CANSOFCOM PROFESSIONAL DEVELOPMENT CENTRE

ON HYBRID WARFARE

COLONEL BERND HORN

THE CANSOFCOM PROFESSIONAL DEVELOPMENT CENTRE

MISSION

The mission of the Canadian Armed Forces Special Operations Forces Command (CANSOFCOM) Professional Development Centre (PDC) is to enable professional development within the Command in order to continually develop and enhance the cognitive capacity of CANSOFCOM personnel.

VISION

The vision of the CANSOFCOM PDC is to be a key enabler to CANSOFCOM headquarters, units and Special Operations Task Forces (SOTFs) as an intellectual centre of excellence for special operations forces (SOF) professional development (PD).

ROLE

The CANSOFCOM PDC is designed to provide additional capacity to:

1. develop the cognitive capacity of CANSOFCOM personnel;
2. access subject matter advice on diverse subjects from the widest possible network of scholars, researchers, subject matter experts (SMEs), institutions and organizations;
3. provide additional research capacity;
4. develop educational opportunities and SOF specific courses and professional development materials;
5. record the classified history of CANSOFCOM;
6. develop CANSOF publications that provide both PD and educational materials to CANSOF personnel and external audiences;
7. assist with the research of SOF best practices and concepts to ensure that CANSOFCOM remains relevant and progressive so that it maintains its position as the domestic force of last resort and the international force of choice for the Government of Canada.

ON HYBRID WARFARE

ON HYBRID WARFARE

Colonel Bernd Horn

Canadian Special Operations Forces Command
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Produced for CANSOFCOM Professional Development Centre
by 17 Wing Winnipeg Publishing Office.
WPO31341

Cover Photos: Major Janine Desjardins

MONOGRAPH 19 – ON HYBRID WARFARE

CANSOFCOM Professional Development Centre Monograph Series Editor: Dr. Emily Spencer

ISBN 978-0-660-05137-6 (Print)
978-0-660-05138-3 (PDF)

Government of Canada Catalogue Number D4-10/19-2016E (Print)
Government of Canada Catalogue Number D4-10/19-2016E-PDF (PDF)

Printed in Canada.

The views expressed in this publication are entirely those of the authors and do not necessarily reflect the views, policy or position of the Government of Canada, the Department of National Defence, the Canadian Armed Forces, the Canadian Special Operations Forces Command or any of their subordinate units or organizations.

FOREWORD

I am delighted to introduce our most recent monograph, *On Hybrid Warfare*, to the Canadian Special Operations Forces Command (CANSOFCOM) Professional Development Centre (PDC) series. This publication is both timely and of exceptional importance. The concept of "hybrid warfare," while arguably not new in its core substance, has created a flurry of activity and discourse in the academic, doctrinal and operational spheres. Regardless of the terms used, the operational methodologies, tactics and activities that are encompassed within a "hybrid warfare" approach represent a very significant threat tactically, operationally and strategically. For this reason, it is essential that we fully understand the concept of "hybrid warfare".

As such, *On Hybrid Warfare* provides an in-depth examination of the term, its application, as well as the threat it poses and measures that can be taken to mitigate the threat. Importantly, Colonel Horn has created an excellent monograph that will allow practitioners, theorists, and those with an interest in military operations, strategy and *Realpolitik* to gain useful insight into "hybrid warfare".

As always, the intent of the PDC monograph series is to provide interesting professional development material that will assist individuals in the Command, as well as those external to it, to learn more about human behaviour, special operations, and military theory and practice. I hope you find this publication informative and of value to your operational role. In addition, it is intended to spark discussion, reflection and debate. Please do not hesitate to contact the PDC should you have comments or topics that you would like to see addressed as part of the CANSOFCOM monograph series.

Dr. Emily Spencer
Series Editor and Director of Education & Research
CANSOFCOM PDC

ON HYBRID WARFARE

Terminology has a tyranny all of its own. Historically there is a tendency to view defence and security conundrums through the filter of a "new" form of warfare. However, as Dr. Emily Spencer has argued, "Redefining a problem because you cannot find a solution that is palatable does not actually change the circumstances; rather, it simply perverts your point of view."[1] In many ways, the discourse on the concept of Hybrid Warfare falls into this realm. Some analysts, scholars and practitioners argue that hybrid represents a new evolution in warfare. Others are equally convinced that hybrid warfare, or as the Americans now refer to it, "Gray Zone Warfare," represents nothing new aside from changing terminology (e.g. irregular warfare, unrestricted warfare, asymmetric warfare, compound warfare, 4th Generation Warfare, the indirect approach, compound warfare, low intensity warfare).

History has shown us that it is easy to be seduced into new terminology. However, as Dr. Spencer noted, "rather than creating a new lexicon, it is important to refocus on the basics of war in order to obtain viable solutions for the contemporary and future security environments."[2] And, when one focuses on the root of conflict and war it becomes evident that hybrid warfare is a methodology to conduct war, not a redefinition of the term. The great theorist, Carl von Clausewitz explained, "War is thus an act of force to compel our enemy to do our will."[3] He clearly recognized that war is just a tool and not the objective itself. As he clarified, "War is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means." Clausewitz rationalized, "The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose."[4]

Within this discourse is the basic premise that combatants, whether state or non-state, have at their disposal all means available to them to wage war to achieve their desired political outcome. Whether they choose to mobilize all means available to wage an unlimited war or to restrict themselves to a limited one is totally their prerogative. As such, to define the use of asymmetric or previously untapped methodologies as somehow "new" belies an ignorance of history.

A focus on even just some contemporary examples illuminates the continuities of warfare. American diplomat George Keenan described in 1948:

> In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[5]

Similarly, US President John F. Kennedy addressed West Point graduating military cadets in 1962 and warned:

> This is another type of war, new in its intensity, ancient in its origin — war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him.[6]

More recently, in 2014, the British Ministry of Defence asserted:

> Our adversaries are unlikely to engage us on our terms and will not fight solely against our conventional

> strengths. They will seek an asymmetric advantage and some will employ a wide range of warfighting techniques, sometimes simultaneously in time, space and domain. Their logic will not necessarily be our logic and thus our ability to understand adversaries – and our ability to make them understand our intent – will be challenging… In some conflicts, we are likely to see concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder. Tactics, techniques and technologies will continue to converge as adversaries rapidly adapt to seek advantage and influence, including through economic, financial, legal and diplomatic means. These forms of conflict are transcending our conventional understanding of what equates to irregular and regular military activity; the conflict paradigm has shifted and we must adapt our approaches if we are to succeed.[7]

Finally, more recently, two researchers from the Wilson Center, Kennan Institute concluded, "Despite sounding new and in vogue, its [hybrid warfare] analytical utility is limited. The "hybrid" aspect of the term simply denotes a combination of previously defined types of warfare, whether conventional, irregular, political or information."[8]

In essence, war, regardless of terminology, is arguably the oldest method of resolving conflict. In the pursuit of some desired victory, combatants will undertake, within their own political and military contexts (i.e. limited or unlimited approach to a conflict), whatever means are required and at their disposal to achieve their desired end state.

The objective of war – to achieve a desired end state – is thus unchanging. History has shown that from antiquity combatants have used every methodology available to them to achieve surprise,

minimize the superiority of their enemies and maximize their own relative strengths. The decisions of how to fight, how great the mobilization of resources will be, whether to approach the conflict as a limited or unlimited/total war, as well as the technology available may differ between epochs and combatants, however, the underlying premise of how combatants approach war has not changed.

An examination of hybrid warfare through this prism is therefore useful because it illuminates the fact that hybrid warfare does not represent an evolution of warfare. Rather, it merely represents the manifestation of globalization's effect on the means and methods available to combatants to wage war to achieve their desired political outcomes.

Defining Hybrid Warfare

Despite the fact that hybrid warfare is not a radically new evolution of war, it does warrant understanding how technology and globalization have impacted the manner in which conflict can now be arguably waged more effectively. Initially, it is important to understand how hybrid warfare has been framed from a definitional perspective. Not surprisingly, definitions vary widely. Part of the apparent confusion arises from the perspective taken on hybrid warfare as it can be viewed from a tactical/operational perspective, or from a larger strategic viewpoint. For instance, when discussing counter-insurgency or operations against a non-state antagonist such as Hezbollah or the Islamic State (IS) hybrid warfare takes a very tactical approach blending the ideas of asymmetry, conventional and irregular warfare. However, at the strategic level, when discussing a nation's manipulation of its entire spectrum of resources, such as the Russian approach to conflict in Georgia and the Ukraine, hybrid warfare takes on a different complexity. Regardless, in each case, however, the means and motive remain

consistent – use all resources available to attain the desired political outcome.

The articulation of "new methods" was actually tabled as early as 1999, when two Chinese colonels, Qiao Liang and Wang Xiangsui, broached the subject of hybrid warfare, although using a different term, when they published their treatise *Unrestricted Warfare*. In their work they clearly delineated:

> If we acknowledge that the new principles of war are no longer "using armed force to compel the enemy to submit to one's will," but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests." …Perhaps people already have no way of accurately pointing out when it first began that the principal actors starting wars were no longer only those sovereign states, but Japan's Shinrikyo, the Italian Mafia, extremist Muslim terrorist organizations, the Columbian [sic] or "Golden New Moon" drug cartel, underground figures with malicious intent, financiers who control large amounts of powerful funds, as well as psychologically unbalanced individuals who are fixed on a certain target, have obstinate personalities, and stubborn characters, all of whom can possibly become the creators of a military or non-military war. The weapons used by them can be airplanes, cannons, poison gas, bombs, biochemical agents, as well as computer viruses, net browsers, and financial derivative tools. In a word, all of the new warfare methods and strategic measures which can be provided by all of the new technology may be utilized by these fanatics to carry out all forms of financial attacks, network attacks, media attacks, or terrorist attacks. Most of these attacks are not military actions, and yet they can be completely

> viewed as or equal to warfare actions which force other nations to satisfy their own interests and demands. These have the same and even greater destructive force than military warfare, and they have already produced serious threats different from the past and in many directions for our comprehensible national security.[9]

