Naval Affairs Program Briefing Note # 46

Information Operations & Warfare

In the years since the Second World War, many people have thought about war as the contest between opposing state military forces using weapons and behaving according to rules such as the Geneva Conventions. This vision is reinforced by television and movies, but it has never been accurate and certainly is not accurate now.

What we are seeing are growing complexities which now include threats from land and sea to space, cyber and information. We have asymmetric war, gray zone warfare and hybrid warfare in addition to the 'traditional' methods of war. We often think that there are clear lines between war and peace. But this has become less and less accurate. Often the lines are blurred. This is the case in terms of information operations. In this Briefing Note, we will examine information warfare/operations.[1]

What do we mean by this term? Depending on what sources you consult, 'information warfare/operation' has a variety of meanings. Technopedia defines information warfare as "the tactical and strategic use of information to gain an advantage."[2] For Western militaries, it is often placed in the category of electronic warfare or cyber security/warfare. In this category would be included Information Technology networks (like the internet, telecommunication networks, computer systems, and software and data within them) as well as infrastructure, users and related activities. The goal is to protect the availability, integrity and confidentiality of systems and/or the information they contain. (See BN #34 Cyber Security and the RCN.)

Some analysts, however, are beginning to place information operations outside the framework of cyber operations/security. Some would argue, as this Briefing Note does, that "[i]nformation warfare should be classified under two separate domains of warfare: the cyber domain (virtual) and a psychological domain (cognitive)."[3] Whereas cyber security involves the integrity of networked systems, information operations focus on shaping the battlespace through massaging 'facts' and influencing citizens. Information operations are about spreading propaganda or disinformation to demoralize or manipulate the enemy and its public, and undermine the quality of the opposing force's information. As Jeffrey Baptist and Julian Gluck argue, "[i]f warfare is an attack on the will or means to conduct the basic functions of statecraft, then an attempt to covertly subvert (especially deceptively) another nation's decision-making ability (democracy, public sentiment) is as nefarious an action as a blockade or skirmish."[4] This Briefing Note will focus on the psychological elements not the cyber elements.

What we are discussing here is not new. Military strategists from Sun Tzu to Carl von Clausewitz to Mao Zedong have contributed to the discussion of fighting and winning wars.

[1] Information warfare vs. information operations? Unlike Westerners, the view in Asia, for example, is that "IW appears to have borrowed too much from conventional understandings of war fighting. IO is the broader, more important discipline to read or to deflect an enemy without distinguishing between peacetime and wartime." See Alan Chong, "Information Warfare? The Case for an Asian Perspective on Information Operations," *Armed Forces and Society*, Vol. 40, No. 4 (2014), p. 619.

[2] "Information Warfare, What Does Information Warfare Mean?" *Technopedia*, Last updated: January 4, 2017.

[3] Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," *Strategic Studies Quarterly*, Fall 2018, p. 86.

[4] Jeffrey Baptist and Julian Gluck, "The Gray Legion: Information Warfare within our Gates," *Journal of Strategic Security*, Vol. 14, No. 4 (2021), pp. 38-9.

Their discussion includes elements that are becoming prevalent once again – information operations. In his book *The Art of War*, Sun Tzu wrote that "all warfare is deception," and that "[t]he supreme art of war is to subdue the enemy without fighting."[5] He wrote that information is part of treating war as a game of deception. In the early 1800s, Carl von Clausewitz wrote that war is the continuation of politics by other means – and the means need not be military.

Thus it is not new to use disinformation and deception in warfare. Nor are psychological operations new since states have long used propaganda. The Allies perpetrated widespread deception/misinformation in the run up to the D-Day invasion in WWII. The Soviet Union used propaganda (agitprop) widely during the Cold War. The KGB had thousands of officers working on psychological and (dis)information warfare, and the office was not dismantled after the Cold War ended. What's new is the technology available to propagate and spread mis/disinformation and shape the battlefield. The invention and widespread adoption of the internet and social media has been a game changer for information operations.

What makes information operations via social media effective is that they are low cost, much cheaper than funding a conventional military with all its weapons and equipment. The operations are anonymous so the target may not know the source of the information. Actors avoid conventional confrontation, and hide behind anonymity. Attribution – i.e., determining who is behind false information – is time-consuming and difficult, which means deniability is high. With easy access to social media and some elements of traditional media (that are foreign funded, do not check sources or are politically motivated), information operations are cheap and effective.

Russian general Valery Gerasimov claims that information warfare can, in only a few days, transform a society into "a web of chaos, humanitarian catastrophe, and civil war... The scale of casualties and destruction ... are comparable with the consequences of any real war."[6] The so-called 'Gerasimov doctrine' claims 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 or weapons in their effectiveness."[7]

Why would foreign states conduct information operations? The West/United States is too powerful to engage militarily, so enemies focus on other spheres. Information operations promote inaccurate or false information that undercuts trust in government (and fellow citizens) and thus influence citizens' votes, exacerbate cleavages (eg., about race, immigration, crime), promote demonstrations that sometimes involve violence, create the view that elites are the enemy, and in general divide society.[8] Citizens are so busy questioning and fighting each other that they ignore the world, slow down decision-making and make it less consensual, which can create a vacuum of power and interest. The result? "If the state cannot extract from its people the will to ensure internal order (state making), exert force upon external rivals (war making), or check rivals to state power internally and externally (protection, analogous to counterterrorism), then the state may as well be defenseless throughout, if not entirely defunct."[9]

[5] Sun Tzu, *The Art of War*, translated by Lin Wusun, second reprint (Beijing: Foreign Languages Press, 2005), p. 3.
[6] Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military-Industrial Kurier*, 2016, p. 24. Translated by Robert Coalson, in *Military Review*, Vol. 96, No. 1 (2016).
[7] Nick Brunetti-Lihach, "Information Warfare Past, Present, and Future," RealClear Defense, 14 November 2018, https://www.realcleardefense.com/articles/2018/11/14/ information_warfare_past_present_and_future_113955.html
[8] Hans Klein, "Information Warfare and Information Operations: Russian and US Perspectives," *Journal of International Affairs*, Vol. 71, No. 1.5 (Special Issue 2018).
[9] Baptist and Gluck, "The Gray Legion," p. 41.

