated." September 2 2015; North Atlantic Treaty Organization. "Greater solidarity, strength and readiness": NATO Secretary General marks opening of six new headquarters in Eastern Allies." September 3 2015

[126] North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016; Supreme Headquarters of the Allied Powers of Europe. "High Readiness Forces and Headquarters in the NATO force structure".

[127] North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015; North Atlantic Treaty Organization "A Whole NATO Initiative". April 6 2014.; Mizera, Miroslav. "NATO force 2020: role of connected forces initiative". CENAA. 2013.

[128] North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015.

and training such as, resident courses, key leader training, multinational exercises and e-learning initiatives.[129] As mentioned, Operation Trident Juncture was the "flagship" high visibility event for the CFI in 2015. In addition, the new CFI package provides the framework for NATO to continue major exercises in 2016 and onward. Particularly, this involves utilizing and implementing technology to help deliver interoperability.[130] Finally, the updated CFI package created a Special Operations Component Command Headquarters, which facilitates the command and control by the SACEUR of SOF operations and exercises with a focus on high readiness.

During the February 2016 Summit Meetings, the EU and NATO followed up on signing a technical agreement regarding their mutual cooperation on cyber defence issues, as was set out during the Wales Summit. This technical agreement provides a framework under which the guidelines for the sharing of information on specific cyber threats, the sharing of technical procedures, lessons learned and best practices, and the configuration of networks among both institutions.[131] NATO Secretary General Jens Stoltenberg noted at the February 2016 Summit Meetings that this technical agreement is a concrete example of how the two institutions have begun to work together and use their complementary tools and resources on issues related to combating elements of hybrid warfare.[132]

The creation of the new NATO Strategic Communication (StratCom) Centre of Excellence in Riga, Latvia in January 2014 demonstrates NATO's commitment and contribution efforts in the area of strategic communications. Importantly, the creation of this StratCom Centre is an acknowledgement on NATO's behalf that a 21st century security environment is increasingly influenced by social media networks and the 24 hour news cycle – "the perception is always relevant to, and can have a direct effect on the success of NATO operations and policies".[133] As was discussed in Section 2, public diplomacy, public affairs, military public affairs, information operations and psychological operations are all key elements used in hybrid warfare, and were clearly present during the crisis in Ukraine. This StratCom Centre is responsible for countering those elements of hybrid warfare, by providing a narrative of correct and unbiased information to audiences within and beyond NATO's territory.[134] In addition to their operational work, the StratCom Centre has published several documents and essays on topics related to issues previously discussed in this paper, such as Internet trolling as a tool of hybrid warfare and the use of social media during the Ukraine conflict.[135]

To conclude, it is apparent that all initiatives set out by the 2014 Wales Summit focus on a few common themes: the need for military operations to be swift, nimble and responsive to a

[129] North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015.
[130] Ibid.
[131] North Atlantic Treaty Organization "NATO and the European Union enhance cyber defence cooperation." February 10 2016; North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015.
[132] North Atlantic Treaty Organization "NATO and the European Union enhance cyber defence cooperation." February 10 2016.
[133] NATO StratCom Centre of Intelligence. "About Strategic Communications."
[134] Ibid.
[135] NATO StratCom Centre of Intelligence. "Publications."

variety of 21st century crisis, the need for a restructuring of the existing command and control structures to reflect, support and facilitate those high readiness military operations, the need for NATO to include non-military type projects and resources (i.e., the StratCom Centre) into their defence systems to make them 21st century appropriate, and the need to cooperate with other institutions and outside Allies who have complementary systems and resources to combat elements of hybrid warfare. The following section will expand on these initiatives and provide possible recommendations as to how NATO could further adjust its strategic, policy and operational options to counter hybrid warfare.

5.0 **Recommendations for how NATO could adjust to this form of aggression**

One conclusion that can be drawn from the Wales Summit is that it set out ambitious policy, operational and strategic initiatives that largely focused on reassurance for member states in light of Russian aggression in Ukraine.[136] Building upon the previous section, which evaluates NATO's efforts to date to counter hybrid warfare, this section seeks to provide policy, strategic and operational recommendations that not only focus on reassurance but also on deterrence[137] and resilience[138] moving forward, all while using a comprehensive security approach.[139] The recommendations in this section either outline entirely new recommendations for the Alliance, or identify areas, projects and initiatives that current NATO efforts are successful in countering this new form of aggression and thus should be continued. Together, these include: further cooperation with the EU in areas beyond cyber and economic domains, improving surveillance and intelligence capacities, redefining resources and defence spending, continuing the operational and tactical nimbleness while also improving structural nimbleness, addressing the

[136] Interviews with DND Officials, March 4.

[137] Deterrence in terms of deterrence by punishment (meaning, Article 5 collective defence), as well as deterrence by denial (meaning, to deter an enemy from attacking in the first place based upon the notion it would be very costly to do so).

[138] McInnis, 2014. A crucial aspect of defence planning is resilience: the state or institution's ability to withstand and recover from catastrophic attack or accident. It is important to note that resilience is largely political. While the military component of resilience plays central role in building resilience in advance, McInnis argues it is often the political response to the attack that matters the most. To achieve this, significant political coordination and collaboration among allies and partners before hand must take place. This is important because once an attack occurs, and if no previous political discussion as how to respond and do so in a timely manner does not arise, then leaders are left responding disjointedly and incoherently during critical points of the crisis. The events in Ukraine have shown that NATO needs to further enhance and promote resilience in its immediate neighbours and partners, as well as their own operational and structural components.

[139] A comprehensive security approach is a strategy under which the leading organization, institution or government, cooperates in a concerted and coordinate manner with national, regional and international actors (civil society, individuals, networks, non-governmental organizations, institutions, other government departments, etc.) in an effort to combine their complementary range of resources and technical expertise address a certain crisis or situation that has multiple components and dimensions.[139] Essentially, political, civilian and military tools are deployed in a coherent and cooperative manner in order to meet and counter complex 21st century security challenges and threatsJamie Shea, 'NATO, the challenges ahead', *Global Affairs*, Volume 1, number 2, 2015; Miklaucic, 2011; Williams, Andrew. "Implications of Operationalizing a Comprehensive Approach: Defining what Interagency Interoperability Really Means." The International C2 Journal, Vol 4, No. 1. 2010; The North Atlantic Treaty Organization. "A comprehensive approach to crises." September 2015.

lack of doctrine against hybrid warfare, and addressing challenges it poses to Article V and VI of the Washington Treaty. [140]

Further cooperation with the EU in areas beyond cyber and economic domains

It is recommended that NATO begin its hybrid warfare deterrence and resilience measures by further engaging and cooperating with the EU beyond the economic and cyber domain. As of present, and as discussed in the previous section, the EU and NATO have already begun cooperation in these two domains in light of Russian aggression in Ukraine: NATO and the EU have recently signed a technical agreement on cyber defence, and economic sanctions through the EU against Russia have been introduced.