One of the first uses of the term "hybrid war" was in a research paper written by Major William J. Nemeth at the Monterey Naval Postgraduate School in 2002. In his work, "Future War and Chechnya: A Case of Hybrid Warfare," he postulated that "Chechen society was in a hybrid situation between a pre-modern and contemporary state, where the architecture of the modern society was built upon the basis of a traditional, pre-state clan and family ties." He argued "this structure enabled Chechens to mobilize their society for war and provide widespread support for the fighting through family ties." Importantly, he asserts that "from this hybrid society a hybrid form of warfare emerged, which combined elements of regular and irregular warfare in a highly flexible and efficient way." Specifically, he maintains that the "Chechens were successful in synthesizing elements of Western and Soviet military doctrines with guerrilla tactics and the sophisticated use of modern technology."[10]

Another interpretation was put forward in 2008 by Colonel John McCuen who published an article in *Military Review* in 2008. He defined hybrid conflict or, more specifically, wars as follows:

> Hybrid wars are a combination of symmetric and asymmetric war in which intervening forces conduct traditional military operations against enemy military forces and targets while they must simultaneously—and more decisively—attempt to achieve control of the combat zone's indigenous populations by securing and stabilizing them (stability operations). Hybrid conflicts therefore

> are 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. In hybrid war, achieving strategic objectives requires success in all of these diverse conventional and asymmetric battlegrounds.[11]

Following the theme evident in McCuen's interpretation of Hybrid Warfare, Finnish researchers Aapo Cederberg and Pasi Eronen identified a key component of the concept. They explained, "Hybrid warfare intentionally blurs the distinction between the times of peace and war making it hard for the targeted countries to devise policy responses in a proper and timely manner."[12]

Other writers have followed in a similar vein. Colonel Margaret Bond forecast, "War of the next century will comprise a kind of hybrid war, projecting all elements of national power along a continuum of activities from stability, security, and reconstruction operations, to armed combat."[13] Researchers from the American Joint Special Operations University (JSOU) concluded, "Hybrid warfare is then violent conflict utilizing a complex and adaptive organization of regular and irregular forces, means and behaviour across multiple domains to achieve a synergistic effect which seeks to exhaust a superior military force indirectly."[14] Israeli military theorists describe hybrid warfare "as a method of social warfare which is unbounded by social constraints….gain a cognitive advantage by the very lack of social restrictions that conventional state forces must adhere to such as the Law of Land Warfare, Geneva Conventions and Rules of Engagement."[15]

Theorists David Sadowski and Jeff Becker argue that "the essential aspect of hybrid warfare is the underlying unity of cognitive and

material approaches in generating effects. Such a unity of cognitive and material domains allows for flexibility in a strategic context in which social 'rules' can be redefined in an iterative process to the hybrid's advantage in terms of legality and military norms."[16] Rand analyst Dr. Russell Glenn articulated two variations of a definition of hybrid threats:

> Hybrid threat (1): Any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battlespace. Rather than a single entity, a hybrid threat or challenger may be comprised of a combination of state and non-state actors.[17]

> Hybrid threat (2): An adversary that simultaneously and adaptively employs some combination of (1) political, military, economic, social, and information means, and (2) conventional, irregular, catastrophic, terrorism, and disruptive/criminal warfare methods. It may include a combination of state and non-state actors.[18]

Frank Hoffman, an internationally recognized expert on hybrid warfare, believes that "hybrid wars blend the lethality of state conflict with the fanatical and protracted fervor of irregular warfare." [19] He asserted:

> Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve

> synergistic effects in the physical and psychological dimensions of the conflict. These effects can be gained at all levels of war.[20]

He further clarified that:

> Future adversaries (states, state-sponsored groups, or self-funded actors) exploit access to modern military capabilities including encrypted command systems, man-portable surface-to-air missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosive devices, and assassinations. This could include states blending high-tech capabilities such as anti-satellite weapons with terrorism and cyber warfare.

US Joint Force Command weighed in on the concept in 2009 and defined a hybrid threat as "Any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battlespace."[21] The Command noted that a hybrid threat or challenger could be composed of a combination of state and non-state actors. Three years later, theorists Williamson Murray and Peter R. Mansoor defined hybrid warfare as "a conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose."[22]

Significantly, on 3 July 2014, NATO officially adopted the term "hybrid warfare" and declared it a new form of warfare. In September 2014, the NATO Wales Summit issued a formal declaration that described hybrid warfare as "a wide range of overt and covert military, paramilitary, and civilian measures [...] employed in a highly integrated design."[23]

Similarities abound. An Australian assessment noted that conflict is being replaced by "Hybrid Wars and asymmetric contests in which there is no clear-cut distinction between soldiers and civilians and between organised violence, terror, crime and war."[24] Canadian defence scientists argued that the term hybrid warfare "describes a conflict in which at least one belligerent employs organized military, paramilitary, and non-state (irregular) forces simultaneously, coordinating multiple forms of warfare as one means in a more-or-less comprehensive strategy meant to achieve a political end."[25] Another analyst defined hybrid warfare as a term "that sought to capture the blurring and blending of previously separate categories of conflict" that blended "military, economic, diplomatic, criminal, and informational means to achieve desired political goals."[26]

A Czechoslovakian think-tank espoused a rather lengthy definition:

> Hybrid warfare is an armed conflict conducted by a combination of non-military and military means and aiming with their synergistic effect to compel the enemy to take such steps that he would not do of his own accord. At least one side of the conflict is the state. The main role in achieving the objectives of war is played by non-military means such as psychological operations and propaganda, economic sanctions, embargoes, criminal activities, terrorist activities, and other subversive activities of a similar nature. The attacker's military operations are conducted in secret by irregular forces combining symmetric and asymmetric methods of combat operations against the whole society and, in particular, against its political structures, state authorities and local government, the state economy, the morale of the population and against the armed forces.[27]

Despite the plethora of definitions, there is a general agreement that hybrid warfare blends conventional, irregular, asymmetric, criminal and terrorist means and methods to achieve a political objective. Importantly, whether state or non-state actors, adversaries make use of the proliferation of technologies and information that has accompanied globalization. Instruments such as cyber warfare, economic coercion or even blackmail, exploitation of social/societal conflict in a target country and the waging of disinformation campaigns and psychological warfare are all in the inventory. Criminal behaviour and terrorism are also in the repertoire of combatants. But these are all methodologies that have always been exploited by insurgents and states, whether involved in limited or total wars.

What is of significant concern is the increased use of hybrid warfare by powerful states such as Russia. General Valery Gerasimov, Chief of the General Staff of the Russian Federation, clearly articulated the application of the modern incarnation of Russia's use of hybrid warfare in his article, "The 'Gerasimov Doctrine' and Russian Non-Linear War." He explains:

> Moscow is increasingly focusing on new forms of politically-focused operations in the future. In many ways this is an extension of what elsewhere I've called Russia's 'guerrilla geopolitics,' an appreciation of the fact that in a world shaped by an international order the Kremlin finds increasingly irksome and facing powers and alliances with greater raw military, political and economic power, new tactics are needed which focus on the enemy's weaknesses and avoid direct and overt confrontations. To be blunt, these are tactics that NATO—still, in the final analysis, an alliance designed to deter and resist a mass, tank-led Soviet invasion—finds hard to know how to handle.[28]

General Gerasimov clearly identifies the weakness of modern states. He insists that history has shown that "a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[29] This state of affairs is due, in his estimation, to the fact that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[30] In essence, rather than a kinetic solution to conflict, Gerasimov argues that the focused application of political, economic, informational, humanitarian, and other non-military measures, when applied in a coordinated manner with internal discontent and protest can wield significant results. In addition, all of these actions are also combined, at the right moment, normally to achieve final success, with concealed military action, often "under the guise of peacekeeping and crisis regulation."[31]

As such, hybrid warfare from a strategic perspective then entails the mobilization of a wide range of a state's resources, primarily non-violent, to achieve a desired political end-state. In fact, the use of violence is not remotely desired. In essence, hybrid warfare is seen as a methodology of achieving the political end-state without tripping the threshold of war, which would allow an opponent the recourse to legally use force and/or attract international intervention. In fact, hybrid warfare creates a perfect ambiguity that paralyzes opponents since they are not even aware that they are under attack.

Gray Zone Warfare

If the varied definitions and interpretations of hybrid warfare are not complex enough, the Americans have essentially redefined the term themselves and created yet another addition to the lexicon

by calling the concept "The Gray Zone." A US Special Operations Command White Paper defined gray zone challenges "as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks."[32] Senior SOF commanders asserted, "The Gray Zone is characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[33]

Not surprisingly, American theorists explained the concept in similar terms to hybrid warfare, explaining it was "a range of emerging gray area or unconventional techniques—from cyberattacks to information campaigns to energy diplomacy. They maneuver in the ambiguous no-man's-land between peace and war, reflecting the sort of aggressive, persistent, determined campaigns characteristic of warfare but without the overt use of military force."[34] In that same vein, General Joseph Votel insisted, "The Gray Zone really defines this area between ... for the most part healthy economic, political competition between states, and open warfare." He clarified, "It's a place where actors, sometimes state actors and sometimes non-state actors, act in a manner just below what would normally take us into normal open warfare."[35]

US Army College Professor Antulio J. Echevarria II opined that "Gray Zone war sits below the threshold and level of violence to prompt UN security council resolutions or NATO Article 5 response yet [its] not peace." He explains that countries such as Russia and China "exploit this zone of ambiguity to accomplish 'wartime-like' objectives outside the normal scope of what military strategists and campaign planners are legally authorized or professionally trained to address."[36]

In sum, gray zone proponents tend to stress the ambiguity of techniques that allow an opponent to actively engage in actions contrary to the target's national interests but which all fall under the overt recognized tear line of aggression. Deputy Secretary of Defense Bob Work, while participating at a US Army War College conference in April 2015, observed "that adversaries were increasingly using agents, paramilitaries, deception, infiltration, and persistent denial to make those avenues of approach very hard to detect, operating in what some people have called 'the gray zone'."[37]

In fact, the gray zone, which in fact embodies/describes hybrid warfare, is the artful application of an adversary's entire inventory of "tools," short of combat operations, to realize desired political objectives. It blurs the line between peace and war and targets, if not preys on, existing economic, political and/or social vulnerabilities of its opponent(s). In many, if not most, cases the target is not even aware they are under a concentrated hostile attack until it is too late. This is the strength of the gray zone or hybrid warfare methodology. The opponent(s) is caught in the net of ambiguity, low threshold of violence and plausible deniability of the attacker. As such, a coherent, effective response is often delayed until it is too late and the desired outcome of the antagonist has already been achieved.

