CANIC 2017 Rapporteur's Summary

by Dr. David Charters, Senior Fellow, The Gregg Centre, University of New Brunswick

The theme of this year's conference was "**Hybrid Warfare and the Implications for the Canadian Intelligence Enterprise**". Nine speakers and panelists from the military, government, media, and research communities offered their expertise and perspectives on this topic. What follows is a summary of what I feel were the key themes that emerged from the totality of the presentations. The summary is organized as responses to four questions.

What's in a Name?

Everything. What we call things frames both our understanding of them and our responses to them. We are calling this phenomenon Hybrid Warfare, which suggests an amalgam or fusion of disparate parts. But the Russians call it Next Generation Warfare: This implies a transformation of warfare into something new. Another speaker observed that pairing the words Hybrid and Warfare immediately puts a 'military' frame on a problem that is more than just military. It is a Whole of Government if not Whole of Society problem. A panel member observed that the 'Fake News' phenomenon "should scare all of us." The obvious implication of this is that dealing with that particular aspect of Hybrid Warfare can't simply be left to the military, or even just to the intelligence community. That said, it is hard to escape the notion that in the Hybrid challenge we are confronting a form of warfare. Consider the methods that we have seen being used, not just in Russia's Near Abroad (Crimea/Ukraine), but also by the Islamic State when it invaded Iraq in 2014. What they demonstrated was an integrated and coordinated application of kinetic and non-kinetic activities designed to paralyse, disrupt, and defeat their enemies: conventional, unconventional, and special operations used in tandem with terrorism, information operations, subversion and influence operations, and intelligence activities. These techniques emphasized speed, surprise, deception, and often extreme violence, to disrupt their opponents' leadership, command and control, decision-making, communications, perceptions, and operations. They were meant to get inside the enemy's OODA Loop. And the target expanded to include the enemy's media, population, and its allies. So, if we remove the term warfare from this construct,

with what term do we replace it? Finding the answer to that question will require some brain-storming by both military and civilian thinkers.

Old Wine in New Bottles?

One speaker asserted that the West is facing the most dangerous threat environment in a generation. But he reminded us that Hybrid Warfare is not something entirely new. His recitation of the techniques used by the American rebels during their War of Independence was particularly apt. I reinforced his point by observing that Blitzkrieg was the Hybrid Warfare of its time (1939-41). It relied on the integrated exploitation of conventional and special operations, terror, subversion, and information operations (what was then called propaganda). The intent was the same as it is today: paralyze the enemy as a prelude to defeating them. On the media aspects, the problem of Fake News was recognized long before the Internet Age. During the Northern Ireland conflict in the 1970s, British Prime Minister Edward Heath was said to have remarked that: "A lie can be half way 'round the world before truth has got its boots on." Therefore, before we go searching for a whole new term for this problem, we might gain some useful insights by looking at its history.

So, What's New About Hybrid Warfare?

Technology. The Internet, smart phones, and cyber systems, tools, and weapons have "revolutionized" Hybrid Warfare. Several features of this phenomenon stand out. First, speed. Events occur or are reported faster than we can react to them. So, speed in recognizing the facts and features of Hybrid Warfare attacks is essential. Second, "information overload". Media, governments, intelligence services, and militaries are being bombarded simultaneously or in quick succession by more events from more places, each with a more compelling reason to respond to it. This condition favours the Hybrid Warrior who prefers persistence over plausibility. Sorting the wheat from the chaff (including the Fake News) is just half of the problem; deciding responses and prioritizing them is equally challenging. Third, reach. The FEBA is everywhere, not just where the kinetic fight is occurring. Because the most important fight is non-kinetic; it is for the public mind, and that takes place mostly online. Which brings us to the fourth implication: credibility (which is closely tied to the twin challenges of plausibility and deniability). The instantaneous broadcast of data and images without the filters of editing, source- and fact-checking, and context (central components of the print media in particular)

increases the scope and capacity for generating false data and images or for manipulating real ones. Compounding this is the very structure of the Internet. The ubiquity of networks, social media, nodes, and bots makes it easy to disguise the perpetrators of cyber attacks and/or influence operations. The Russian exploitation of social media outlets like Facebook and Twitter to disseminate ads designed to influence the American election campaign is just one example of this phenomenon. This case highlights a unique feature of the Russian approach: for them, information operations are not limited to wartime; they are non-stop. It also reminds us that while Hybrid Warfare is a 'macro' problem, its most vital aspects may play out at the 'micro' level, without us even realizing it. The implication of this (reinforcing what was noted earlier) is that Hybrid Warfare blurs the boundaries between domestic and expeditionary operations, between the military, intelligence, diplomatic, and policing domains of national security, and between these and the responsibilities of government, the media, and the citizenry themselves. This is a form of warfare that truly is "too important to be left to the generals".

What Does This Mean for the Intelligence Community?

As one panellist states, Intelligence problem is to detect, attribute, and then discern the enemy's intent and campaign. The Hybrid Warfare operator uses "noise" to avoid detection, force misattribution when detected, and offer benign or ambiguous narratives when attribution is achieved. Against this challenge another speaker staked out the intelligence community's ground in unambiguous terms: all operational activities in the Hybrid Warfare domain must be Intelligence-Led. That includes readiness to engage in and/or respond to Hybrid Warfare. But this means that those operations must be driven by commanders who believe in the concept. And the Intelligence community must be the pre-eminent voice in preparing the intelligence estimate for Hybrid Warfare operations. It is up to that community to develop an understanding of the problem, then to educate, advise, and warn commanders and their civilian political leaders. Others said that they need to see the guts of the process, the challenge of decision-making in uncertainty, and the consequences of missed decisions. The solution suggested, may lie in harnessing the capabilities of Artificial Intelligence (AI) to predict and detect Hybrid campaigns. It could be possible to model such campaigns using AI, Natural Language Processing, and Deep Learning systems. This might produce a useable AI prototype for predicting and detecting a campaign. But technological tools are only part of the solution. The CF intelligence community

can lead change to adapt to Hybrid Warfare only if they themselves are well-versed in knowledge of the problem. But, it was suggested that we aren't there yet. One speaker suggested that we need a new Intelligence workforce, while another asserted that what we need is a new training paradigm: one that prepares them not only to grasp the big picture of Hybrid warfare but also to recognize and make sense of what they see at the micro level. And we have to be able to see the world through the eyes of our adversaries. Given the multi-faceted, multi-jurisdictional nature of Hybrid Warfare intelligence sharing across agencies and other boundaries is essential. As things stand the Five Eyes community fights at the Secret level, but shares only at the Top Secret level. This can be fixed, but it requires a push from the top. Unfortunately, it may take a disaster to generate that push. And by then it may be too late. Because Hybrid Warfare is already here, and here to stay. We need to recognize this, and to realize that Canada is not a "fireproof house" and that time is not on our side.