Yale FOX INTERNATIONAL FELLOWSHIP

FOG OF INFORMATION WAR: THE PROBLEMS OF THE MILITARIZED INTERNET

Alexander Kulnev

2015 POLICY BRIEF SERIES

Fog of Information War: The Problems of The Militarized Internet

The tremendous speed in which the Internet took over the world surprised national governments. At first, most states decided to leave online communications unattended and unregulated. During this period of 'regulatory vacuum' technology continued to evolve, attracting not only a few tech-savvy professionals but also a global audience of billions.

Governments seeking to control the internet following the «wild west» era, found it difficult, owing to the prevlance a series of decentralized modalities. As a result, some digital platforms became conduits for social and political change . This ability to circumvent authoritarian state control was exhibited clearly in the "Twitter revolution" in Moldova and in the Arab spring. Following this wave, Western media celebrated the Internet as liberation technology, a tool which would allow oppressed people across the world to overthrow their oppressors. Some governments, most notably Russia and China, interpreted these events differently. They saw the Internet as a tool of regime change promoted by the USA, rather than a medium for the bottom-up political organization. According to this perspective, the non-interventionist model needed to be changed with a « militarized approach» to internet use and regulation.

Under the doctrine of militarized internet; a government's digital regulation policies are shaped by concerns about national security and the stability of the political regime, not by notions of freedom of expression. This shift in priorities has dramatic consequences for online discourse, as history clearly shows that the willingness to protect dissident ideas is lowest when the safety of the state is concerned.

Russia is an interesting case in that it rapidly shifted from the laissez-faire approch to the militarized one. It’s not hard to point to events that lead to such change: the Arab Spring, 2011 political protests in Russia, Snowden revelations and the overthrow of government in Ukraine. Over a period of three years (2013-2015) the Russian government implemented the policy of militarized internet on three levels: in rhetoric, in law and in extralegal practices.

Rhetoric

One indicator of support for an increasingly militarized policy towards information technologies is found in the rhetoric of key decision-makers. In Russia, for example, Vladimir Putin in 2010, as Prime-Minister, claimed that the Web mostly consists of pornography, so it should not be a concern of the state. In 2014, however, Putin called the internet "a special CIA Project", implying that it should be treated with suspicion. In the same vein, Igor Sechin, a close associate of President Putin, claimed that high-level Google executives were involved in inciting and organizing popular unrest in Egypt in 2011.

This change in rhetoric coincided quickly into legal and governmental actions.

Legal Reforms

The Militarization of the internet lead to legal restrictions on transferring personal data. In July of 2014, the State Duma passed a law which requires storing all personal data of Russian citizens within the country's borders.

Restrictions on foreign ownership of internet companies can potentially be the next step. The law already does not allow foreigners (companies or invididuals) to hold more than a 20% share of Russian media outlets.

By its nature, the Internet is a global network: online projects often do not have a physical office in their country of operation. Attempts to regulate this aspect of the tech business will do a lot of damage to the industy and to millions of users.

Extralegal practices

Modern states usually have great leeway in using extralegal practices in protecting national security. Therefore, if the internet as a whole is declared a threat to national interests, there are almost no restraints on the state's power to regulate it.

Viewing cyberspace as the battlefield in an "information warfare" challenges the principle of government neutrality and opens the door for manipulations of online discourse. An example of such efforts are the infamous troll brigades, which are reportedly organized with an assent of the Russian government. Groups of trolls leave thousands of comments to promote viewpoints favorable to the government. Their primary goal is to sabotage conversations about important subjects in international politics: the Syrian War, Ukrainian Crisis and others.

Path forward:

While discussing potential proposals for countering the militarization of the internet, it is important to provide important caveats. This doctrine gained ground because powerful political actors in countries like Russia and China believe that the USA has an expansionist foreign policy, ultimately aimed at changing regimes in adversary countries. The logic of the militarized internet is just a deduction of this worldview. This fact limits the scope of potential interventions: changing the minds of very specific leader cannot be a meaningful policy prescription. Governments, however, can take certain steps to ensure that the doctrine of militarized internet does not take root in national legal systems.

1. **Addressing Incentives**

Government investments in projects aimed at "domesticating" key internet services, such as national search engines or social networks, create powerful interest groups.

Potential profiteers are directly incentivized to support and promote the narrative that global infrastructure of the Internet is a threat to national interests.

Laws that prohibit public funding of internet-related projects, would choke off these incentives and eliminate at least one source of fuel for militarization of the internet.

2. Empirical research

There is a lot of work to for academics, media and other thought leaders to determine the actual impact of the interent on the political process. The Tremendous political power of the internet has been hypothesized, but never convincingly proven. On the contrary, several authors contested the narrative of the Western media about the Arab Spring. Evgeny Morozov and Malcolm Gladwell argue that the Web is not an inherently liberating technology, but can actually be detrimental to political mobilization.

If the internet is actually a minor factor for instigating popular unrest, the view that the USA uses it to change regimes becomes undefendable.

3. **Demilitarization of the Internet**

Countries that are committed to free speech, can explicitly prohibit manipulation of online discourse by the government. This principle should cover even the defensive "information warfare." Such laws would reinforce the most basic principle of free speech jurisprudence: that harmful, wrong or dangerous ideas should be defeated in open discussions, rather than banned by decrees of the government.