Impact of Globalization

As already noted, hybrid warfare is not a new phenomenon. The application of the concept, however, has gained incredible impetus and effectiveness as a result of globalization and the increased access, if not proliferation, of advanced technology and information. Undeniably, the world has become extremely interconnected. This connectivity has created great advantages, wealth and opportunity; however, it has also created enormous security concerns. In

fact, globalization has arguably reshaped the security landscape. It has changed the access and flow of information, making means of communicating, planning and financing as well as the ability to gather important and relevant information extremely easy. Moreover, the global market place has also allowed advanced technology, which was once the purview of nation states, into the grasp of organizations and individuals.

Furthermore, the pervasive media, broadcast news, the internet and social media have created a crisis of immediacy. Information travels faster and farther, reaching millions in real time. As such, the ability to respond to a developing story, whether real or not, becomes extremely difficult for governments and security organization.

Exacerbating this reality is the fact that the interconnected and interdependent world, with a complex web of transnational corporations, foreign investment, economic and political interests, transnational criminal and terrorist organizations, has also generated an arguably unrestricted market place where advance technology, historically the purview of nation states, is now as accessible to non-state actors as it is to sovereign powers. In fact, many non-state actors such as narco-trafficers and terrorists have greater wealth than many of the countries in which they operate.

As result of globalization, the ability to conduct hybrid warfare has increased in its effectiveness and reach. At the tactical and operational level, opponents have greater ability to access advanced weapons and information technology with which to fight. In addition, their ability to attack political will, reach into the homeland and/or conduct terrorist attacks has increased.

At the strategic level, states, through the coordinated application of the entirety of their resources at their disposal can take advantage of social, political and economic vulnerabilities of their

opponents and cripple them without actually taking any overt violent or military action. Rather, by utilizing a hybrid methodology, they insidiously weaken, if not outright destroy, their adversaries without firing a shot.

Characteristics of Hybrid Warfare

Hybrid warfare entails the mobilization of all means available to a state or non-state actor to achieve specific political goals. Its effective application in the new "globalized world" ideally means the actions should be undetectable, or more accurately un-attributable. Creative asymmetric methodologies utilizing an indirect approach through cut-outs or plausibly deniable intermediaries can mask ownership of action. Nonetheless, hybrid warfare possesses some identifiable characteristics. These are:

1. The element of surprise;
2. Ambiguity – is there actually external participation or agitation? Has a hostile act actually occurred?;
3. Propaganda and disinformation – including fabrication of malicious stories;
4. Agitation;
5. Cyber attack;
6. Economic measures (e.g. embargo, blockade, boycott);
7. Denial of involvement;
8. Military participation, if involved, is indistinguishable from civilian participants;
9. Synchronization across all domains (i.e. an integrated campaign) – an adversary is able to coordinate and link

the varied lines of attack (e.g. cyber, disinformation, agitation, economic actions) across time and space to achieve desired effects; and

10. A slow persistent campaign designed to achieve political objective over time rather than a quick decisive outcome. A key requirement is to keep actions below the threshold of outright war.[38]

China's "three warfares" captures the essence of hybrid warfare's characteristics. Specifically they compromise of:

1. Psychological Warfare seeks to disrupt an opponent's decision-making capacity; create doubts, foment anti-leadership sentiments, deceive and diminish the will to fight among opponents;

2. Legal Warfare ("Lawfare") can involve enacting domestic law as the basis for making claims in international law and employing "bogus" maps to justify China's actions; and

3. Media Warfare is the key to gaining dominance over the venue for implementing psychological and legal warfare.[39]

Extrapolating from the characteristics of hybrid warfare, a European think-tank captured the basic tenets under the concept of subversion, noting there were four distinct stages:

1. demoralisation of the target society;

2. destabilisation of the target society;

3. precipitation of a crisis in the target society;

4. seizing control of the target society by internal forces acting in concert with the attacker.[40]

Theorists and studies have repeatedly noted that hybrid warfare challenges Western liberal democracies and their militaries because it targets "strategic cultural weakness of the West." [41] Methodologies such as cyber warfare, information warfare, exploitation of social or political divisions within a society, as well as economic intimidation or coercion makes the use of violence unnecessary, which in turn makes it difficult for the target country to resort to the use of force under the existing international legal framework. In addition, since they target the entirety of society across the full spectrum of economic, informational, political and social domains, Western societies are stymied in their ability to defend because of interagency parochialism within the security and defence sectors.

Recent Use

Recent examples of the application of hybrid warfare are not difficult to identify. The 2006 conflict in Lebanon, the Russian intervention in Georgia and the more recent case in Ukraine, Boko Haram's reign of terror in Nigeria, as well as the Islamic State's campaign in Syria and Iraq are but the most obvious. For Frank Hoffman, the Hezbollah campaign during the 2006 Lebanon War exemplified the "prototype" hybrid force. In its fight against the Israeli Defense Force (IDF) Hezbollah forces demonstrated that they were well trained and highly disciplined. They operated in distributed cells and combined a "blend of the lethality of the state with the fanatical and protracted fervor of irregular warriors." Hoffman believed that they "clearly demonstrated non-state actors' ability to study and probe the weaknesses of a Western style military, and then devise appropriate countermeasures."[42]

He was not alone in his assessment. Michèle A. Flournoy, the U.S. Under Secretary of Defense for Policy, reflected that the IDF were "stunned" by Hezbollah's "advanced battlefield tactics and weaponry, including the successful use of an advanced ground-

to-ship missile and anti-tank weapons" during the 34-day conflict. Moreover, she insists that "The Israeli experience in Lebanon has become a textbook case of the kind of hybrid warfare that many defense analysts believe will be a defining feature of the future security environment."[43]

The British Ministry of Defence concurs. They assessed:

> In the 2006 Lebanon War, Hezbollah employed an integrated strategy. They held ground, conducted limited manoeuvre, and they restricted IDF maritime access. They utilized cutting-edge anti-armour missiles (destroying or damaging approximately 50 Main Battle Tanks in the process), armed Unmanned Aerial Vehicles (UAVs), Signals Intelligence technology, anti-ship-cruise missiles, urban strong-points and deep tunnel complexes in difficult terrain which the IDF could not bypass. They evaded the Israeli Air Force and exploited an Israeli inability to conduct combined arms air/land manoeuvre. Hezbollah conducted their own deep strike operation, using surface-to-surface missiles and a comprehensive Information Operations campaign to strategic effect. Hezbollah shares its military strategy across a wide variety of our potential adversaries in near real time.[44]

Other analysts echoed the assessment noting that the use of decentralized cells that were comprised of both regular forces as well as guerrillas, and who were armed with a lethal inventory of precision guided missiles, short and medium range rockets, UAVs and sophisticated improvised explosive devices (IEDs) were able to conduct an effective urban campaign against a very capable IDF. In fact, Hezbollah, mentored by Iranian Quds Force operatives, "downed Israeli helicopters, damaged Merkava IV tanks, communicated with encrypted cell phones, and monitored Israeli

troops movements with night vision and thermal imaging devices." Moreover, Hezbollah fighters, by leveraging information technology, uploaded and distributed battlefield pictures and videos in near real-time, allowing them to dominate the battle of perception throughout the conflict. This domination resulted in the "overwhelming perception within the international community of an Israeli military defeat at the hands of Hezbollah."[45]

RAND analyst Russell Glenn agrees with the overwhelming assessment of the effectiveness of the Hezbollah hybrid warfare campaign. He went beyond the battlefield tactics, however, and noted Hezbollah's "long game" strategy and how they used that as an integrated approach, bringing it all together in a coordinated manner at the right time and place. He described:

> Hezbollah is more than a military force, and therein lies its real strength. It has political, social, diplomatic, and informational components that provide bedrock support for its military organization. That foundation, established by years of providing humanitarian aid, building physical infrastructure, educating Lebanese, and serving as medical provider would remain even in the aftermath of military defeat. Like the deep roots of a plant, these other facets of Hezbollah would over time spawn new forces to replace those lost in combat.[46]

Case Study – Russian Hybrid Warfare in the Ukraine

For others such as current USSOCOM commander General Joseph Votel though, the clearest example of hybrid warfare (or "Gray Zone activity" according to the Americans) is the case of the Russian campaigns in Crimea and the Donbass region in the Ukraine. "They are operating at a level below open warfare with us," Votel asserted, "but they're certainly operating in hybrid

approaches where they're making use of information operations, of surrogates, of ethnic Russians that are in those areas, of their own military forces, of their own special operations capabilities."[47]

Votel was referring specifically to the volatile situation in the Ukraine. In April 2014, separatist riots broke out in the eastern part of the country, in a manner similar to those in late February of that year, which subsequently evolved into the Russian annexation of Crimea in March 2014. Specifically, what appeared to be highly-trained and heavily-armed men appeared in Donetsk and Luhansk and they started to agitate politically organizing demonstrations and seizing public administration buildings, as well as police stations. Their justification was consistently that they were local separatists dissatisfied with the new Kyiv leadership. Significantly, the take-over of the first major buildings in Donbass was quickly followed by a proclamation by the Donetsk and Luhansk People's Republics, hitherto two non-recognized separatist organizations.

These local actions were not isolated. In fact they were in consonance with an aggressive, highly focused and extremely carefully coordinated diplomatic, economic and informational campaign both in the Ukraine, as well as internationally. Furthermore, additional duress was put on the Ukrainian government and indirectly on the West and the North Atlantic Treaty Organization (NATO) by the Russian deployment of a large number of combat units along the border, ostensibly for routine exercises. Much like the coordinated actions in Crimea, the combination of "highly-trained separatist forces," (believed to be Russian special operations forces (SOF)) and local separatist allies, combined with the larger coordinated actions of Russian were able to quickly disrupt, if not disable, the Ukrainian government.