Beyond cyber and economic domains, NATO could benefit from the EU's civilian power strengths. One important area in which NATO-EU partnership could further evolve to deter and create resilience against hybrid warfare is through the proactive promotion of good governance, social cohesion and outreach to minority groups in potential target countries and public messaging to counter information warfare.[141] Although it is embedded within NATO's strategic identity to promote a Western Liberal Democratic order, as a military Alliance, it does not have the mandate nor all the appropriate tools to necessarily create, maintain and implement the democratic institutions, good governance, anti-corruption campaigns, and social cohesion that goes hand-in-hand with Western Liberal Democratic order. While, by contrast, the EU, as a civilian power, has the ability, resources and legal authority to implement, monitor and maintain democratic institutions, good governance, anti-corruption, and social cohesion, etc. both within its borders and beyond through the draw of potential membership for current non-member states. The maintenance of strong liberal democratic institutions and social cohesion among all groups of the population can be a crucial factor in how easily hybrid warfare tactics can penetrate a target country. States whose governance and institutions are weak are more vulnerable to outside pressure and can create pretexts for hybrid warfare campaigns.[142]

The EU and NATO should also establish a joint strategy or action plan for projects aimed at propaganda and misinformation.[143] It is recommended the EU and NATO work in collaboration to create a common and coherent narrative that clearly communicates and promotes the Liberal Democratic values that both institutions promote. Currently, both institutions have only just recently established Strategic Communications Centres aimed at countering misinformation, and still fall behind Russian strategic communication capacities. [144] If these individual efforts by NATO and the EU are not coordinated and on the same page, they could do more harm than good – mixed messaging, spread of confusion, and inefficiency through duplication are some examples. In addition, efforts cannot only be about the promotion of a pro-Western message or

[140] These recommendations also reflect the advice and comments given by the SACEUR General Breedlove in light of Russian aggression in Ukraine. "SACEUR: 'Allies must prepare for Russia hybrid warfare". *Military.com*. September 2104.

[141] Maigre, 2015.

[142] Bernstein, Paul. "Rethinking deterrence and assurance." NDC Conference Report. *NATO Defense College*. September 2015.

[143]Pernik, Piret. "EU and NATO: Enhancing cooperation to counter hybrid threats". *European Leadership Network.* September 7 2015.; Maigre, 2015.

[144] Drent, 2015.

narrative – factual non-partisan information must be transmitted within and outside NATO and the EU's reach, and both institutions must work together to assist independent Russian-language media with their messaging and narratives to counter misinformation disseminated by the Russian state.

Improve surveillance and intelligence capabilities

It has been a common theme throughout interviews conducted with practitioners[145], academic work[146]and press releases made by high-ranking NATO officials[147], that NATO must improve and increase its intelligence gathering capabilities and situational awareness in regards to deterring and becoming resilient to hybrid warfare tactics – both within the Alliance, as well as with the EU. Former Canadian Ambassador Yves Brodeur stated NATO is simply not doing enough in regards to sharing intelligence amongst its own member states and there continues to be a culture of wariness when it comes to sharing intelligence within the Alliance.[148] He argues that 21st century 'faceless conflict/hybrid warfare' requires NATO to share intelligence more effectively; otherwise the Alliance will remain ill-equipped to deal with 21st century threats.

First, NATO requires better intelligence gathering and early-warning capabilities.[149] This can be and should be done by increased sharing of intelligence within the Alliance, as well as in partnership with the EU. Prior to February 2014, Western European and North American countries were not necessarily aware that there was a mounting threat of Russian aggression in Ukraine, while countries geographically closer to the Eastern Flank of the Alliance and who had experience first-hand various forms of Russian aggression (cyber warfare, informational warfare, psychological warfare, etc.), were very aware of this threat. If intelligence sharing within the Alliance been more balanced, widely distributed and taken seriously/acted upon, early warning signals and responses could have been created, either deterring or preventing Russia from creating a *fait accompli* in Ukraine.[150] The EU can also play a vital role by providing situational awareness through early warning intelligence sharing and monitoring for countries that are at risk of weak institutions, poor governance and minority group fractures within the society, and can offer incentives and capacity building tools to strengthen these at risk countries.[151] As a result, NATO and the EU could establish early warning indicators for at risk/vulnerable countries.[152] This database should include information outlining existing, growing and specific areas of vulnerabilities in the given country. In the event of hybrid warfare attack, member states both in the EU and NATO would be able to respond more effectively and efficiently, as each

[145] Yves Brodeur, "Panel 3: Terrorism, Non-State Actors, and Faceless Conflict." CDAI Conference 2016; Interviews with DND Officials, March4 4 2015.

[146] McInnis, 2014.

[147] Ukraine Today. "NATO must adapt to counter modern threats from Russia: Stoltenberg". January 2016;
U.S. Department of Defense. "Department of Defense Press Briefing by General Breedlove in the Pentagon Briefing Room". April 3 2015; Englehart, Katie. "US Plan for Eastern Europe Is 'Not Provocative,' Says NATO Head — Yet Moscow Disagrees". Vice News. June 19 2015.

[148] Yves Brodeur, "Panel 3: Terrorism, Non-State Actors, and Faceless Conflict." CDAI Conference 2016; McInnis, 2014.

[149] Drent, 2015; McInnis, 2014.

[150] McInnis, 2014.

[151] Interviews with DND Officials, March 4 2015; Drent, 2015.

[152] Pernik, 2015.

situation and use of hybrid warfare tactics are tailored to the specific vulnerabilities in the target country.

NATO must also improve its ability to gather intelligence to determine faster and with greater certainty from where and from whom the hybrid tactics are emanating from.[153] As previously discussed in this paper, the issue of attribution in hybrid warfare is a main challenge for the Alliance. Improved intelligence capabilities should be enhanced and targeted with the goal of determining, with greater certainty who the hybrid actor is. This allows for a more effective and tailored NATO response against the perpetrator. No matter the kind of warfare conducted, it always remains important for an actor to know and recognize who the enemy/perpetrator is in order to fully understand their capabilities, interests, rationales, and goals, which then allows the appropriate deployment of the necessary set of countermeasures. Therefore, enhanced intelligence capabilities facilitating attribution will assist in a successful NATO response.

