

By Prof. Viljar Veebel

Estonian National Defense College

The international community faces serious challenges arising from a new mode of information warfare that Russia has deployed during the Russian-Ukrainian conflict in 2014-2016.
This ongoing "propaganda war" is the most recent and frightening example of information warfare. It reflects the wide array of nonmilitary tools used to exert pressure and influence the behavior of countries. When skillfully combined, disinformation, psychological pressure, and malicious attacks on large-scale information and communication systems can be even more dangerous than traditional weapons systems since they are extremely difficult to discover and combat.

This article examines Russian "propaganda machinery" and discusses Estonia's experience in combating threats from Russian information warfare.

TOOLS OF MANIPULATION

Psychological warfare follows the same logic as traditional warfare. The actions of one party involved in a conflict create the need for actions by the other party to balance the situation. Preventive actions provoke counteractions, and each successive step can be more aggressive than the previous one. This leads to conflict escalation, even as the parties to the

conflict are convinced that they are focused only on self-defense and are acting pre-emptively.

As practiced today, psychological warfare involves certain best practices. Disinformation, media propaganda, threats and psychological techniques are used to deter or to destroy opponents.

Defending against such attacks requires an open and balanced model that is based on facts, reflects reality and is not prejudiced. The best antidote to information warfare is for the public to assess the situation rationally and individually, and to guarantee that communication is not

filtered or manipulated. Facts should take precedence, as should the assessment of alternative viewpoints. Knowledgeable and critical consumers of news do not expect simplified and exaggerated solutions. They expect a thorough analysis of all aspects of a story. But providing this model of careful journalism is resource-intensive.

When starting to lose while using a fact-based and open model in information warfare — as was the case for the Russian government during the Ukrainian conflict — a solution is often found in reconstructing or manipulating images of oneself and the enemy, allowing a government to retake the initiative with fewer resources. As a general rule, replacing an objective image in the media with a distorted or manipulated one is first justified by a practical need to retaliate, to mislead an adversary, or to help mobilize and motivate the "man in the street."

This use of reconstructed information neither requires nor involves in-depth analysis of the facts nor the use of scientific methods, because it would no longer be credible by applying them. Instead, self-legitimizing "expert opinions," presented by confident government officials or so-called opinion leaders, glorified with a fancy title, tend to prevail.

In the process, the essayists of propaganda departments gather wind under their wings, while factual news reporters are forced out of the media, labeled as boring skeptics, defeatists or even influence agents of the opponent. The disbelievers are equated with the enemy ("You're either with us or against us!"), and a difference of opinion in one matter is considered a sign of disloyalty in all other matters. Anyone seeking comparative information from alternative sources will be seen as dangerous and negative. Once experts and academics have been tarred with the label of skeptic or opponent, they can be excluded from further debate.

The main objectives of a reconstructed information campaign are to:

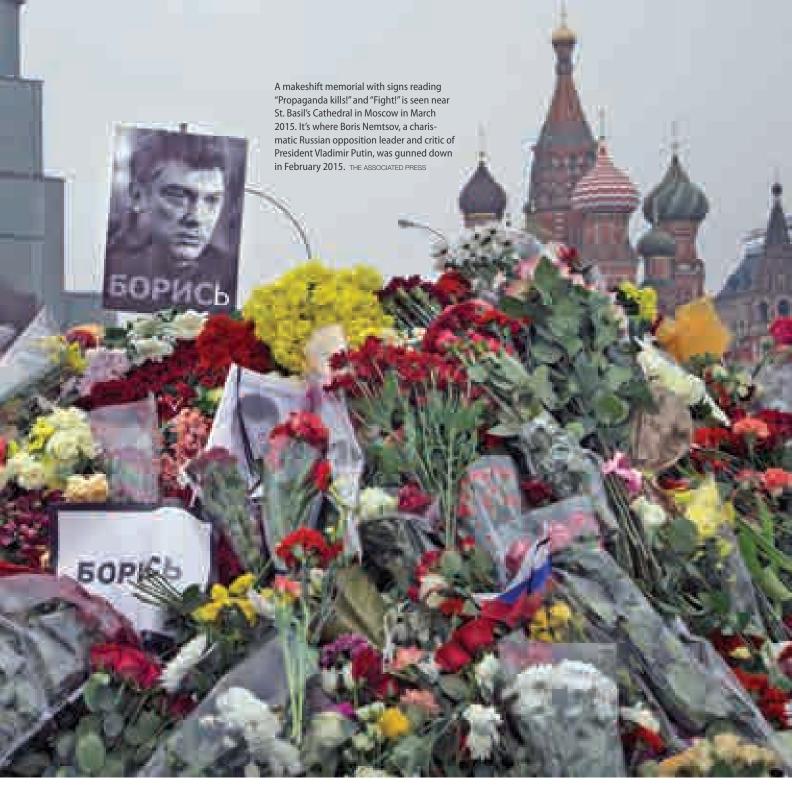
- · demonize the adversary
- · deter and demoralize the adversary
- · legitimize one's own activities to the general public
- · mobilize target populations
- · promote one's own political elites