Let us use an example that has been in the news lately – Russia. It is clear that Russia has developed multiple capabilities for information warfare. It is a whole-of-government approach, and whole-heartedly adopted by the military. It is said that the 'Kremlin Troll Army' can "sow discord, spread fear, influence beliefs and behaviors, discredit institutions, diminish trust in the government and ultimately destroy the possibility of using the internet as a democratic space."[10] The Russian Bulletin of the Academy of Military Sciences notes that "[t]he victim country does not even suspect that it is being subjected to information-psychological influence. This leads in turn to a paradox: the aggressor achieves his military and political aims with the active support of the population of the country that is being subjected to the influence."[11] The idea is to create messages to alter adversary's perceptions of a situation, and in a best-case scenario guide the public of the adversary into pushing for decisions that are likely not in their country's interest.

What is the view in the West? The idea of 'total war' fell out of fashion in the West after the invention of atomic weapons. Total war meant the mobilization of the whole of society in order to win, but with atomic weapons, that was thought to be dangerous and, with deterrence, unnecessary. However, outside of the West, many states still see 'war' as a whole-of-government activity to be conducted even during what we in the West think of as peace-time. Thus, certain states and non-state bodies – Russia, China, the Islamic State/ISIS for example – have used information operations very effectively. Western states are less effective at this.

The beauty of using information operations against the West is that a fundamental tenet of democracy is freedom of information/speech. Information flows freely and can be used for unscrupulous purposes. Whole populations can be reached through social media and influenced at low cost in real-time. Information operations do not work as well in non-democratic places because there is no freedom of speech and dissent is not allowed. Information operations can damage reputations of leaders, provide details of events that the domestic government is withholding and encourage disillusionment, but these operations are much more difficult.

But the main difference is that the West has not grasped the power of information operations being used by its adversaries. The West has economic and diplomatic power, and the United States in particular has military power, but "foolishly, however, it has ceded the information arena to those with malicious intent."[12] The West sees war in a different way than adversaries – *we* think we are at peace right now, but *they* are already working to undermine the West.

In the West, information is seen as valuable but the focus is information that enhances military operations (eg., more accurate knowledge of adversary movements and location of targets through networks, sensors and satellites), not information that affects the perceptions and ideas of a target population. While adversaries blend political and military operations, the West avoids including political considerations in military campaigns. Thus, "military success is presumed to lead inexorably to a favorable political outcome overseas."[13] There is a difference between means and will in warfare. In the West, we focus on the means (ships, planes, weapons) but not on the will (whether citizens agree to use the means).[14] Adversaries do not make this mistake. This is a problem.

There is some movement to change this. There is now recognition of the extent of foreign

[10] Ajir and Vailliant, "Russian Information Warfare."
[11] Russian Bulletin of the Academy of Military Sciences. Quoted in Ajir and Vailliant, "Russian Information Warfare."
[12] Baptist and Gluck, "The Gray Legion," pp. 39-40.
[13] Brunetti-Lihach, "Information Warfare Past, Present, and Future."
[14] See Baptist and Gluck, "The Gray Legion," p. 40.

meddling via social media in the countries of the West. Western countries are forming agencies to attempt to address and counter foreign disinformation. The response has been a mixture of civilian and military activity.

Conclusions

Since the end of the Cold War, the United States has assumed that it will win wars because it has military superiority. But in war, it is not always the strong that wins. Weaker powers utilize asymmetric warfare – they fight in ways that overcome their weaknesses or capitalize on the weaknesses of the enemy. Clausewitz talked about the 'fog of war' as a factor in victory – in modern times, information operations have thickened the fog because of problems with attribution, outright lies and loss of credibility leading to lack of will.

In conflicts in Afghanistan, Iraq, Syria, for example, social media preempted, shaped or denied 'facts' on the ground faster than could happen through Western military or government means. This (dis)information shaped the perceptions of both local and international actors, and affected government decisions. Deployed Western militaries are slow to release information as it travels through multiple layers of public relations before release. By the time information is released, the 'facts' of a situation have been created and perceptions have already been formed. And at home, slow action on releasing information and countering disinformation allows foreign operations to massage and deform the discourse.

The bottom line? Ancient theorists of war knew that the objective is *winning* – to subdue the enemy without fighting, as Sun Tzu wrote. The West needs to recognize this. Information operations "can prepare the battlefield and set the conditions for victory. Information can soften the enemy's will to fight, deceive, and pollute his or her decision-making cycle. Given the variety of media capable of using information to influence, coerce, or deceive, it is conceivable information operations may surpass fire and maneuver in importance at times."[15] Militaries do not need to join in the game of deceit, but the West needs to recognize that information operations are being undertaken at home. At a minimum, militaries and governments can increase the amount and speed of information they release, and state agencies can work to identify foreign (and/or domestic) sources of disinformation and counter the disinformation.

[15] Brunetti-Lihach, "Information Warfare Past, Present, and Future."