The Russians achieved the annexation of the Crimea and the political disintegration of Eastern Ukraine without engaging in open

combat. Although unable to stop the annexation of Crimea, the new Ukrainian leadership under President Petro Poroshenko did stabilize itself and when the Russians commenced action in the Donbass region the government was able to begin to restore its control over its lost territories and it launched a major counter-attack known as the "Anti-Terror Operation." This counter-attack led to open conflict and a vicious civil war. Importantly though, the Russians had achieved their political objectives without NATO becoming engaged.[48]

In essence, the Russians deployed unidentifiable SOF across the Ukrainian border to capture key government buildings and weapons armories. They then passed control to pro-Russian separatist groups. Concurrently, the Russians waged a clandestine offensive against Ukraine, disconnecting, jamming, and attacking digital, telephone, and cyber communications throughout the country. Significantly, "Russia enlisted virtual 'privateers' and bounty hunters to conduct cyber-attacks against Ukrainian government information and logistic infrastructure, from Internet servers to railway control systems."[49] In fact, "Russia bankrolled a 'troll army' to wage *deza*, a Russian hacktivist term for disinformation, paying millions for each troll to post 50 pro-Russian comments a day on social media, blogs, and news sites that were critical of Russia's actions."[50] As result, they were able to create ambiguity and confusion through distorted reports of what was occurring in the Ukraine and consistent denials of any participation.

Analyst who study Russia quickly recognized the Russian approach, namely their belief that "modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy's armed forces personnel and civil population."[51] This approach is

highly advantageous as it removes the requirement of deploying combat power and risking an all-out war. Moreover, if the campaign is successful, the target country will turn on itself to its own detriment.

Notably, this approach is not new. Students of Russian foreign policy note that the Russian use of "advanced forms of hybrid warfare" relies heavily on "an element of information warfare that the Russians call 'reflexive control'…[which] causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[52] In the case of the Ukraine, Russia was able to skillfully manipulate the US and its NATO allies to remain largely passive while Russia dismembered the Ukraine.[53]

Experts identified the key elements of Russia's reflexive control techniques in Ukraine as:

- Denial and deception operations to conceal or obfuscate the presence of Russian forces in Ukraine, including sending in 'little green men' in uniforms without insignia;
- Concealing Moscow's goals and objectives in the conflict, which sows fear in some and allows others to persuade themselves that the Kremlin's aims are limited and ultimately acceptable;
- Retaining superficially plausible legality for Russia's actions by denying Moscow's involvement in the conflict, requiring the international community to recognize Russia as an interested power rather than a party to the conflict, and pointing to supposedly-equivalent Western actions such as the unilateral declaration of independence by Kosovo in the 1990s and the invasion of Iraq in 2003;

- Simultaneously threatening the West with military power in the form of overflights of NATO and non-NATO countries' airspace, threats of using Russia's nuclear weapons, and exaggerated claims of Russia's military prowess and success; and

- The deployment of a vast and complex global effort to shape the narrative about the Ukraine conflict through formal and social media.[54]

The Russian success did not go unnoticed by NATO. During a Security Summit in September 2014, the Supreme Allied Commander Europe (SACEUR), General Philip Breedlove, proclaimed that Russia's use of hybrid warfare in Eastern Ukraine represented, "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[55] Similarly, the NATO Secretary General, Jens Stoltenberg, underscored the threat. He explained:

> Russia has used proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability. So NATO must be ready to deal with every aspect of this new reality from wherever it comes. And that means we must look closely at how we prepare for; deter; and if necessary defend against hybrid warfare.[56]

He elaborated, "Hybrid [warfare] is about reduced warning time. It's about deception. It's about a mixture of military and non-military means. So therefore we have to be able to react quickly and swiftly."[57]

A subsequent "lessons learned" report supported the observations of the senior NATO leadership. It captured the Kremlin's strategic objectives as:

- undermining our perception of the world order as we know it;
- creating and maintaining a permanent state of confusion and destabilization;
- deliberately misinterpreting and thus distorting the core Euro-Atlantic values which serve as a basis of our democratic societies; and
- distracting from the causes and objective circumstances of the conflict, obstructing self-reflection and discussion on solution scenarios.[58]

The report further noted the impact that informational warfare can have. Specifically, it noted that the manipulation of messages in the social media "can promote the chaotic mass behavior, the escalation of rumor, confusion, panic and even violence." Amazingly, this behaviour can be instigated simply by promulgating "falsified photos or videos, or a status post using false identity offering highly alarming information that is designed in a way to drive audience into hysteric response – preferably in the real life, not only in the virtual domain." For instance, during the conflict in Ukraine social media was used to "spread rumors about large refugee flows, soldiers deserting the Ukrainian army, Ukrainian militaries being extremely violent towards the local population and even resorting to cannibalism, and the last but not the least – contaminating the water." The conflict in Ukraine became an important example of how vulnerable societies can be. Much of this stems from the fact that "social media platforms are trust-based and the manipulative 'signal' can easily go viral due to the obvious presence of inter-relations between the users and our lack of understanding that it is not only the TV-set where the government-sponsored propaganda may appear."[59]

The Russian use of informational warfare is certainly not new, however, their theorists believe its application is now more effective due to the "improved coordination and integration capacity and the new opportunities provided by network, grid, and internet technologies." Key is the networking capability of modern informational technology, which "provides fast, efficient coordination between the military and other elements of the campaign." In addition, cyber-attacks can be used to debilitate your opponent by causing power-supply failures, communications breakdowns and transportation paralysis. In short, it can create economic, political, military and social collapse in a target country.[60]

The case study of the Russian intervention in Ukraine is illustrative of a very carefully sequenced hybrid warfare campaign. The Finnish Institute of International Affairs (FIIA) broke it down in four specific Phases, each comprising of layered activities:

1. Preparatory Phase – this phase consisted of identifying all the strategic, political, economic, social and infrastructural weaknesses and vulnerabilities of the target country, and developing the requisite strategies to take advantage of them. In the case of the Ukraine this entailed identifying or creating political and cultural organizations loyal to Russia, gaining economic influence, developing a robust media strategy and strengthening separatist and anti-government movements and sentiments. This approach put tremendous pressure on the Ukrainian government. FIIA further clarified that preparatory phase could be further broken into three sub-sections:

    a. Strategic preparation:

        i. Exploring points of vulnerability in the state administration, economy and armed forces of the target country;

ii. Establishing networks of loyal NGOs and media channels in the territory of the target country; and

iii. Establishing diplomatic and media positions in order to influence the international audience.

b. Political preparation:

i. Encouraging dissatisfaction with the central authorities in the target country by using political, diplomatic, special operation and media tools;

ii. Strengthening local separatist movements and fueling ethnic, religious, and social tensions, among others;

iii. Actively using information measures against the target government and country;

iv. Bribing politicians, administrative officials and armed forces officers, and then 'turning them over';

v. Establishing contacts with local oligarchs and business people; making them dependent on the attacking country via profitable contracts; and

vi. Establishing contacts with local organized crime groups.

c. Operational preparation:

i. Launching coordinated political pressure and disinformation actions;

ii. Mobilizing officials, officers and local criminal groups that have been 'turned over'; and

iii. Mobilizing the Russian armed forces under the pretext of military exercises.

The FIIA researchers noted that importantly, during the preparatory phase, the antagonist does not engage in any open violence and did not undertake any actions that could be construed to trip the political or legal threshold that would allow the target country or its allies to take serious, active countermeasures. They highlighted that self-doubt and fear constituted a key component of the Kremlin's foreign policy approach.[61]

2. Attack Phase: This phase is the stage where the attacker unleashes a full scale hybrid warfare offensive. At this point organized, armed violence is undertaken. In the case of the Crimean and Donbass offensives, "little green men" (SOF) and unmarked Russian units using state of the art equipment, vehicles and weapons appeared and commenced to erect checkpoints and barricades to block the entrances to the Ukrainian military and police barracks. Although no shots were fired, it forced the Ukrainian security services to either remain in their barracks or use force against the militants.[62]

Importantly, the security forces did not defend the besieged buildings. Analysts ascribe this lack of defence to low morale, as well as poor leadership and lack of clear direction from their chain of command. Concomitant with the seizure of key buildings, suspected Russian military personnel, dressed in civilian attire and demonstrating a high degree of tactical acumen and skills, began to seize and occupy other less secure public administration buildings, media outlets and civilian infrastructure, such as television stations, radio stations and broadcasting towers. This combination allowed the Russians and their surrogates to control the air waves and the messages that were being broadcast. Not surprisingly, these means were used to reinforce the message that the protestors were locals dissatisfied with the Kiev government.

The neutralization of security forces and the seizure of key buildings and infrastructure were also reinforced by a very aggressive

information campaign designed to paralyze decision-makers and plant the seed of panic and inevitability in the minds of the public, but especially the security forces still loyal to the central government.[63] Concurrently, cyber-attacks as well as sabotage were used to destroy, disrupt or neutralize Kiev's command and control network. In Crimea, this led to the almost wholesale surrender of Ukrainian police and military units, some of which switched allegiance. The methods and results were similar in Eastern Ukraine.

Equally significant was the ability of Russia to paralyze a Western response by ensuring enough ambiguity and doubt. As such, President Vladimir Putin continually insisted there were no Russian troops in the Ukraine even when detailed information provided the intelligence to prove otherwise. To support the paralyzation of Western decision-makers he also deployed military units on the border, thereby creating additional trepidation of a decision by the West to intervene, as well as tempering the Kiev government's reactions to the "protesters" in fear of providing an excuse for a Russian invasion. In the end, the ploy worked and Putin was able to achieve his political objectives in both Crimea and the Donbass region without triggering a major war.

