The international community faces serious challenges arising from a new mode of information warfare, which Russia has deployed during the Russian-Ukrainian conflict in 2014-2015. This ongoing “propaganda war” is the most recent and frightening example of information warfare. It reflects the wide array of non-military tools used to exert pressure and influence the behaviour of countries. When skilfully combined, disinformation, malicious attacks on large-scale information and communication systems, psychological pressure, can be even more dangerous than traditional weapon systems, since they are extremely difficult to discover and combat.

The Logic and Toolbox of Psychological Warfare

Psychological warfare follows the same logic as does “traditional” warfare. The actions of one party to the conflict create a need for the actions from the other party to balance the situation. Preventative actions provoke counteractions, and each successive step can be more aggressive than the previous one. This leads conflicts to escalate, even as the parties to the conflict are convinced that they are focused only on self-defense and acting only 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 the facts, that reflects reality, and that 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.

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 at times becomes believed even by the initial source of the initial disinformation. Once falsehoods begin to circulate, it is difficult to limit their spread.

Russia’s Concept of Information Security in Theory and Practice

Russia has placed information war tactics at the center of its foreign policy. The Information Security Doctrine of the Russian Federation published in 2000 lays down the foundations of Russia’s 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, there have been many references to the
importance of assuring the “spiritual renewal of Russia,” increasing “civic responsibility for the destiny of the country” and reinforcing the “moral values of society and traditions of patriotism” in the declaration. 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.”\(^1\) 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 to prevent cyber threats. The convention was signed in 2001, came into force in 2004, and is currently active in more than 40 countries. But Russia has declined to sign in part 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 in Russia to damage to its neighbour. Russian politicians arrived in Estonia to “rile things up” while Russian-language websites offered instructions on how to attack Estonian sites.\(^2\) On top of this, Russia’s Federation Council called on its government to cut off diplomatic relations with Estonia. The Estonian embassy in Moscow was blockaded by Russian youth movements and Russian officials called for boycotts against Estonian productions. 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 to Estonia was cut off.\(^3\) 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. Russia-controlled TV-channels (such as LifeNews, Россия1, Россия24, Первый канал, НТВ, РЕН ТВ) as well Ukrainian TV-channels (like Inter, Украина 24), which are run by pro-Russia oligarchs or Russian news providers, occupy prominent positions in the Ukrainian TV-channels, are a key tool. 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 v Ukraine, that is the Ukrainian edition of 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 on attacking their relatives and families by splitting families along the lines of ethnic, religious, political and regional identities.

Russian information channels have relentless 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 very aggressive and emotional rhetoric. Demonstrably false stories of crucified children and raped women were created and replicated in order 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’s Propaganda

What should the international community learn from Russia’s information warfare techniques in Estonia in 2007 and Ukraine in 2014-2015?\(^4\) 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 labelled “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 sources to Russians is an important policy goal.

- In Estonia, the local public broadcasting has opened a new, Russian-language TV-channel called ETV+ in September 2015. The aim of the TV-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

---


\(^2\) Ibid.

entertainment (such as shows and films purchased not produced by the ETV+, such as the TV and web programs of Deutsche Welle in Russian).

- However, as Estonia’s current experiences with integrating the local Russian-speaking population into the Estonian society have shown, there is a vast gap in the resources allotted to this end. 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 EU member states is necessary both in terms of optimizing resources and in sharing reliable information.

- More generally, Europe needs to devote more financial resources to create balanced sources of information that are based on facts rather than prejudice. The EU’s recent 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 establishment of the permanent EU communication unit EastStratCom Team, promotion of media freedom in the EU eastern partnership countries, and making communication materials available in Russian language.