If NATO is able to determine who the hybrid actors are and is able to create early warning systems, the Alliance can become resilient against these threats, as well as deter future hybrid actors from using similar sets of activities as the chances of NATO being able to pinpoint attribution to the given perpetrator (thus resulting in punitive action) will be much greater.

Continual improvement of operational and structural nimbleness

As outlined in Section 3, hybrid warfare poses challenges relating to operational and structural flexibility and nimbleness of the Alliance. Section 4 outlined the various ways in which the Alliance has begun to adapt operationally to this challenge by creating and deploying a Readiness Action Plan that includes a Very High Readiness Joint Task Force, which can deploy on extremely short notice to address and respond quickly and swiftly to new security challenges. However, the Alliance has still yet to address the issue of structural flexibility and nimbleness in specific regards to the NAC decision-making process (of which this paper has identified as a key challenge to the Alliance when countering hybrid warfare or other high intensity and fast-acting security threats).

NATO's 28 member states are all entitled to their own interests and opinions as to how best to react (or not act) to a variety of risks and threats. However, as was previously mentioned and was apparent during the Ukraine crisis, this issue has stalled the NAC's ability to come to a swift and coherent decision on course of action. Therefore, this paper recommends that NATO develop and improve the ways in which it can address the structural rigidity of their decision-making and political negotiations processes. Although it is beyond the scope of this paper to fully and deeply evaluate and debate the spectrum of ways in which this can be done, a common popular academic recommendation[154] is for NATO to encourage smaller groupings or coalitions of Allies within the Alliance to collaborate to address emerging security threats. The smaller coalition would still be required to seek approval of the NAC and be required to be in constant consultation with the NAC in order to maintain Alliance solidarity, which is important for the

[153] Interviews with DND Officials, March 4 2015

[154] McInnis, 2014; Michel, Leo. "NATO decision-making: Au Revoir to the Consensus Rule?" *Strategic Forum, Institute for National Strategic Studies.* Washington, D.C.: National Defense University. August 2003; McNamara, Sally. "Principles and Proposals for NATO Reform." Heritage. December 2008.

credibility and legitimacy of NATO. It is less likely the NAC would be slowed down in such type of decision making processes, because countries who would have been weary of giving a yes-vote, would be more inclined to do so given they no longer are required to contribute to the mission. Contributing member states to this smaller coalition would be award decision-making capacities that are in proportion to their contributions. In addition, new member states could join the mission at various stages of the conflict depending on their interests and resources. This solution facilitates burden sharing as well as increased ability to swiftly respond to crises as they arise.

By improving the flexibility and nimbleness of structural decision-making processes, NATO will project resilience to future enemies and threats. Improvement in this area would reaffirm that an attack on NATO members or partners would not critically impair, disable or delay its functioning and decision-making processes. Operational flexibly and agility will only be successful if the mechanisms and structures that instruct and deploy them are equally flexible and agile. Therefore, it is of the utmost importance that NATO consider matching its operational flexibility with structural flexibility and nimbleness.

Addressing the lack of doctrine against hybrid warfare

Section 3 has also identified the lack of doctrine against hybrid warfare to be a challenge to the Alliance. Simply put, it is recommended NATO come to a coherent and common definitional understanding of hybrid warfare and incorporate it into a formal doctrine or formal Strategic Concept. At the Wales Summit, NATO was still grappling with how to react and counter this new form of aggression. Therefore, looking forward it will be of importance for future research endeavours to pay attention to the Warsaw Summit in July 2016 in order to see if NATO announces plans to develop or create a hybrid warfare doctrine or create a new Strategic Concept that includes hybrid warfare (the last Strategic Concept was issued in 2010), or continue to counter and adapt to this form of aggression in an ad hoc manner. The strength in creating a hybrid warfare doctrine or incorporating it into a new Strategic Concept, would allow for a coherent strategic narrative that would demonstrate NATO's willingness and resolve to reassure, deter and become resilient to new forms of aggression and threats in the 21st century.[155] Like all Strategic Concepts, it would also serve as an important overarching guide for the operational, policy and strategic development (importantly including a guide for defence spending and procurement, as explored below) moving forward and demonstrate to future enemies and perpetrators of hybrid warfare that the Alliance is in agreement and ready to respond to such types of threat with refined coherence, swiftness and with the appropriate tools and resources.

Re-define resources and defence spending through the continuation of Smart Defence

NATO should consider redefining and re-evaluating its resources and defence procurement and spending to reflect the challenging fiscal environment and the nature of 21st century warfare.[156] As was mentioned in Section 3, the existing defence expenditure budgets do not

[155] Lindley-French, Julian. "Hybrid Warfare: NATO needs a Stoltenberg Doctrine." Blog on LinkedIn. May 2015.

[156] Interviews with DND Officials, March4 4 2015; Maigre, 2015; Harper, 2015.

necessarily match the needs of countering hybrid warfare tactics.[157] Given that most Allies face a challenging fiscal environment, the re-evaluation of defence spending and resources is not only about increasing or meeting NATO's defence spending quota. The recommendation of this paper is to also use existing tools and resources and budgets in a manner that addresses hybrid warfare tactics – buying the right equipment – thus a continual pivot towards NATO's 'Smart Defence'. Smart Defence is a "cooperative way of generating modern defence capabilities that the Alliance needs, in a more cost-efficient, effective and coherent manner." [158] This would allow for greater resources to be allocated to areas that reflect the nature of 21st century warfare, such as ballistic missile defence, cyber defence, intelligence and reconnaissance and strategic communications strategies and tools.[159] Strengthening purely conventional resources would only further encourage hybrid actors to rely on hybrid tactics, placing NATO at a greater disadvantage.[160] The redefining of NATO's resources and defence budgets into a Smart Defence strategy must reflect counter-measures of an increasingly interconnected and comprehensive security environment – policing, citizenship, organized crime networks, energy networks, cyber networks and strategic communications must all be considered and included in new defence spending budgets and discussions. [161] The creation of a budget and procurement plan that matches NATO's rhetorical commitment to countering hybrid threats will have a deterrent effect on possible future hybrid actors, as they will be aware NATO can respond beyond conventional military means.

The previous section, a review of NATO's efforts to date, to adapt to Russian hybrid warfare, largely reflected a theme of reassurance to partners and member states. This included the need for highly visible, nimble, swift and responsive forces that are equipped with conventional style, albeit technologically advanced tools and resources, and the creation of brand-new Strategic Communications Centres along the Eastern Flank to reassure the most vulnerable Allies. This section sought to move beyond reassurance measures and attempted to provide recommendations that either built upon[162] , or provided entirely new[163] policy, strategic or operational initiatives in order to create an Alliance who not only can reassure partners and member states but also can become resilient to hybrid warfare and deter hybrid warfare.

