RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Analysis

The Challenges of Hybrid Warfare

Eve Hunter with Piret Pernik

April 2015

ISSN 2228-2076

International Centre for Defence and Security
Toom-Rüütli 12-6, 10130 Tallinn, Estonia
info@icds.ee, www.icds.ee
Tel.: +372 6949 340
Fax: +372 6949 342

ICDS Analysis
ISSN 2228-2076

Introduction

Russia's invasion of Ukraine has sparked a rethinking of traditional geopolitical norms and warfare tactics. For this reason, ICDS convened a panel of experts to shed light on recent developments and in particular, Russian use of hybrid warfare. This report is largely drawn from discussions with those experts.

"Hybrid war" is defined by analyst and author Frank Hoffman as a "blend of the lethality of state conflict with the fanatical and protracted fervor of irregular war." [1] The expanded definition is as follows:

> *Sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion.*[2]

The international community has almost universally accepted the term hybrid warfare to refer to Russia's invasion of Ukraine. As many have recognized,[3] hybrid war in itself is not a new concept, but many of the technologies used inspire new challenges. Current debate surrounding cyber threats include basic terminology agreements, strategy, and national and international information sharing, to name a few. This lack of clarity and paucity of specified norms for how to deal with cyber threats in general and the situation in Ukraine in particular has only added to the weaknesses in the international system that Russia is exploiting.

Currently, we lack a legally or politically-recognized division with which to determine at what point network intrusion and sabotage becomes an act of war. These issues are of particular concern for the Baltic States, which are some of the most at risk for Russia's aggressive expansionist policies. In fact, NATO has even committed to new battle command stations in Estonia, Latvia, and Lithuania as of February 2015. Taking these vulnerabilities into consideration, this analysis will examine hybrid warfare and Russian politics more generally.

Meeting strategic goals

Russia's convergence of a variety of war tactics to bring about "hybrid war" are the means to accomplishing a broader strategy. Briefly enumerated by Edward Lucas of *The Economist* at the ICDS event on 24 November 2014, these goals are as follows: to recreate a Russian empire ("Novorussia" or New Russia), to stop the European Union's ability to control energy pipelines, and finally, to weaken

---

1 Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, 2007, p. 38.

2 Military Balance 2015, International Institute for Strategic Studies.

3 http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html; http://thediplomat.com/2015/02/a-tempest-in-a-teacup-forget-hybrid-warfare/

and divide the West. In modern terms, these goals reflect realist goals of a former, less inter-connected world.

The Western refrain that economic interdependence is a means of preventing conflict is much less of a factor in President Vladimir Putin's rationale than expected. In a February interview with BuzzFeed, President Barack Obama said this about Putin's world view:

> *I think he looks at problems through this Cold War lens, and, as a consequence, I think he's missed some opportunities for Russia to diversify its economy, to strengthen its relationship with its neighbours, to represent something different than the old Soviet-style aggression.*

Russian build-up of nuclear arms is certainly a classic Cold War pursuit of power; however, the build-up of smaller tactical bombs belies a more alarming departure from theory – the collapse of the Mutually Assured Destruction Doctrine (MADD).[4] Western use of the bomb is considered extremely unlikely given the high number of civilian casualties and the resulting humanitarian crisis. Generally, use of this weapon is internationally condemned but Moscow continues its nuclear posturing suggesting a disregard for this "taboo." [5] Russia is employing an old school strategy in a world where the West can no longer definitively claim the moral high ground.

Tactical Convergence: Information Warfare

Information Warfare takes on a different meaning in the Russian Federation. While in the West there is an emphasis on information "operations" as distinct from concrete acts of war, Russian doctrine specifically talks about war. Information war is defined as follows:

> *Confrontation between two or more states in the information space to damage the information systems, processes and resources, which are of critical importance, and other structures, to undermine the political, economic and social system, and effect massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party.* [6]

Interestingly enough, Russian infiltration of Ukrainian social media and networks would, under this definition, constitute information warfare.

---

4 James Conca, "Does Russia Think Their New Nuclear Weapons Could Win a War?" Forbes.com, November 10, 2014.

5 Nina Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use." International Organization (1999), 53, pp. 433-468.

6 Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011), https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

Psychological warfare is named as a key threat against Russian national security and sovereignty. Russia's first Information Security Doctrine document was published in 2000.[7] This paper specifically laid out tasks for improving electronic and intelligence combat abilities to include elements to counter propaganda. In that document, the key method of ensuring information security for the Russian Federation is defined as:

> *Stepping up counterpropaganda activities aimed at preventing the negative consequences of the spread of disinformation about Russian domestic policy*.

Including support of the regime in the core interests of the state ensures that civil society is an integral part of national security operations. Current Russian doctrine, and therefore leadership, operates under the supposition that regime security and national security are one and the same.[8]

Yet information warfare is not limited to psychological operations. At ICDS' event on this topic, Ulrik Franke specifically notes a focus within the doctrine on attacks on Command and Control (C2) systems.[9] In these documents, the first Gulf War is given as an example of effective C2 cyber operations. This tactic was seen in the invasion of Georgia in 2008 in the disabling of governmental, military, and logistical communications systems.

More and more, Russia is being considered one of the greatest powers in terms of offensive cyber capabilities. According to the 2015 "Worldwide Threat Assessment by the US Intelligence Community", the Kremlin is now establishing a Cyber Command similar to the Americans' CYBERCOM – a centre for directing offensive cyber attacks and propaganda operations.[10] This report furthermore, notes the ability of Russian "cyber actors" to infiltrate industrial control centres. Using malware, these actors will be able to affect the systems of critical enemy infrastructures.