The FIIA researchers elaborated that the "attack phase" of the hybrid war can also be partitioned into three distinct sub-sections as follows:

a. Exploding the tensions:

    i. Organizing massive anti-government protests and riots in the target country;

    ii. Infiltrating SOF, disguised as local civilians, to conduct sabotage attacks and capture administrative buildings in the targeted regions (with the active or passive

support of corrupt local officials and police), in cooperation with local criminal groups;

iii. Concurrently, provocations and sabotage attacks are conducted throughout the target country, in order to divert the attention and resources of the central power;

iv. The media of the attacking country launches a strong disinformation campaign; and

v. Concurrently, counter-attack options by the attacked government are blocked by Russian regular forces, which are deployed along the border, to present an imminent threat of an overwhelming conventional attack.

b. Ousting the central power from the targeted region:

i. Disabling the central power by capturing administrative buildings and telecommunications infrastructure in the targeted region;

ii. Blocking the central power's media, thereby establishing a communication and information monopoly;

iii. Disabling the local armed forces of the central power using non-kinetic methods (e.g. blockading their barracks, bribing their commanders, breaking their morale). Disabling the border guards is particularly important;

iv. Concurrently, the diplomacy, media, economic actors and armed forces of the attacking country put strong pressure on the target country. The media of the attackers tries to mislead and disorientate the international audience, and discredit the target country.

c. Establishing alternative political power:

i. Declaring an alternative political centre, based on the captured administrative buildings, by referring to real or fabricated traditions of separatism;

ii. Replacing administrative organs of the central power with newly established political bodies, thereby creating a quasi-legitimacy;

iii. Media of the attacking country strengthens the legitimacy of the new political bodies;

iv. Alienating local population from the central power through disinformation and the information monopoly; and

v. Counter-attack options of the central power are continuously blocked.[64]

3. Stabilization phase: Once the political objectives of the attacking country are achieved, it is necessary to strengthen and legitimize its (or proxy) rule. The FIIA researchers labelled this third phase "strategic stabilization." It can be broken into three distinct sub-sections:

a. Political stabilization of the outcome:

i. Organizing a "referendum" and decision with regards to secession/independence in the target country, all with the strong diplomatic and media support of the attacking country; and

ii. The new "state" requests assistance from the attacking country.

b. Separation of the captured territory from the target country:

   i. Attacking country annexes the captured territory (e.g. Crimea); or

   ii. Attacking country establishes (open or covert) military presence there, and starts fighting the central government in the name of the newly established "state," thereby continuing to weaken the target country in the political, economic and military context (e.g. Eastern Ukraine). A sub-variant is an open invasion under the pretext of "peacekeeping" or "crisis management."

c. Lasting limitation of the strategic freedom of movement of the attacked country:

   i. Loss of territory (e.g. economy, population, infrastructure) results in severe economic hardship, domestic political destabilization and possibly grave humanitarian crisis; and

   ii. Lacking full control over its territory, the attacked country is unable to join any political or military alliance that requires territorial integrity.[65]

Eastern European researchers also studied the conflict in the Ukraine, particularly the Russian application of hybrid warfare, and they too developed a framework for a hybrid campaign. Their interpretation included eight distinct phases:

Phase 1 – non-military asymmetric warfare (encompassing information, moral, psychological, ideological, diplomatic, and economic measures as part of a plan to establish a favorable political, economic, and military setup);

Phase 2 – special operations to mislead political and military leaders by coordinated measures carried out by diplomatic

channels, media, and top government and military agencies by leaking false data, orders, directives, and instructions;

Phase 3 – intimidation, deceiving, and bribing government and military officers, with the objective of making them abandon their service duties;

Phase 4 – destabilizing propaganda to increase discontent among the population, boosted by the arrival of Russian bands of militants, escalating subversion;

Phase 5 – establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private military companies in close cooperation with armed opposition units;

Phase 6 – commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions. All types, forms, methods, and forces, including SOF, space, radio, radio engineering, electronic, diplomatic, and secret service intelligence, and industrial espionage;

Phase 7 – combination of targeted information operation, electronic warfare operation, aerospace operation, continuous air force harassment, combined with the use of high precision weapons launched from various platforms (e.g. long-range artillery, and weapons based on new physical principles, including microwaves, radiation, non-lethal biological weapons); and

Phase 8 – roll over the remaining points of resistance and destroy surviving enemy units by special operations conducted by reconnaissance units to spot which enemy units have survived and transmit their coordinates to the attacker's missile and artillery units; fire barrages to annihilate the defender's

resisting army units by effective advanced weapons; airdrop operations to surround points of resistance; and territory mopping-up operations by ground troops.[66]

The Russian use of hybrid warfare in the Crimea provides an excellent example of its efficacy. As one Estonian official noted, "in the hands of Russia hybrid warfare could cripple a state before that state even realizes the conflict had begun, and yet it manages to slip under NATO's threshold of perception and reaction."[67] In essence, the skillful use of an opponent's full range of resources (e.g. diplomatic, economic, informational, military) coordinated carefully across time and space, enabled by technology and the globalization of information, economies, if not societies, has created vast opportunities for crippling a target without the recourse to internationally recognized war.

The "New" Threat

Whether at the tactical/operational or the strategic level, hybrid warfare represents a major threat. Its methodologies are all encompassing and go beyond the conventional thinking to which military and political decision-makers are accustomed. Each is constrained by their education, training and experience. As such, there is a tendency to see the world/operations in terms of how we conduct diplomacy, operations and/or war. The failure to realize others utilize a different "playbook" leads to failure and crisis. Operations in Afghanistan, Iraq and the current problem with Hezbollah, the Islamic State and other terrorist entities around the globe are examples of an inability to recognize the threat of hybrid warfare until substantial damage has been done.

At the strategic level a significant problem is the fact that a target country is normally not even aware it is under attack until it may be too late. This phenomenon is not hard to understand. First,

politically there is tendency to trust other international actors and institutions, despite historic precedence. Moreover, even if distrust is present, there is certainly no inclination to act forcefully unless there is international consensus and blatant violations of international law that can be clearly proven. Within a democratic institution or coalition, reaching consensus is normally a long, painful process. The slow response to the annexation of the Crimea and occupation of the Donbass region in the Ukraine, the metamorphism of Hezbollah, and the expansion of the Islamic State are but three examples.

Second, governments and their electorates are far more concerned about economic prosperity rather than potential dangers of selling off key components of a nation's economy. As such, foreign investment is seen through the filter of opportunity rather than a potential threat. For example, the sale of key segments of Canada's resource, transportation or manufacturing sectors, although potentially a short-term win for politicians because of the infusion of investment dollars and the increase in jobs, represents a potential threat if the control rests in the hands of a potential adversary such as the Chinese or Russians. Moreover, large deficits, often funded through bond issues, also open a country to potential pressure by external powers financing the debt.

Third, the Western liberal democratic tradition holds personal freedoms sacrosanct. As a result, there is a near apoplectic reaction to any attempt to monitor or investigate individuals or organizations that may be manipulated by a foreign power but represent a distinct national interest group. The ability to create social discord or political dissent that can paralyze or consume a target government is after all a major instrument in the hybrid warfare playbook. As a result, an adversary can easily manipulate vulnerabilities in a target society by creating incidents or financing agitators. The potential threats are legion. One need only look at

some of Canada's own hot-button issues such as eco-terrorism/extremism, First Nation land rights/political aspirations/social issues, and Quebec separatism. Notably, the revelation that "legitimate" groups that advance these example causes, would trigger a major outcry and condemnation that it represents an affront to the constitution.

Finally, competition between governmental organizations, law enforcement and/or intelligence/security agencies can create bureaucratic barriers that may fail to detect an adversary's thrusts into a target society. Although the contemporary security environment has necessitated a closer working relationship between agencies, particularly security and intelligence agencies, a degree of "stove-piping" still transpires as protection of careers, budgets, institutional reputation and practices, as well as information is undertaken.

The insidious nature of hybrid warfare methodologies is another reason it poses such a great threat. By intent the very actions designed to undermine and weaken a target are also intended not to be detected or identified as an attack. For instance, in June 2016, A *New York Times* investigation revealed a web campaign that attempted to create panic in the US by spreading bogus Twitter messages, Wikipedia pages, and online news reports on topics such as an Islamic State attack in Louisiana, Ebola outbreaks and police shootings in Atlanta. The perpetrators were identified as Russian financed and being launched from a Kremlin-backed "troll farm" in St. Petersburg.[68] Researchers from the Geneva Centre for Security Policy explained that "'troll factories' consistently challenge the narratives in national and global media." They asserted that there has been a vast "improvement in the quality and quantity of disinformation, which has unfortunately been successful in having an impact in the opinions of both decision-makers and those of ordinary citizens."[69]

The large numbers of cyber-attacks that have transpired further demonstrate the reach and power of hybrid warfare methodologies. Members of the German parliament, as well as hundreds of private sector companies, SONY being but one graphic example, have been subjected to elaborate cyber-attacks. In fact, as has been shown already, key infrastructure and decision-making bodies have been crippled through cyber-attack.

To further understand the danger hybrid warfare poses, it becomes useful to examine the "Kremlin Tool Kit" as described by researchers from the Institute of Modern Russia:

- The Kremlin exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods.
- The Kremlin is increasing its "information war" budget. RT, which includes multilingual rolling news, a wire service and radio channels, has an estimated budget of over $300 million, set to increase by 41% to include German- and French-language channels. There is increasing use of social media to spread disinformation and trolls to attack publications and personalities.
- Unlike in the Cold War, when Soviets largely supported leftist groups, a fluid approach to ideology now allows the Kremlin to simultaneously back far-left and far-right movements, greens, anti-globalists and financial elites. The aim is to exacerbate divides and create an echo chamber of Kremlin support.
- The Kremlin exploits the openness of liberal democracies to use the Orthodox Church and expatriate NGOs to further aggressive foreign policy goals.

- There is an attempt to co-opt parts of the expert community in the West via such bodies as the Valdai Forum, which critics accuse of swapping access for acquiescence. Other senior Western experts are given positions in Russian companies and become de facto communications representatives of the Kremlin.

- Financial PR firms and hired influencers help the Kremlin's cause by arguing that "finance and politics should be kept separate." But whereas the liberal idea of globalization sees money as politically neutral, with global commerce leading to peace and interdependence, the Kremlin uses the openness of global markets as an opportunity to employ money, commerce and energy as foreign policy weapons.

- The West's acquiescence to sheltering corrupt Russian money demoralizes the Russian opposition while making the West more dependent on the Kremlin.

- The Kremlin is helping foster an anti-Western, authoritarian Internationale that is becoming ever more popular in Central Europe and throughout the world.

- The weaponization of information, culture and money is a vital part of the Kremlin's hybrid, or non-linear, war, which combines the above elements with covert and small-scale military operations. The conflict in Ukraine saw non-linear war in action. Other rising authoritarian states will look to copy Moscow's model of hybrid war—and the West has no institutional or analytical tools to deal with it.

- The Kremlin applies different approaches to different regions across the world, using local rivalries and resentments to divide and conquer.

- The Kremlin exploits systemic weak spots in the Western system, providing a sort of X-ray of the underbelly of liberal democracy.

- The Kremlin successfully erodes the integrity of investigative and political journalism, producing a lack of faith in traditional media.