[157] Shea 2015; Drent, 2015. This is largely because defence spending and procurement are guided by and are in accordance with the current Strategic Concepts. The last Strategic Concept was issued in 2010 and is therefore out of date considering recent security threats such hybrid warfare and the rise of ISIL.

[158] North Atlantic Treaty Organization. "Smart Defence". September 2015.

[159] Ibid.

[160] Drent, 2015.

[161] Galkins, Kaspars. "NATO And Hybrid Conflict: Unresolved Issues From The Past Or Unresolvable Threats Of The Present?" Naval Postgraduate School of Monterey, California. September 2012; Miklaucic, Michael. " NATO Countering the Hybrid Threat." The North Atlantic Treaty Organization. September 2011.

[162] E.g. what should the way forward be for the Strategic Communications Centres, or greater emphasis on Smart Defence.

[163] E.g. new forms of cooperation between NATO and the EU, improvements in intelligence sharing and gathering capabilities, incorporating hybrid warfare into a new Strategic Concept, or improvements in nimbleness of structural decision-making.

Finally, one challenge that was mentioned in Section 3 was in regards to hybrid warfare and Article V and VI of the Washington Treaty. While attempting to fit hybrid warfare into Article IV and V is a credible and real challenge for the Alliance and impacts its deterrence and resilience to hybrid threats, this paper argues that it would be much harder and may not even be desirable or feasible for the Alliance (or some member states in particular) to concretely define hybrid warfare and label its components as possible future Article V worthy attacks. Issues explored previously in this paper such as: concerns with decision making processes, political negotiation processes and power balances within the Alliance and the NAC; the lack of consistency that is applied in hybrid warfare; and hybrid warfare's ability to conduct its operations below a threshold of attribute, can all be factors that will deter or hinder the Alliance's ability and capacity to define hybrid threats squarely under Article IV or V.

6.0 Canada's role within the Alliance in confronting hybrid warfare

This section will offer a Canadian perspective of NATO's efforts to counter hybrid warfare. It will provide a brief overview of Canada's current contributions to the Alliance in light of Russian aggression in Ukraine, as well as recommendations as to how they can further these contributions.

Apart from the NATO operations that have deployed a rotational force of member state personnel in Central and Eastern Europe, some NATO member states have provided additional assistance and aid to Ukraine on a bi-lateral basis. Canada is one of the NATO member countries that has contributed both to the rotational assurance force, as well as contributed additional aid and assistance. Since January 2014, the Canadian Government has contributed an additional approximately $700 million in assistance to Ukraine.[164] This assistance is aimed at providing support in areas such as human rights, rule of law, promotion of civil society, advancement and strengthening of democracy, strengthening of security, and promotion of economic stability and growth. The form of military assistance Canada has provided is in the form of non-lethal aid – meaning equipment such as communications systems, explosive ordnance disposal equipment, tactical medical kits, night vision goggles, mobile field hospital equipment, etc.

Currently, the Canadian Armed Forces (CAF) are involved in two operations that are aimed at assisting and supporting NATO member states and Ukraine: Operation UNIFIER and Operation REASSURANCE. Operation UNIFIER brings together personnel and resources from the CAF and Global Affairs Canada to facilitate and support Ukrainian forces in their efforts to maintain sovereignty, security and stability through capacity building and military training.[165] Approximately 200 CAF personnel are deployed to Ukraine on a sustained and periodic basis until March 31, 2017.[166] The primary focus of this capacity building and military training includes: "tactical solider training which consists of marksmanship, moving, communication, survival, ethics and weapons training." [167] Operation REASSURANCE refers to the Canadian contribution to NATO's request of enhancing assurance measures and promotion of security and

[164] "Operation UNIFIER." Department of National Defence and the Canadian Armed Forces. February 2016.
[165] Ibid.
[166] "Operation UNIFIER." Department of National Defence and the Canadian Armed Forces. February 2016.
[167] Ibid.

stability in Central and Eastern Europe. As previously mentioned in this paper, this NATO led operation includes training, planned exercises, demonstrations and other assigned NATO tasks along the Eastern Flank of the Alliance. Canada has contributed Maritime and Land Task Forces who conduct and take part in surveillance, reconnaissance, monitoring, training and exercises. The Canadian Maritime Forces are currently deployed to the Aegean Sea, and the Land Task Forces are deployed to Estonia, Latvia, Lithuania, and Romania.[168]

There are a few ways in which Canada can and should continue its efforts and contributions to the Alliance and to Ukraine, especially in regards to building resilience against hybrid warfare. Specifically, Canada's strengths include intelligence gathering and sharing[169] and strategic communications.[170] Canada's strengths in the field of strategic communications have already begun to be realized, with its involvement in the Strategic Communications Centre of Excellence. Canada is contributing their knowledge and teaching expertise in advance counter-propaganda techniques.[171] Given that intelligence gathering and sharing and strategic communications are key areas in which this paper has identified NATO must improve on, Canada can and should be a key player in furthering these efforts in creating a more resilient NATO to hybrid warfare tactics.

7.0 Conclusions

While the concept of hybrid warfare is not necessarily new, Russia's unique way of employing hybrid means and methods of operation against Ukraine have reignited the international community's and NATO's interest in this particular form of warfare and caused them to reassess their strategy to it. It has resulted in an internal struggle within NATO as how to best adapt to this form of aggression – one that allows perpetrators to fuse a highly integrated combination of covert and overt military presence, information warfare, cyber warfare and economic warfare in a tailored case specific manner to achieve broader political objectives.

This paper argues that Russia's use of hybrid warfare has indeed exposed gaps within current NATO doctrine and methods of operation. Some challenges that were explored include the following. First, hybrid warfare does not easily lend itself in all cases to fit squarely within the key NATO articles (V and VI), as it largely operates below the threshold of attribution, and therefore cannot provoke or allow for a collective military response or defence. Second, NATO lacks nimbleness and flexibility in responding to this new form of aggression, both operationally as well as within the North Atlantic Council decision making structure. Third, NATO defence spending does not necessarily match what is required for a hybrid warfare defence strategy. Finally, a great strength (and at the same time, a great challenge to NATO) of hybrid warfare is that it extends beyond the scope of the military alliance's mandate, resources and capabilities – hybrid warfare actors knowingly and strategically uses non-violent civilian means and methods of operation, thus reducing NATO's ability to have a full and successful deterrence against it.