The methods in this stage include mixing truth with lies so that the news consumer — while recognizing a familiar fact — also trusts the information that has been manipulated. As a general rule, quantitative information is not source-referenced and, in case of conflicting data, a more favorable version is presented. Later on, if a piece of information turns out to have been fabricated, it is suppressed. The main criterion for producing news and press releases is conformity to the correct ideology and terminology. One of the keys to popularity is clear, resolute and increasing confrontation with rival parties.



NEED FOR DEFENSE

Despite the cost, it is important to combat psychological attacks, for two reasons. First, as the scale and significance of information warfare grows in scope, it draws attention away from the objective circumstances of the conflict, including from self-criticism and potential solutions to the conflict. Second, distorted information initially intended to distract opponents takes on a life of its own, believed even by the initial source of the disinformation. Once falsehoods begin to circulate, it is difficult to limit their spread.



A psychological war can be won — regardless of ideology — by using certain best practices, methods and patterns. Showing empathy for the opponent scores no points in this game and has no place in the history books. Interestingly, in the Ukrainian case, in light of public opinion polls on support to their respective governments and opposition to their adversaries, all three parties (Russia, Ukraine and the Western allies) have mostly reached their objectives. But should this standoff be considered evidence of tactical success and a sustainable strategy in the longer run?

RUSSIAN TACTICS

Russia has placed information war tactics at the center of its foreign policy. The Information Security Doctrine of the Russian Federation, published in 2000, describes national interests in the information sphere. The main objectives of the doctrine are as follows: to protect strategically important information, to protect against deleterious foreign information, and to inculcate in the people patriotism and Russian values. Indeed, the declaration refers to the importance of the "spiritual renewal of Russia," "civic responsibility for the destiny of the

country" and "moral values of society and traditions of patriotism."

Furthermore, the doctrine warns that "foreign special services use media operating within the Russian Federation to inflict damage to the nation's security and to spread disinformation." All of these statements reflect Russia's deployment of its domestic media as a propaganda tool. The Kremlin focuses on creating an image of Western countries as "dangerous and aggressive" toward Russia.

Yet Russia's propaganda efforts are also directed abroad. Russia has refused to join Europe's

Convention on Cybercrime, which aims to increase cyber security and counteract cyber threats. The convention was signed in 2001, came into force in 2004, and is active in more than 40 countries. But Russia has declined to sign because it uses such techniques to further its political ambitions.

Recent history has seen several prominent examples of this. In 2007, when Estonia removed a memorial to Soviet soldiers, Russia responded aggressively, deploying a wide array of info war resources to damage its neighbor. Russian politicians arrived in Estonia to "rile things up" while Russian-language



websites offered instructions on how to attack Estonian sites. On top of this, Russia's Federation Council called on its government to cut diplomatic relations with Estonia. The Estonian Embassy in Moscow was blockaded by Russian youth movements, and Russian officials called for boycotts of Estonian goods. Trade on the Russian-Estonian border ground to a halt as truck traffic at the main bridge into Estonia was blocked and the delivery of oil, coal and petroleum products was cut off. Cyber attacks accompanied the psychological onslaught.

The Russian-Ukrainian war has revealed just how damaging this new type of warfare can be. Russia uses a variety of channels to transmit its preferred content.