- Offshore zones and opaque shell companies help sustain Kremlin corruption and aid its influence. For journalists, the threat of libel means few publications are ready to take on Kremlin-connected figures.

- Lack of transparency in funding and the blurring of distinctions between think tanks and lobbying helps the Kremlin push its agendas forward without due scrutiny.[70]

In sum, the threat posed by hybrid warfare is substantial. Its application is insidious as it deludes decision-makers into separating the specific tactics being utilized by an adversary from the actual strategic level political objectives that are driving their campaign. In short, it becomes hard to recognize that one is under attack or at "war." As such, it becomes difficult to recognize the seemingly disconnected series of events as a carefully synchronized campaign designed to achieve specific political objectives.

Countering Hybrid Warfare

A prevalent criticism against the West at present is that it is reacting to hybrid attacks rather maintaining the initiative. As such, it is necessary to first understand the threat and then develop the necessary counter measures. The largest factor is the complacency that often exists. From a tactical/operational perspective it is often difficult for commanders at all levels to see beyond their training

and theoretical understanding of war and how it should be fought. From a strategic point of view it is often difficult to recognize the peril that exists and differentiate it from the normal clutter of day-to-day "political" life. For these reasons it is important to develop clear national strategy for countering hybrid warfare.

The first step is education. It is important that the national security infrastructure, as well as the political leadership and society as a whole comprehend the nature of hybrid warfare, its characteristics, means and political objectives. As part of this process, national vulnerabilities should be identified (e.g. economic susceptibilities, social cleavages, political frailties). Parallel to these efforts "trip wires" must be identified that can signal a potential attack and defensive mechanisms put into place. Next, practitioners in the security sectors (e.g. intelligence, military, law enforcement) must be especially well-informed with regard to hybrid warfare so that they can continually monitor events, protect core institutions and functions from malicious activities and provide early warning, act proactively or at a minimum react immediately to defuse a potential crisis initiated as part of a hostile attack.

Important to a robust defence against hybrid warfare is a comprehensive security approach. This approach begins with education but must extend into the larger society. All major stakeholders within a given state or society must share a common understanding of the threat and situational awareness. In essence, it is not only the government that takes the responsibility for countering hybrid attacks but rather the entire society, including the private sector and society at large. For instance, private industry can identify and inform on new, aberrant activities and practices that may be harmful to the nation or industry. It is important to know who is buying up key components within the economic sector.

In addition, the media can strengthen its efforts to verify the accuracy of information prior to widespread dissemination to

prevent malicious disinformation intended to inflame targeted audiences; service providers can restrict accounts of those who use them to radicalize, agitate or attempt to create hate; and special interest forums can pressure members to transparently disclose funding sources (or, alternatively, citizens can support their government in monitoring those that fail to do so). Quite simply, it is very important to know who is financing protest and special interest groups.

However, this collaborative form of national security requires a shared understanding of the threat, risks and defence concept. As such, it relies on strong political leadership and a government that is credible and transparent. This requirement entails information sharing and a cooperative relationship with the private sector, particularly the media.[71]

Another key component to the defence against hybrid threats is the battle for the narrative, or in other words, strategic communications. A robust, well-informed, aggressive effort must be placed into disseminating information that lays out a narrative that explains national intentions and actions, as well as challenging disinformation and competing storylines. This sharing of information is extremely difficult and does not guarantee people will always accept what is being said. For that reason, truth, transparency and credibility must always be paramount. An understanding of audiences is key to ensure the proper messages are formulated and the correct media utilized to reach the intended "targets" with the proper effect. In essence, it is absolutely critical to align the strategic narrative to the objectives desired. It is for this reason that researchers argue that cyber and media power become instrumental in both offensive and defensive hybrid war.[72]

Counter measures to hybrid warfare can also take on a more aggressive form. The application of economic sanctions, the deployment of military forces, diplomatic actions, restrictions on media

and focused cyber counter-measures can all signal to adversaries that the cost of their actions may entail too great a cost to continue. Additionally, counter intelligence efforts can be focused on foreign countries that are known to utilize hybrid warfare (e.g. Russia, China) to block their efforts at subverting or manipulating target societies. It is important that analysis is continually conducted to detect adversary preparations or attacks. As such, an effort must be made to expose their actions and destroy their networks.

Finally, military force can be used. For example, when the Estonian top military commander, General Riho Terras, was queried on how he would "counter 'green men' crossing the border from Russia," he bluntly asserted, "You shoot the first one to appear."[73] The grandiloquent statement is more than bluster. As some researchers have noted, as long as the defender has the requisite "military strength to be able to prevail in the initial, limited conflict fought under the guise of a purely internal armed struggle," this counter-hybrid warfare strategy is viable. After all, the aggressor normally attempts to keep their actions below the trip-wire of overt international intervention and war.[74]

A NATO working group studying hybrid warfare promulgated a number of lessons with regard to defence against hybrid threats drawn from their observations of adversary actions. These can be informative in assisting in the development of a national program. The NATO report stipulated that the key lessons to apply include:

- Unite the efforts of the civic society and the government for the analysis of the threats and opportunities offered by the new information environment and related levers of influence which can be applied by an adversary;
- Strengthen the national media landscape by offering plurality of high-quality content, encouraging and

protecting investigative journalism, and addressing the transparency of media ownership;

- Support the quality content in the languages of minorities through Public Broadcasting as well as exploring alternative platforms like online and social media. This can be implemented effectively only after an accurate target audience analysis has been performed in order to understand not only the media consumption habits but also clear the general characteristics and interests in order to make the content and delivery methods relevant;

- Develop the content-sharing platforms with partner countries for Russian-language content corresponding to Western standards (news and entertainment) in order to decrease costs and promote common effort;

- Support the grass-root initiatives for exposing manipulated or fake information in the traditional, new and social media, and encouraging international cooperation for sharing the findings and alerting the public;

- Develop the mechanisms for the identification of the organized political trolling; monitor, prevent and investigate the social cyber-attacks and introduce laws defining liability;

- Significantly strengthen the national authorities responsible for the media monitoring in order to prevent illegal, hostile content engaging in hate-speech, promoting acts of violence and war and spreading falsified information;

- Introduce the mass media and digital media literacy as a part of the standard school curriculums in order to ensure critical thinking of the society;

- Strengthen the international cooperation in terms of cyber security and developing legal language to reflect the evolving threats in the social media platforms.[75]

Is Canada Prepared?

In light of the threat that hybrid warfare poses, the question becomes, is Canada ready? Importantly, the immediate thought is – does it have to be? Is Canada actually threatened? After all, capability and effort must be juxtaposed against actual risk. Equally significant, however, is the fact that complacency and blissful ignorance must not be taken for due diligence. Although Canada is often seen, as Raoul Dandurand described to the League of Nations in the 1920s, as "a fireproof house far from conflagrations," the reality is quite different.[76]

For instance, as Canadian troops deploy to the Middle East and/or North Africa, as well as other potential trouble spots in the years to come, they will face adversaries that utilize the full breadth of hybrid warfare to achieve their political objectives. At the strategic level, Canada will continue to face opponents in its exercise of its national interests, whether territorial, economic or resource related (e.g. the Arctic), or diplomatic/political (e.g. Russia, Syria, Iran). In addition, as a member of a number of alliances and coalitions, adversaries may wish to distract and disrupt Canadian efforts by targeting it for hybrid attacks, thereby shifting its focus onto more domestic, pressing issues and away from international affairs.

As a result, Canada is at risk and should have a strategy for countering, if not engaging in, hybrid warfare. Unfortunately, complacency and a failure to fully recognize, understand and/or perceive that there is a threat dampens the nation's ability to counter hybrid warfare. This failure to acknowledge the threat (or capability) that exists eliminates the necessary top level leadership to ensure a comprehensive societal approach. Although individual methodologies (e.g. cyber, intelligence, foreign investment review protocols) are addressed as significant factors with regard to national security, they are not necessarily coordinated or "calibrated" to see events through a lens of potential hybrid attacks. In short, as noted early, the security infrastructure, although better partnered than in years past, is still largely focused on traditional threat streams.

For instance, the Department of National Defence (DND) is arguably the most advanced of the governmental departments in its education with regards to hybrid warfare. It is a topic covered on courses, a short concept paper has been written by CAF Force Developers, a monograph was produced by the Canadian Special Operations Forces Command and a number of DRDC research papers have been written (mainly on the use of Russian information war). Moreover, a hybrid warfare scenario has been produced to assist with force capability requirement. These efforts, however, are largely tactical in nature and far from comprehensive.

In fact, little Canadian-specific research and analysis has actually been conducted on the topic. Moreover, the Force Development scenario designed fits neatly into the "Afghanistan reboot" category. In fact, the scenario is based on a failing state of Pakistan, saddled with an insurgency, which now requires an international effort to save it. The hybrid warfare component deals almost exclusively with the insurgent threat and the asymmetric tactics they employ.

Furthermore, influence activities are still not fully recognized for the important driver they are. Arguably, they are still seen as an ancillary capability. Moreover, strategic communication, and its importance, is not fully embraced as a tool to achieve military and political objectives. Finally, the staff officer sent to the NATO working group on hybrid warfare was sent with no higher direction or national position. He was deployed armed only with his perspective of what the Canadian position should be, since there actually was none.

In the end, there is a recognition that hybrid warfare exists. To most it is manifested at the tactical/operational level, specifically through asymmetric methodologies utilized by non-state actors and insurgents to achieve military and political objectives. The Russian use of hybrid warfare in Ukraine is also widely recognized as both a clever and sinister application of state power to achieve a political goal without triggering an actual war with the West. However, there seems to be a glass wall. There appears to be an inability to stretch the agility of thought beyond the conventional paradigm of international conflict and war. Or, perhaps it is a calculated decision – the risk assessment being that the time, effort and expense of educating and mobilizing the nation to develop a comprehensive societal approach to countering hybrid warfare is just too hard or expensive to do. In the end, arguably, the nation is not yet fully prepared.