[168] Ibid.

[169] Payton, Laura. "Petro Poroshenko urges additional loans and intelligence sharing with Canada." CBC News. September 2014.

[170] Interviews with DND Officials, March 4 2016.

[171] NATO StratCom. "Countering propaganda: NATO spearheads use of behavioural change science." May 2015; NATO StratCom. "Canada contributes to capabilities of NATO StratCom COE." February 2015.

Current efforts NATO has made in an attempt to adapt to this new form of aggression primarily include reassurance measures for Allies along the Eastern Flank. These initiatives and projects include: the Readiness Action Plan, an updated Defence Planning Package, a technical agreement with the EU on cyber security, and the creation and establishment of the new NATO Strategic Communication Centre of Excellence in Riga, Latvia. This paper has recommended and concluded that going forward the Alliance must focus not only on reassurance measures for Allies but also focus on deterrence and resilience to this form of aggression. The areas in which NATO should continue its strategic, policy and/or operational counter-measures to combat hybrid warfare include: further cooperation with the EU in areas like cyber security and intelligence sharing, and the continuation of redefining defence spending and procurement with a pivot towards Smart Defence. Areas in which it is recommended for NATO to begin deterrence and resilience measures include: endorse cooperation with the EU on promoting good governance and social cohesion within countries and beyond the institutions borders; create a joint database and early warning system with the EU that will target countries that are particularly vulnerable to hybrid warfare; improve its intelligence sharing and gathering primarily within the Alliance; address the lack of doctrine against hybrid warfare, and finally; improve operational and structural nimbleness.

Together these measures would create a reality of resilience and deter a possible future hybrid aggressor by: 1) demonstrating NATO has created a coherent doctrine or a new Strategic Concept paper on hybrid warfare, putting no doubts in the minds of Allies and possible hybrid warfare perpetrators that the Alliance considers hybrid warfare to be an act of aggression worthy of clear and firm collective repercussions; 2) demonstrating both the EU and NATO are ready to respond jointly and swiftly with all means and resources available to both institutions, and 3) make it apparent to the hybrid aggressor that they no longer hold the advantage in the battle space, because with increased operational and structural nimbleness, intelligence gathering and sharing capacities, and emphasis on Smart Defence systems, NATO no longer primarily relies on conventional traditional equipment and forces when a hybrid attack occurs.

The upcoming Summit meeting in Warsaw in July 2016 will be especially important and influential for the practical and academic study of hybrid warfare and the defence and deterrence of this form of aggression. It will be important for future research and work to explore if the Warsaw Summit offers any evaluation and/or performance measurement strategies for how effective and efficient the current reassurance initiatives have been since established at the Wales Summit in 2014. As this paper has shown, many of the initiatives were newly created and are currently operational. However, as mentioned, because these measures are largely of reassurance nature it will be interesting to see whether NATO can comment to their effectiveness in combating hybrid warfare and the impact they have had on Russia's involvement in the region. Secondly, the Warsaw Summit should be providing new initiatives and projects that are focused on deterrence and resilience, as per the recommendations in this paper have outlined. Currently there is a trend towards closer collaboration with the EU (this is apparent in both high level rhetoric and within the increased numbers of technical agreements and working groups). Future research and work could evaluate the true effectiveness and success (or failures) the two institutions have achieved together in working towards a defence against hybrid warfare. Finally, the challenge of defining the concept hybrid warfare that is suitable and acceptable to all 28-

member states remains. Future research could explore the political negotiations and processes that would allow for a doctrinal definition of hybrid warfare and/or if the common, coherent and doctrinal definition is even feasible and desirable and the impacts it would have on future Article 5 operations.

As a final word of caution, it is sometimes said that militaries plan and organize themselves based on the last war fought. Consequently, it is important that the concept of hybrid warfare and the debate over its definition and meaning does not blind or divide NATO or take NATO's focus away from its *raison d'etre*. The Alliance must vigilant to the reality that war fighting at the high-end of the spectrum (traditional conventional war-fighting) can and will occur in the 21st century. Therefore, it is also important that academics and practitioners do not discount or completely disregard the need for these conventional capabilities. A blending of capabilities, means and methods of operation and doctrine that reflect both high-end and hybrid war fighting would be the ideal over-arching strategy moving forward for the Alliance.

Bibliography

1. Aaronson, Michael. “NATO Countering the Hybrid Threat.” *Institute for National Strategic Studies*. 2011.

2. Akkoc, Raziye. “MH17 airliner destroyed by Buk missile fired from eastern Ukraine, Dutch report confirms”. *The Telegraph UK*. October 13 2015. http://www.telegraph.co.uk/news/worldnews/europe/ukraine/11928778/MH17-hit-by-Buk-missile-Ukraine-plane-crash-Russia-live.html

3. Adler, Katya. “Baltic states shiver as Russia flexes muscles”. *BBC News*. March 6 2015. http://www.bbc.com/news/world-europe-31759558

4. Alexey Nikolsky, “Little, Green, and Polite: The Creation of Russian Special Operations Forces,” in *Brothers Armed: Military Aspects of the Crisis in Ukraine* (Minneapolis: East View Press, 2014, 1st ed., pp. 124-131.
5. Aslund, Anders. “Russia’s War on Ukraine’s Economy.” *Project Syndicate*. July 9 2015. http://www.project-syndicate.org/commentary/russia-war-on-ukraine-economy-by-anders-aslund-2015-07?barrier=true

6. Backzynska, Gabreila. “More foreign fighters break cover among Ukraine separatists”. *Reuters*. June 1 2014. http://www.reuters.com/article/us-ukraine-crisis-vostok-idUSKBN0EC1LL20140601

7. BBC News. “Ukraine Crisis: Timeline.” November 13, 2014.

8. BBC News. “NATO to Counter Hybrid Warfare from Russia.” May 14 2015.

9. Black, Christopher. “Trident Juncture: NATO’s Largest Military Exercise since Cold War. The “Fictitious Target” is Russia”. *Global Research*. October 29 2015. http://www.globalresearch.ca/trident-juncture-natos-largest-military-exercise-since-cold-war-the-fictitious-target-is-russia/5485587

10. Biscop, Sven. “Hybrid Hysteria.” *Security Policy Brief.* No. 64. June 2015.

11. Brodeur, Yves. “Panel 3: Terrorism, Non-State Actors, and Faceless Conflict.” CDAI Conference 2016.

12. Bernstein, Paul. “Rethinking deterrence and assurance.” NDC Conference Report. *NATO Defense College*. September 2015.