Recent research by Vladimir Sazonov has described the different channels used in Russian information operations to transmit messages that include misinformation: Russia-controlled TV channels (such as LifeNews, Russia1, Russia24, Channel 1, NTV and REN TV), as well as Ukrainian TV channels (like Inter and Ukraina 24) run by pro-Russia oligarchs or Russian news providers, occupy prominent positions in Ukraine and are key tools.

But the battle is moving to the Internet as well. The resources of the online media (Russian newspapers, but also Ukrainian newspapers like *Komsomolskaya Pravda in Ukraine*, the Ukrainian edition of a Russian-based newspaper), and Web pages (such as LiveJournal and Liveinternet), are instruments of disinformation. Massive Internet trolling on social media, the Russian radio (e.g., Radio Majak), separatists' information channels (such as Novorus.info), and even mobile phone operators (KyivStar and MTS) round out the Russian arsenal. During the Ukrainian-Russian war, Russia's strategy has focused not only on destroying the morale of Ukrainian soldiers, but also attacking their relatives by splitting families along the lines of ethnicity, religion, politics and region.

Russian information channels have relentlessly portrayed the Ukrainian Army as murderers, criminals and Nazi perpetrators, while ignoring the causes of the war or discussion of Russia's involvement. This image has been created methodically using aggressive and emotional rhetoric. Demonstrably false stories of crucified children and raped women were created and replicated to discredit the Ukrainian Army. By bombarding the Ukrainian population with this information — all of it skewed and some of it false — Russia hopes to undermine support for the government in Ukraine.

RESPONDING TO RUSSIA

What should the international community learn from Russia's information warfare techniques in Estonia in 2007 and Ukraine in 2014-2015? There are several key lessons:

• Over the past decade, disinformation has

- been a main tool of Russian propaganda during conflicts. The targets of Russian media are labeled "fascists" or "criminals," which is intended to discredit those countries in the eyes of the West and to convince the Russian people that their government's actions are just. In this light, providing balanced information to Russians is an important policy goal.
- In Estonia, the local public broadcasting opened a new Russian-language television channel called ETV+ in September 2015. The aim of the channel is to keep the Russian-speaking minority in Estonia informed about local and international issues (two one-hour programs per day and regular daily news in Russian) and to provide the audience entertainment (such as shows and films purchased by ETV+, such as the television and Web programs of Deutsche Welle in Russian).
- However, as Estonia's current experiences with integrating its Russian-speaking population into Estonian society have shown, there is a vast gap in the resources allotted. The financial resources directed to the Estonian Russian-language media have not been comparable to the resources with which Russia feeds its propaganda machine. In this regard, co-operation between European Union member states is necessary to optimize resources and share reliable information.

More generally, Europe needs to devote more money to creating balanced sources of information that are based on facts rather than prejudice. The EU's initiative from March and June 2015 to counter Russian media propaganda with "positive messages" serves as a first step. The initiative includes several activities, such as the establishment of the permanent EU communication unit EastStratCom Team, promotion of media freedom in EU Eastern Partnership countries and making communication materials available in Russian. \square

References

- Roth, Mathias. "Bilateral Disputes between EU Member States and Russia,"
 Centre for European Policy Studies Working Document 319 (August 2009). http://
 www.isn.ethz.ch/Digital-Library/Publications/Detail/Plang=en&id=105021
 2. Sazonov, Vladimir, et al. (2016) "Russian Information Warfare against the
 Ukrainian State and Defence Forces: April-December 2014." Riga: NATO
 Strategic Communications Centre of Excellence.
- 3. Smith, David J. "How Russia Harnesses Cyberwarfare," American Foreign Policy Council: Defense Dossier 4 (August 2012): 7-11. http://www.afpc.org/files/august2012.pdf.
- Veebel, Viljar. (2015a) "From Psychological Defence to Propaganda War," Latvian Institute of International Affairs, Riga. http://liia.lv/en/blogs/ from-psychological-defence-to-propaganda-war/
 Veebel, Viljar. (2015b) "Russian Propaganda, Disinformation
- and Estonian Experience," Foreign Policy Research Institute, E-Notes, October 2015. http://www.fpri.org/article/2015/10/russian-propaganda-disinformation-and-estonias-experience/