Russia's Ukrainian Civil and Military Campaign

In Ukraine, theoretical visions of information warfare have become a reality. In September 2014, according to a report from security firm F-Secure, a Russian cybercrime gang was uncovered distributing targeted malware called BlackEnergy to Ukrainian governmental organizations.[11] Difficulties with

---

7 Information Security Doctrine of the Russian Federation (2000). http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

8 Franke, Ulrik. War by Non-Military means pp. 19-20. http://foi.se/en/Top-menu/Pressroom/News/2015/War-by-Non-Military-means/

9 http://www.icds.ee/events/event/icds-hosts-hybrid-warfare-discussion/

10 http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

11 F-Secure believes this can be attributed back to Russia for the following reasons. BlackEnergy is a piece of malware that has been identified in the Russian cyber underground since 2007. There is also evidence to show that some of the materials used to bait Ukrainian officials were created on a Russian version of Microsoft Office.

attribution aside, it would be convenient for Moscow to maintain deniability because "patriotic hackers" may be acting on their own accord. On the other hand, they could also be state-backed. While actions have consequences, with plausible deniability, the Russians are able to maintain a buffer to prevent any concrete international action against them.

The majority of Russian attacks in cyberspace have been psychological in nature. The attacks are aided by the fact that over the past 15 years, media has become more and more dominated by the state. This level of control domestically, and within loyal Russian communities, has allowed for more psychological tactics such as playing on positive emotions by personifying soldiers and demonizing the West.

According to a NATO StratCom Center of Excellence report, Russia has been using social media as a platform for spreading disinformation and anti-Western sentiment. [12] In fact, Russia has set up "troll farms" to infiltrate news sites and other social media sites to diminish dissenting voices. Information control is vital to the Russian strategy to maintain control of its citizens and prevent any dissent. In November 2014, Russia set up the government-controlled news site, Sputnik News, dubbed by Foreign Policy the "BuzzFeed of propaganda."

Cyberspace actors seem to have a keen awareness of how to manipulate human emotion, which therefore can be used to exploit the biggest weakness in computer systems – the users. Russia has been focusing its efforts on being able to effectively tailor its weapons, surveillance tools, et cetera to cater to the weaknesses of the users. Malware and surveillance techniques emanating from Russia make use of this psychological knowledge specifically in order to gain unauthorized and often high-level access to state and organizational affairs. In this respect, Estonia is held up as an example; it has exhibited strong defence by excelling in trying to increase the capacities of its citizens, but this remains an uphill battle. The sophistication of Russian social engineering[13] makes clear the fact that they believe information will give them the upper hand in future conflicts. It furthermore makes clear the tangible uses of private data in conducting psychological attacks.

Quite clearly, Russia has vast experience in spreading disinformation; but the West's traditional tactics cannot counter it. Current mainstream Western media has recently fallen under fire for inaccuracy and false reporting. However, the ubiquity and accessibility of the internet provides an opportunity. Despite Russian attempts at limiting internet freedom, the Russian people still have the means to examine outside news sources to distinguish fact from fiction. Trust in all media is at an all-time low, leaving the West's role in protecting the world order increasingly ambiguous, but certainly a free and open internet can give citizens the opportunity to dig deeper, beyond the Kremlin's rhetoric.

---

12 NATO StratCom Center of Excellence, Analysis of Russia's Information Campaign Against Ukraine, 2014.

13 Defined by the US-CERT as "an attacker us[ing] human interaction (social skills) to obtain or compromise information about an organization or its computer systems." https://www.us-cert.gov/ncas/tips/ST04-014

Conclusions

1. Espionage and network intrusion has preceded conventional military invasion, providing a warning before the conflict escalates to the use of force. In the cases of the 2008 invasion of Georgia, and in Ukraine, Russian forces spent up to years monitoring governmental networks. Any evidence of Russian intrusion serves as something of a warning shot – a very long one.

2. Coordination among government agencies, non-governmental bodies, and private individuals is key to the execution of hybrid warfare.

Russia executes its control over its territory in a manner that adds to the multifaceted nature of hybrid warfare. Not only does the international community need to deal with the variety of operations occurring inside and outside of cyberspace, it has to examine the relationship of a wide variety of groups and organizations in determining liability.

3. Psychological warfare is a dangerous tool that can indirectly lead to physical harm.

Following the end of the Cold War, information campaigns fell out of popularity in the West. People worldwide have access to so much information; a broadcast like Radio Free Europe would no longer have nearly the same impact. However, Russian attempts to spread disinformation have proved surprisingly effective. Freedom of speech is an important human right, but in some cases, Russian-catered media can serve as a method of indoctrinating susceptible individuals who can then carry out more dangerous plans. The use of psychological means of manipulating large swaths of people should not be taken lightly.

What can be done? Hybrid warfare is the future of warfare. Each state (and ideally the entire international community) must embrace this uncertainty in its policy and doctrine. The current lack of legal and political means for addressing cyber operations leaves the international community vulnerable to these kinds of coordinated attacks. Because there are essentially no precedents with which to address cyber warfare, most states shy away from directly addressing a nation's misbehaviour in cyberspace. If there had been a response to aggressive behaviour within the Ukrainian network sphere, perhaps the West could have had a more expedient and cohesive response to the Russian physical invasion. As it is, there are very few binding legal documents that would serve as guidance when dealing with cyber operations; there is not even any clear legal consensus on whether or not accessing the system of an attacker is permissible.

The kinds of operations that Russia is conducting in Ukraine are not terribly novel, or even that sophisticated; rather, they exploit the fact that any operations in the cyber domain are befuddling to Western nations. The ensuing debates leave them plenty of time and leeway to continue their aggressive behaviour.