13. Bolton, Doug. “Ukraine says major cyberattack on Kiev's Boryspil airport was launched from Russia” *The Independent.* January 18 2016. http://www.independent.co.uk/news/world/europe/ukraine-cyberattack-boryspil-airport-kiev-russia-hack-a6818991.html

14. “Charting NATO's Future Intro and Panel 1: Introduction and NATO’s New Threat Horizon.” *The North Atlantic Council.* October 6 2015. http://www.atlanticcouncil.org/news/transcripts/charting-nato-s-future-intro-and-panel-1

15. “Crimean – the Russian Cyber Strategy to Hit Ukraine.” InfoSec Institute. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/

16. Cullison, Alan. “Malaysia Airlines Flight MH17 Crash Illustrates Different Realities in Russia vs. West”. *The Wall Street Journal.* July 22 2015. http://www.wsj.com/articles/mh17-crash-illustrates-different-realities-in-russia-vs-west-1437557400

17. Charap, Samuel. “The Ghost of Hybrid Warfare.” *Global Politics and Strategy.* November 23 2015

18. Davidson, Janine. “Local Capacity is the First Line of Defense Against the Hybrid Threat. *The German Marshall Fund of the United States*. September 14 2015. http://www.gmfus.org/publications/local-capacity-first-line-defense-against-hybrid-threat#sthash.BCZBomre.dpuf

19. Davis, John. “Continued Evolution of Hybrid Threats.” *The Three Swords Magazine*. 2015.

20. Deep, Alex. “Hybrid war: old concept, new techniques.” *Small Wars Journal*. March 2015

21. Drent, Margiret. New Threats, New EU and NATO Responses. *Netherlands Institute of International Relations*. July 2015.

22. DW. “Breedlove says all tools on the table to help Ukraine.” March 22 2015.

23. “DDoS Attacks Hit NATO, Ukrainian Media Outlets”. *Information Week: Dark Reading*. March 17 2014. http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742

24. Ennis, Stephen. “How Russian TV Changed during Ukraine Crisis.” *BBC News*. June 26 2015. http://www.bbc.co.uk/monitoring/how-russian-tv-changed-during-ukraine-crisis

25. Englehart, Katie. “US Plan for Eastern Europe Is 'Not Provocative,' Says NATO Head — Yet Moscow Disagrees”. *Vice News*. June 19 2015.

26. The European Union. “EU sanctions against Russia over Ukraine crisis.” March 8 2016.

27. Galeotti, Mark. “The rising influence of Russian special forces” *IHS Janes Intelligence Review*. 2014.

28. Galkins, Kaspars. “NATO And Hybrid Conflict: Unresolved Issues From The Past Or Unresolvable Threats Of The Present?” *Naval Postgraduate School of Monterey, California.* September 2012.

29. Griebeler, Monika. “Lithuania's deep fear of Russia”. *DW Akademie*. May 24 2014. http://www.dw.com/en/lithuanias-deep-fear-of-russia/a-17659404

30. Gosu, Armand, and Manea, Octavian. “Russian Pyschological Warfare.” *Black Sea in Access Denial Age*. September 11 2015.

31. Harper, Jon. “NATO Funding Shortfalls Likely to Continue.” *National Defense Magazine.* September 2015. http://www.nationaldefensemagazine.org/archive/2015/September/pages/NATOFundingShortfallsLikelytoContinue.aspx

32. Honakanen, Karoliina. “The influence of small states on NATO making decisions”. *Swedish Defence Research Agency*. November 2002.

33. “How NATO’s Article 5 Works.” *The Economist*. March 9 2015. http://www.economist.com/blogs/economist-explains/2015/03/economist-explains-6

34. Hoffman, Frank. “Hybrid Warfare and Challenges.” *JFQ issue 52 (1*). 2009.

35. Hoffman, Frank. “Hybrid vs. Compound.” *Armed Forces Journal*. October 2009.

36. Hoffmann, Frank. “Conflict in the 21st Century: The Rise of Hybrid Wars”, Potomac Institute for Policy Studies, Arlington, Virginia, Dec 2007. Pg. 8

37. “Hromadske.tv under DDoS-attack.” *Ukrainian non-governmental Organization: Institute of Mass Information.* November 26 2013. http://imi.org.ua/en/news/42266-hromadsketv-under-ddos-attack.html

38. Interviews with DND Officials, March 4.

39. Interviews with Global Affairs Canada Officials, January 12, 2016.

40. International Centre for Defence Studies. “Background Paper: Russia’s Actions against Ukraine.” June 10 2014.

41. The Interpreter. “T-64s Appear Between June 12 and June 18.” https://pressimus.com/Interpreter_Mag/press/9301

42. “Internet trolling as a hybrid warfare tool: the case of Latvia.” *NATO StratCom Centre of Excellence Publication.* 2016.

43. The Firearm Blog. “Comparative Weapon Analysis of Crimea Troops and Eastern Ukraine Militias.” April 2014. http://www.thefirearmblog.com/blog/2014/04/17/comparative-weapon-analysis-crimea-troops-eastern-ukraine-militias/

44. Frier, Nathan. “Hybrid Threats and Challenges: Describe… Don’t Define.” *Small Wars Journal.* December 2009.

45. Freier, Nathan. “Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context.” *Strategic Studies Institute.* May 2007.

46. Freedman, Lawrence, “Ukraine and the art of limited war”. *War on the Rocks*. October 8 2014.

47. Finkle, Jim, and Polityuk, Pavel. “Ukraine says communications hit, MPs phones blocked.” *Reuters.* March 4 2014. http://www.reuters.com/article/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304

48. Flintoff, Corey. “A New Front In The Ukrainian Conflict: Russian Gas Imports” *NPR Radio.* March 2 2015. http://www.npr.org/sections/parallels/2015/03/02/390154800/a-new-front-in-the-ukrainian-conflict-russian-gas-imports

49. Jacobs, Andreas, and Lasconjarias, Guillaume. “NATO’s Hybrid Flanks”. *NATO Defense College Research Paper*. April 2014.

50. Lasconjarisa, Guillaume, and Larsen, Jeffery. “NATO’s Response to Hybrid Threats.” *NATO Defense College*. 2015.

51. “Latest from OSCE Special Monitoring Mission (SMM) to Ukraine based on information received as of 18:00 (Kyiv time), 3 November 2014” *Organization for Security and Co-Operation in Europe.* November 4 2014. http://www.osce.org/ukraine-smm/126364

52. Lindley-French, Julian. “Hybrid Warfare: NATO needs a Stoltenberg Doctrine.” *Blog on LinkedIn*. May 2015.

53. Lee, Lawrence. “NATO drill aims to reassure nervous Baltic states”. *Al Jazeera*. May 21 2015. http://www.aljazeera.com/news/2015/05/nato-drill-aims-reassure-nervous-baltic-states-150521141041752.html

54. Lucas, Edward, and Mitchell, Wess. “Central European Security After Crimea: The Case for Strengthening NATO’s Eastern Defenses”. *Centre for European Policy Analysis*. March 25 2014.