Colonel Bernd Horn, OMM, MSM, CD, PhD is a retired Regular Force infantry officer who has held key command and staff appointments in the Canadian Armed Forces, including Deputy Commander of Canadian Special Operations Forces Command, Commanding Officer of the 1st Battalion, The Royal Canadian Regiment and Officer Commanding 3 Commando, the Canadian Airborne Regiment. He is currently the Director of the Canadian Special Operations Forces Command Professional Development Centre, an appointment he fills as a reservist. Dr. Horn is also an adjunct professor of the Centre for Military and Strategic Studies, University of Calgary, as well as an adjunct professor of history at the Royal Military College of Canada. He has authored, co-authored, edited or co-edited 40 books and well over a hundred monographs/chapters/articles on military history, Special Operations Forces, leadership and military affairs.

NOTES

1 Dr. Emily Spencer, "Back to Basics: Old School Rules," in Dr. Emily Spencer, ed., *"By, With, Through": A SOF Global Engagement Strategy* (Kington: CDA Press, 2014), 66.

2 Ibid., 66. See also Stuart Lyle, "Maoism versus 'Hybrid' theory - Is the military being distracted by this latest doctrinal buzz-word?" *UK Defence Forum*, http://www.ukdf.org.uk (December 2011).

3 Carl von Clausewitz, *On War,* edited by Michael Howard and Peter Paret (New York: Alfred A. Knopf, 1993), 83.

4 Ibid., 99.

5 George Kennan, Policy Planning Staff Memorandum, "The Inauguration of Organized Political Warfare," May 4, 1948, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm (accessed 29 January 2016). Interestingly, in 1953, the US Army in describing the role of the new "Lodge Act Soldier" (a result of the Alien Enlistee Act of 1950, the Lodge-Philbin Act, which allowed the US Army to enlist foreign nationals from certain European countries, which would then allow them to conduct irregular warfare) the documentary film described: *They have launched a subtle war of diplomatic maneuver, propaganda, deception, and calculated intimidation. It is a war of incidents rather than campaigns. It is a war in which carefully timed show of force can be more effective than a pitched battle. It is an economic, political, and psychological struggle. It is the sort of war that is new to the American Army.*
The Big Picture, Episode: "The Lodge Act Soldier," 1953. https://www.youtube.com/watch?v=ez8oC38IEXU (accessed 18 March 2016).

6 John F. Kennedy, "Remarks at West Point to the Graduating Class of the U.S. Military Academy," June 6, 1962, http://www.presidency.ucsb.edu/ws/?pid=8695 (accessed 25 January 2016).

7 Ministry of Defence (UK), *Strategic Trends Programme: Future Character of Conflict*, 13.

8 Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War,'" *Kennan Cable*, No. 7 (April 2015), 1.

9 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 7 and 116-117.

10 Quoted in András Rácz, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA Report 43, 29.

11 Colonel John McCuen, "Hybrid Wars," *Military Review* (March-April 2008), 108. http://www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf (accessed 25 January 2016). According to McCuen, contemporary hybrid wars are fought on three decisive fronts:

1. The Conventional battleground, which holds both symmetrical and asymmetrical threats.
2. Host nation population (i.e. where operations are conducted). He identifies a need to attain the support of the often hostile and/or alienated population.
3. Domestic population, whose support is essential for long, protracted wars.

McCuen also believes that it is important to cease "planning operationally and strategically as if we were going to be waging two separate wars, one with tanks and guns on a conventional battlefield, the other with security and stabilization of the population. Symmetric and asymmetric operations are critical, interrelated parts of hybrid war, and we must change our military and political culture to perceive, plan, and execute them that way. To become effective modern warriors, we must learn and retain the lessons of the past; we must strategize, plan, and conduct war under a new paradigm—hybrid war." Ibid.

12 Aapo Cederberg and Pasi Eronen, "How can Societies be Defended against Hybrid Threats?" *Strategic Security Analysis*, Geneva Centre for Security Policy, September 2015, No.9, 2. Importantly, they

identified that "the multi-pronged hybrid threat demands that defence planners engage all parts of society in defensive efforts. Intergovernmental or interagency efforts are not enough anymore."

13 Colonel Margaret S. Bond, "Hybrid War: A New Paradigm for Stability Operations in Failing States," Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 30 March 2007), http://www.comw.org/qdr/fulltext/0703bond.pdf (accessed 28 January 2016).

14 Timothy McCulloh and Richard Johnson, *Hybrid Warfare* (Tampa: JSOU Report 13-4, August 2013), 56. They describe a "hybrid force" as "a military organization that employs a combination of conventional and unconventional organizations, equipment, and techniques in a unique environment designed to achieve synergistic strategic effects." Ibid., 2.

15 Quoted in ibid., 10.

16 Quoted in ibid., 12.

17 Definition adopted in support of U.S. Joint Forces Command hybrid war conference held in Washington, D.C., February 24, 2009. Quoted in Dr. Russell W. Glenn, "Thoughts on 'Hybrid' Conflict," *Small Wars Journal*, http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf?q=mag/docs-temp/188-glenn.pdf (accessed 28 January 2016).

18 Glenn, "Thoughts on 'Hybrid' Conflict".

19 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007), 28. "Modern hybrid war practitioners apply "conventional capabilities, irregular tactics and formations, and terrorist acts including indiscriminate violence, coercion, and criminal activity" simultaneously." Ibid., 20-22.

20 Ibid., 8.

21 Quoted in András Rácz, Russia's *Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs, FIIA Report 43, 33.

22 M. Williamson and P. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press, 2012), 321.

23 Rácz, 41.

24 Hoffman, *Conflict in the 21st Century,* 11.

25 Neil Chuka and Jean François, *Hybrid warfare. Implications for CAF force development.* Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2014-R43, August 2014.

26 Nadia Schadlow, "The Problem With Hybrid Warfare," *War on the Rocks*, 2 April 2015, http://warontherocks.com/ (accessed 25 January 2016).

27 *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* (Prague: Jagello 2000, 2015), 8.

28 General Valery Gerasimov, Chief of the General Staff of the Russian Federation, "The Value of Science in Prediction," in "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows. Analysis and Assessment of Russian Crime and Security,* https://inmoscows-shadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (accessed 6 February 2015). Gerasimov stated, "Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."

29 Ibid.

30 Ibid.

31 Ibid. Gerasimov noted, "These days, together with traditional devices, nonstandard ones are being developed. The role of mobile,

mixed-type groups of forces, acting in a single intelligence-information space because of the use of the new possibilities of command-and-control systems has been strengthened. Military actions are becoming more dynamic, active, and fruitful. Tactical and operational pauses that the enemy could exploit are disappearing. New information technologies have enabled significant reductions in the spatial, temporal, and informational gaps between forces and control organs. Frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The defeat of the enemy's objects is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. The application of high-precision weaponry is taking on a mass character. Weapons based on new physical principals and automatized systems are being actively incorporated into military activity."

32 USSOCOM White Paper, *The Gray Zone*, 9 September 2015, 1.

33 They also noted, "It is hardly new, however. The Cold War was a 45-year-long Gray Zone struggle in which the West succeeded in checking the spread of communism and ultimately witnessed the dissolution of the Soviet Union." Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin, "Unconventional Warfare in the Gray Zone," National Defence University Press, January 01, 2016. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/643108/unconventional-warfare-in-the-gray-zone.aspx (accessed 18 January 2016).

34 Michael J. Mazarr, *Mastering The Gray Zone: Understanding A Changing Era Of Conflict*, Strategic Studies Institute and U.S. Army War College Press, December 2015, 1. The authors believed that gray zone conflict should be understood as having a number of characteristics:

- Pursues political objectives through cohesive, integrated campaigns;
- Employs mostly non-military or non-kinetic tools;

- Strives to remain under key escalatory or red line thresholds to avoid outright, conventional conflict; and,
- Moves gradually toward its objectives rather than seeking conclusive results in a specific period of time. Ibid., 58.

35 Howard Altman, "Army Gen. Joseph Votel calls the Islamic State 'a non-state actor attempting to operate like a state," *Tampa Tribune* (28 November 2015).

36 Antulio J. Echevarria II, "How Should We Think about 'Gray-Zone' Wars?" *Infinity Journal,* Vol 5, Issue 1, (Fall 2015), 16.

37 Deputy Secretary of Defense Bob Work, Speech at the U.S. Army War College Strategy Conference, April 8, 2015, available from http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1930 (accessed 29 January 2016). He added, "that's the zone in which our ground forces have not traditionally had to operate, but one in which they must now become more proficient."

38 See for example, Michael J. Mazarr, *Mastering The Gray Zone: Understanding A Changing Era Of Conflict*, Strategic Studies Institute and U.S. Army War College Press, December 2015, 84-85; Aapo Cederberg and Pasi Eronen, "How can Societies be Defended against Hybrid Threats?" Strategic Security Analysis, Geneva Centre for Security Policy, September 2015, No. 9, 3; and Philip Kapusta, "The Gray Zone," *Special Warfare,* Vol. 28, No. 4 (October-December 2015), 22.

39 Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of Strategic Studies*, Vol. 37, No. 2 (2014),198-221, http://www.tandfonline.com/doi/pdf/10.1080/01402390.2013.870071 (accessed 29 January 2016).

40 *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* (Prague: Jagello 2000, 2015), 11.

41 Hoffman*, Conflict in the 21st Century*, 9. See also, Aapo Cederberg and Pasi Eronen, "Wake up, West! The Era of Hybrid Warfare is Upon Us." The case of Russia is a good example. One study determined:

1. The "weaponization of information" is "a vital part of the Kremlin's hybrid, or non-linear, war";
2. The Kremlin "exploits the openness of liberal democracies." The Kremlin "exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or to earn credibility but to sow confusion via conspiracy theories and proliferate falsehood";
3. The Kremlin's "info weapon" is well funded. Russia Today (RT), a TV station that broadcasts in Russian, English, Spanish, Arabic, German and French, has an estimated budget of over US $300 million. Recently, the news agency RIA Novosti and the international radio broadcaster Voice of Russia, have been merged into "Sputnik", a multimedia news service. Sputnik is available in Russian, Chinese, Arabic, English, German, Polish, Spanish, Turkish and other languages. In addition, the Kremlin is working with "trolls", paid commentators on the Internet.

Ulrich Speck and Anthony Seaboyer, *Russia's Information Warfare: Impact on the Ukraine Debate in Germany*. Defence Research and Development Canada Report 2015-C103, May 2015, 7.