55. Kofman, and Rojansky. “A Closer look at Russia’s Hybrid War”. *Kennan Cable.* April 2015

56. Manea, Octavian. “Hybrid War as a War on Governance: Interview with Mark Galeotti”. *Small Wars Journal*. August 19 2015.

57. McCaney, Kevin. “Russia’s Hybrid warfare tactics gain upper hand in Ukraine.” *Defense Systems*. March 24, 2015. https://defensesystems.com/articles/2015/03/24/russia-hybrid-warfare-ukraine-nato.aspx

58. Maigre, Merle. “Nothing new in hybrid warfare: the Estonian experience and recommendations for NATO”. *The German Marshall Fund of the United States.* February 12 2015.

59. Maurer, Tim. “Cyber Proxies and the Crisis in Ukraine.” *NATO CCD COE Publications*, Talinn, 2015.

60. Maurer, Tim and Janz, Scott. “The Russian-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.” *The International Relations and Security Network*. October 17 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345

61. McCuen, J.J. “Hybrid Wars”, Military Review, March-April 2008.

62. McInnis, Kathleen. “NATO: Charting the Way Forward”. *Chatham House.* July 21 2014.

63. McNamara, Sally. “Principles and Proposals for NATO Reform.” *Heritage*. December 2008.

64. Miklaucic, Michael. “ NATO Countering the Hybrid Threat.” *The North Atlantic Treaty Organization*. September 2011.

65. Michel, Leo. “NATO decision-making: Au Revoir to the Consensus Rule?” *Strategic Forum, Institute for National Strategic Studies.* Washington, D.C.: National Defense University. August 2003

66. Mizera, Miroslav. “NATO force 2020: role of connected forces initiative”. *CENAA*. 2013.

67. Nest, Daniel. “10 Outrageous ways the Russian Media Covered the Crash of MH17.” *Listverse*. September 7 2015. http://listverse.com/2015/09/07/10-outrageous-ways-russian-media-covered-the-crash-of-mh17/

68. The National Defense Strategy of the United States of America. March 2005.

69. NATO Parliamentary Assembly, “Hybrid warfare: NATO’s new strategic challenge?” April 2015.

70. “NATO to counter hybrid warfare from Russia.” *BBC News.* May 14 2015. http://www.bbc.com/news/world-europe-32741688

71. NATO, Defense expenditures of NATO countries (2008-2015).

72. NATO StratCom Centre of Intelligence. “About Strategic Communications.” http://www.stratcomcoe.org/about-strategic-communications

73. NATO StratCom Centre of Intelligence. “Publications.” http://www.stratcomcoe.org/publications

74. North Atlantic Treaty Organization “NATO and the European Union enhance cyber defence cooperation.” February 10 2016. http://www.nato.int/cps/en/natohq/news_127836.htm

75. North Atlantic Treaty Organization. “A hybrid war – a hybrid response?” July 2014.

76. North Atlantic Treaty Organization. "Greater solidarity, strength and readiness": NATO Secretary General marks opening of six new headquarters in Eastern Allies.” September 3 2015. http://www.nato.int/cps/en/natohq/news_122324.htm

77. North Atlantic Treaty Organization. "NATO Response Force." Mary 11 2015. http://www.nato.int/cps/en/natolive/topics_49755.htm

78. North Atlantic Treaty Organization. "NATO Force Integration Units." Fact Sheet. September 2015. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_09/20150901_150901-factsheet-nfiu_en.pdf

79. North Atlantic Treaty Organization. "Russian-Ukrainian-EU gas conflict: who stands to lose most?" *NATO Review Magazine.* http://www.nato.int/docu/review/2014/nato-energy-security-running-on-empty/Ukrainian-conflict-Russia-annexation-of-Crimea/EN/index.htm

80. North Atlantic Treaty Organization. "Who are the Men Behind the Masks?". Supreme Headquarters of the Allied Powers Europe: General Breedlove's Blog. April 2014. *http://www.aco.nato.int/saceur/blog/who-are-the-men-behind-the-masks*

81. North Atlantic Treaty Organization. "Connected Forces Initiative" August 31 2015. http://www.nato.int/cps/en/natohq/topics_98527.htm#

82. North Atlantic Treaty Organization. "Readiness Action Plan." February 8 2016. http://www.nato.int/cps/en/natohq/topics_119353.htm

83. North Atlantic Treaty Organization. "Cyber Defence." February 16 2016. http://www.nato.int/cps/en/natohq/topics_78170.htm

84. North Atlantic Treaty Organization. "Hybrid War – does it even exist." *NATO Review Magazine*. http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

85. North Atlantic Treaty Organization "A Whole NATO Initiative". April 6 2014. http://www.act.nato.int/article-2014-1-04

86. The North Atlantic Treaty Organization. "A comprehensive approach to crises." September 2015.

87. North Atlantic Treaty Organization. "Smart Defence". September 2015.

88. The North Atlantic Treaty Organization. "NATO Transformation Seminar 2015: White Paper". March 2015.

89. The North Atlantic Treaty Organization. ""Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation". The Lisbon Summit 2010.

90. The North Atlantic Treaty Organization. NATO and the European Union enhance cyber defence cooperation. February 10 2016.

91. The North Atlantic Treaty Organization. "NATO Foreign Ministers discuss boosting cooperation with EU, other partners". May 14 2015.

92. "OSCE drone jammed over eastern Ukraine." Ukraine Today. November 6 2014. http://uatoday.tv/geopolitics/osce-drone-jammed-over-eastern-ukraine-390227.html

93. Ostrovksy, Arkady. "Putin's Ukraine Unreality Show." *The Wall Street Journal.* July 28 2014. http://www.wsj.com/articles/arkady-ostrovsky-putins-ukraine-unreality-show-1406590397

94. Parfitt, Tom. "My life as a pro-Putin propagandist in Russia's secret 'troll factory'". *The Telegraph.* June 24 2015. http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html

95. Parry-Sabet, Rayyan. "Ukraine crisis: Inhabitants of the Baltic states fear that they will be next in the firing-line." *The Independent*. February 19 2015. http://www.independent.co.uk/news/world/europe/ukraine-crisis-inhabitants-of-the-baltic-states-fear-that-they-will-be-next-in-the-firing-line-10058085.html

96. Pernik, Piret. "EU and NATO: Enhancing cooperation to counter hybrid threats". *European Leadership Network.* September 7 2015.

97. Perry, Bret. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations." *Small Wars Journal*. August 14 2015.

98. Popsecu, Nicu. "Hybrid tactics: neither new nor only Russia." *European Union Institute for Security Studies*. January 2015

99. Racz, Andras, "Russia's Hybrid War in Ukraine", *The Finnish Institute of International Affairs*. June 2015.

100. Reuters. "Putin Press Conference with Vladimir Putin". March 2014. http://www.youtube.com/watch?v=7KrRov8IR4M

101. Russian Special Troops Enter Inside in Crimea Parliament, https://www.youtube.com/watch?v=DUH-A3IF3h0

102. "Russia halts gas supplies to Ukraine after talks breakdown". *BBC News Europe*. July 1 2015. http://www.bbc.com/news/world-europe-33341322

103. Rogin, Josh. "Exclusive: Russian 'Blackwater' Takes Over Ukraine Airport," The Daily Beast Company LLC, (28 February 2014),

http://www.thedailybeast.com/articles/2014/02/28/exclusive-russian-blackwater-takes-over- ukraine-airport.html

104. Rosen, Armin. “The Ukraine Crisis is entering a dangerous new phase.” Business Insider. June 2014. http://www.businessinsider.com/ukraine-crisis-is-entering-a-dangerous-new-phase-2014-6

105. Schadlow, Nadia. “The Problem with Hybrid Warfare.” *War on the Rocks*. April 2 2015.

106. Sindelar, Daisy. “The Kremlin’s Troll Army.” *The Atlantic.* August 12 2014. http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

107. “State-Run News Station Accused of Making p Child Crucifixion*.” The Moscow Times*. July 14 2014. http://www.themoscowtimes.com/news/article/state-run-news-station-accused-of-making-up-child-crucifixion/503397.html

108. Stefanini, Sara, and Gurzu, Anca. “Tensions flare over Russia-Ukraine gas deal”. *Politico*. November 9 2015. http://www.politico.eu/article/russia-gazprom-ukraine-trilateral-sefcovic/

109. Stone, Jeff. “Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyber warfare Against Ukraine.” *International Business.* December 17 2015. http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902

110. Simmons, Katie, and Stokes, Burce, and Poushter, Jacod. “NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid.” *PEW Global Research.* June 10 2015. http://www.pewglobal.org/2015/06/10/nato-publics-blame-russia-for-ukrainian-crisis-but-reluctant-to-provide-military-aid/

111. Sisk, Richard, and Osborn, Kris. “Breedlove: NATO needs better response force for Russian threat” *Military.com.* September 15 2014. http://www.military.com/daily-news/2014/09/15/breedlove-nato-needs-better-response-force-for-russian-threat.html

112. Stefanescu, Daniel. “NATO strategy to defeat enemy forces in the hybrid warfare”. *Air Force Academy of Romania*. May 2015

113. Supreme Headquarters of the Allied Powers of Europe. “Six NATO Integration Units activated.” September 2 2015. http://www.shape.nato.int/six-nato-force-integration-units-activated

114. Supreme Allied Headquarters of the Allied Powers of Europe. “NATO Releases Imagery: Raises Questions on Russia’s Role in Providing Tanks to Ukraine.” *North*

Atlantic Treaty Organization. June 14 2014. http://shape.nato.int/statement-on-russian-main-battle-tanks

115. Supreme Headquarters of the Allied Powers of Europe. "High Readiness Forces and Headquarters in the NATO force structure". *North Atlantic Treaty Organization.* http://www.shape.nato.int/page134134653

116. "SACEUR: 'Allies must prepare for Russia hybrid warfare". *Military.com.* September 2014.

117. Supreme Headquarters of the Allied Powers of Europe. "NRF/VJTF News." http://shape.nato.int/nrf-vjtf-news

118. Sukhov, Oleg. "The Media War Behind the Ukraine Crisis." *The Moscow Times.* March 11 2014. http://www.themoscowtimes.com/news/article/the-media-war-behind-the-ukraine-crisis/495920.html

119. Tweet from Oana Lungescu, NATO Spokesperson. https://twitter.com/NATOpress/statuses/445112624578306048

120. Ukraine Today. "NATO must adapt to counter modern threats from Russia: Stoltenberg". January 2016.

121. "Ukraine Liveblog Day 104: Klitschko Receives Cool Reception on Maidan". *The Interpreter*. June 1 2014. http://www.interpretermag.com/ukraine-liveblog-day-104-klitschko-receives-cool-reception-on-maidan/

122. U.S. Department of Defense. "Department of Defense Press Briefing by General Breedlove in the Pentagon Briefing Room". April 3 2015.

123. "Ukrtelecom's Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea." Ukrtelecom. February 28 2014. http://en.ukrtelecom.ua/about/news?id=120467

124. Volchek, Dmitry. "One Professional Russian Troll Tells All" *Radio Free Europe – Radio Liberty*. March 25 2015. http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html

125. Vegue-Martin, Tony. "Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it". CSO Online. April 24, 2015. http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html

126. Weitz, Richard. "Countering Russia's Hybrid Threats". Diplomaatia. November 2014. http://www.diplomaatia.ee/en/article/countering-russias-hybrid-threats/

127. Weisgerber, Marcus. “Now NATO’s Prepping for Hybrid War”. *Defense One.* August 27 2015. http://www.defenseone.com/management/2015/08/now-natos-prepping-hybrid-war/119687/

128. Weiss, Michael, and Pomerantsev, Peter. “The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money” *The Institution of Modern Russia.* 2014.

129. Weiss, Michael, et al. “An Invasion by Any Other Name: The Kremlin’s Dirty War in Ukraine” The institute of Modern Russia. 2015

130. Williams, Andrew. “Implications of Operationalizing a Comprehensive Approach: Defining what Interagency Interoperability Really Means.” *The International C2 Journal,* Vol 4, No. 1. 2010.

131. Williams, M.J., “NATO, Security, and Risk Management”. *Sage Publications*. 2008.

132. W. J. Nemeth, ‘Future War and Chechnya: A Case for Hybrid Warfare’, Thesis, Naval Postgraduate School, Monterey, California, June 2002.

133. https://www.youtube.com/watch?feature=player_detailpage&v=ztuHuSw_zw

134. http://www.youtube.com/watch?v=qPHNiTZe_wI