42 Hoffman, *Conflict in the 21st Century*, 8.

43 Quoted in Glenn, "Thoughts on 'Hybrid' Conflict."

44 Ministry of Defence (UK), *Strategic Trends Programme: Future Character of Conflict*, 19.

45 Alex Deep, "Hybrid War: Old Concept, New Techniques," *Small Wars Journal* (2 March 2015), http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques?page=1 (accessed 28 January 2016).

46 Glenn, "Thoughts on 'Hybrid' Conflict."

47 Howard Altman, "Army Gen. Joseph Votel calls the Islamic State 'a non-state actor attempting to operate like a state," *Tampa Tribune*,

28 November 2015. Votel noted that a "key part of success in the Gray Zone is understanding how and why societies work, knowing the key players and cultures and motivations. It's all part of what the military and academics like to call the "human domain."

48 Rácz, 11.

49 Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly* 79 (4th Quarter 2015), 47. During the conflict in Georgia, Russia also undertook an aggressive cyber-attack campaign targeting at least 38 Georgian websites, including the website of the Georgian president, Ministry of Foreign Affairs, National Bank, Parliament, and Supreme Court. All attacks were assessed as being centrally managed and coordinated. *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* (Prague: Jagello 2000, 2015), 9.

50 Duggan, 47. A "Troll Army" is defined as "a state-sponsored team of commentators, using false identities, that participate in blogs, internet forums and social media to promote propaganda with the intention of swaying opinion, undermining dissident communities or changing the perception of what is the dominant view."

51 Janis Berzins, *Russia's New Generation Warfare In Ukraine: Implications For Latvian Defense Policy*, National Defence Academy Of Latvia Center For Security And Strategic Research, Policy Paper No 02 April 2014, 5.

52 Maria Snegovaya, *Putin's Information Warfare In Ukraine Soviet Origins Of Russia's Hybrid Warfare*, Institute for the Study of War, September 2015, 7, 10.

53 Ibid., 7, 10. Maria Snegovaya explains that reflexive control depends on the ability of the attacker "to take advantage of pre-existing dispositions among its enemies to choose its preferred courses of action. The primary objective of the reflexive control techniques Moscow has employed in the Ukraine situation has been to persuade the West to do something its leaders mostly wanted to do in the first place, namely, remain on the sidelines as Russia dismantled Ukraine. These techniques

would not have succeeded in the face of Western leaders determined to stop Russian aggression and punish or reverse Russian violations of international law." The author clarifies that reflexive control "is a method by which a controlling party can influence an opponent into unknowingly making bad decisions by interfering with its perceptions."

54 Ibid., 7, 10.

55 Duggan, 47. During the conflict in Georgia both waged an aggressive disinformation campaign making it difficult for outside observers to separate fact from fiction. The three main themes that dominated the information campaign were:

1. Georgia and especially President Saakashvili were aggressors.
2. Russia was forced to intervene to defend its citizens and to prevent a humanitarian catastrophe (defensive purpose); and
3. The West has no legitimate reason for criticizing Russia because Russia simply does what the West did in Kosovo in 1999.

Quoted in *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* (Prague: Jagello 2000, 2015), 9.

56 Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks* (11 March 2016). http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/ (accessed 18 March 2016).

57 Ibid.

58 Elina Lange-Ionatamishvili, *New Face Of War: Lessons From Georgia*, NATO Stratcom Center Of Excellence, ND, 5.

59 Ibid., 13.

60 Snegovaya, 13-14.

61 Rácz, 58-69.

62 Ibid. The report noted that political infrastructure was a prime targets as well. For instance the parliament building, the Supreme Council of Crimea, was seized on 27 February 2014, effectively preventing local political decision-making from functioning. In Donetsk, the regional state administration building was one of the first targets taken over in April 2014, and the building still serves as the headquarters of the so-called Donetsk National Republic.

63 Russian General Makhmut Gareev, in his book *If War Comes Tomorrow*, as early as 1995 argued that "the widespread use of electronic warfare, aimed at disrupting the functionality of enemy communication, radar systems and command and control." He believed, "the systematic broadcasting of psychologically and ideologically biased materials of a provocative nature, mixing partially truthful and false items of information […] can all result in a mass psychosis, despair and feelings of doom and undermine trust in the government and armed forces; and, in general, lead to the destabilization of the situation in those countries, which become objects of information warfare, creating a fruitful soil for actions of the enemy." Quoted in Rácz, 35.

64 Ibid.

65 Rácz, 58-69.

66 Janis Berzins, "Russia's New Generation Warfare In Ukraine: Implications For Latvian Defense Policy," National Defence Academy Of Latvia Center For Security And Strategic Research, Policy Paper No 02, April 2014, 6.

67 Quoted in Nadia Schadlow, "The Problem With Hybrid Warfare," *War on the Rocks* (2 April 2015). http://warontherocks.com/ (accessed 25 January 2016). The official also noted that hybrid warfare "allows NATO to avoid action because a range of activities – from the aggressive use of disinformation by Moscow, to economic pressure, to bribery and threats, to use of 'locals' to stir up protests – become conveniently categorized as being under the threshold of war."

68 Peter Pomerantsev, "Brave New War," *The Atlantic*, http://www.theatlantic.com/author/peter-pomerantsev/ (accessed 29 January 2016). The approach is not new. The author points out that "One of the most successful *dezinformatsiya* campaigns was spreading the theory that the CIA was behind the murder of President John F. Kennedy. The KGB sponsored studies and popular books that fired up conspiracy theories about the assassination. According to research conducted by Max Holland, they planted a fake letter in a friendly Italian newspaper, *Paese Sera*, that intimated that a New Orleans businessman called Clay Shaw, already under suspicion for being involved in the assassination, was a senior CIA operative." Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Interpreter Special Report, Institute of Modern Russia, 9.

69 Cederberg and Eronen, "How can Societies be Defended against Hybrid Threats?" *Strategic Security Analysis*, 7.

70 Pomerantsev and Weiss, 6.

71 See Cederberg and Eronen, 6-9 for the Finnish experience.

72 Ibid., 7.

73 Dan Altman, "The Long History of "Green Men" Tactics — And How They Were Defeated," *War on the Rocks*, (17 March 2016), http://warontherocks.com/2016/03/the-long-history-of-green-men-tactics-and-how-they-were-defeated/ (accessed 18 March 2016).

74 Ibid. SOF provides an excellent means of denying opponent entry and/or access to social networks and movements within own or friendly targeted countries. They also provide an offensive capability.

75 Elina Lange-Ionatamishvili, *New Face Of War: Lessons From Georgia*, NATO Stratcom Center Of Excellence, ND, 15. With regard to specifically countering Russian information warfare, a Canadian DRDC report recommended:

1. Enabling a free, open, broad and professional media landscape. A liberal public sphere contains the ability to correct itself as a built mechanism and also provides the necessary means to fight back against information campaigns, to correct errors and to enlighten the public about the workings of such propaganda;
2. Improving official communication. Western governments and international organization (such as NATO, EU, OSCE) should become much more robust and decisive in pushing back against the Russian information warfare;
3. Build a fact-checking team. What could be done to strengthen the resilience of international media against Russian propaganda is to fund an independent, professional team to do the fact checking in a timely and reliable manner, and to provide media with the relevant information through a website; and,
4. Disclose information about how the Russian information warfare works. Governments could inform publics on what they know about how Russia is trying to influence international opinion. Public knowledge about the mechanisms of the Kremlin can help audiences better understand the difference between a public sphere in a liberal democracy, which is guided by the regulative idea of objectivity, and the info war of an authoritarian regime, who's goal is to distort the truth.

Ulrich Speck and Anthony Seaboyer, *Russia's Information Warfare: Impact on the Ukraine Debate in Germany*. Defence Research and Development Canada Report 2015-C103, May 2015, 7.

76 Quoted in Steven K. Holloway, *Canadian Foreign Policy: Defending the National Interest* (Peterborough, ON: Broadview Press, 2006), 84.

CANSOFCOM PROFESSIONAL DEVELOPMENT CENTRE MONOGRAPHS

1. *More Than Meets the Eye: The Invisible Hand of SOF in Afghanistan*
   Colonel Bernd Horn, 2011.
2. *Squandering the Capability: Soviet SOF in Afghanistan*
   Major Tony Balasevicius, 2011.
3. *Military Strategy: A Primer*
   Dr. Bill Bentley, 2011.
4. *Slaying the Dragon: The Killing of Bin Laden*
   Colonel Bernd Horn and Major Tony Balasevicius, 2012.
5. *Between Faith and Reality: A Pragmatic Sociological Examination of Canadian Special Operations Forces Command's Future Prospects*
   Colonel Mike Rouleau, 2012.
6. *Working with Others: Simple Guidelines to Maximize Effectiveness*
   Dr. Emily Spencer and Colonel Bernd Horn, 2012.
7. *Operation Dawn in the Gulf of Aden and the Scourge of Piracy*
   Colonel Bernd Horn, 2012.
8. "*We Murder to Dissect": A Primer on Systems Thinking and War*
   Dr. Bill Bentley, 2012.
9. *Breaching Barriers: A Comprehensive Approach to Special Operations Decision-Making in Non-Traditional Security Environments*
   Major Steven Hunter, 2013.
10. *Chaos in Kandahar: The Battle for Building 4*
    Colonel Bernd Horn, 2013.
11. *"Little Giant Killer": The Bill Underwood Story*
    Dr. Emily Spencer with Robbie Cressman, 2013.
12. *From Assassins to Al-Qaeda: Understanding and Responding to Religious Terrorism*
    Kevin E. Klein, 2013.
13. *Amongst the Eagles: The Battle of Mount La Difensa*
    Colonel Bernd Horn, 2013.
14. *Innovation and Daring: The Capture of Fort Eben Emael, 10 May 1940*
    Colonel Bernd Horn, 2014.
15. *Foreign Fighters: A Clear and Present Danger*
    Colonel Bernd Horn, 2014.
16. *Fear: Dare Not Speak Thy Name*
    Dr. Emily Spencer and Colonel Bernd Horn, 2015.
17. *Escape and Evasion in the First and Second World Wars: Canadian Stories*
    Dr. Nathan M. Greenfield, 2015.
18. *Sapere Aude: Toward a CANSOF Officer Professional Development Model*
    Major R.D. Schmidt, 2016.


VIAM INVENIEMUS


VIAM INVENIEMUS
Professional Development Centre
centre de perfectionnement professionnel