Determinants of information wars: Russia's information attacks in Georgia and Ukraine

Alla Baranovsky-Dewey

Harvard University

2018

ABSTRACT

What factors determine the timing of countries' information attacks on one another? The security dilemma explains the eventual occurrence of information attacks. Fearful and anxious of watching other countries build up informational resources, countries are driven to build theirs up, as well, setting in motion a set of events that culminates, at some unknown point in time, with a cyber or propaganda attack. The second, crucial, set of factors that better explains the timing of such attacks describes the vulnerability of the target state. A polarized political environment, an open mass media market, a pivotal historic event, and the target state's awareness and preparedness combine together in various ways to determine when an attacking country might decide to attack. I apply this theoretical lens to the cases of Russian informational campaigns in Georgia (2008) and Ukraine (2014). The theory presented here has practical implications for gauging the likelihood of Russia's involvement in Western elections.

INTRODUCTION

In 2016, Russia stunned U.S. analysts and citizens by interfering in the American presidential election. Pursuing the twin goals of promoting the candidacy of Donald Trump, and harming that of Hillary Clinton, it engaged in both cyber attacks and a propaganda campaign. In a 2017 report, the U.S. Intelligence Community stated that the Russian strategy combined "covert intelligence operations -- such as cyber activity -- with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls.""[i]

In a late 2017 blog post, Alex Stamos, the Chief Security Officer at Facebook, finally addressed the issue of Russian interference on his platform. Stamos explained that, although his company had been used to deliver roughly $100,000 worth of Russia-produced political messages to U.S. voters, most of these messages did not "specifically reference the US presidential election, voting or a particular candidate." Instead, these messages referenced sensitive ideological and political issues - matters like gun control,

LGBTQ rights, issues of race and others - instigating conflict along ideological and partisan lines.[ii]

This brief acknowledgement did not reveal that the Russia-originated information campaign did not limit itself to stirring passions online. In fact, the messages also attempted to initiate real life, on-the-ground political events by calling for and organizing protests and rallies and even encouraging state secession.[iii] In turn, Russia, predictably, has claimed that the U.S. is guilty of the same actions. When the country experienced a large-scale wave of political protests, in anticipation of, and then following the 2012 presidential election, Putin pointed the finger at then-Secretary of State Hillary Clinton as the driver behind the unrest in the country.[iv] Russia's Parliament, similarly, has accused the U.S. media of informational campaigns seeking to undermine and discredit the 2016 parliamentary election and the 2018 presidential election.[v]

These cases are examples of sovereign states engaging in propaganda campaigns that are designed specifically to meddle in other countries' domestic political affairs. Although in some cases there might be a direct, observable, benefit to the offending state's actions, in many cases this benefit is unclear or obscured. That is, whereas the payoff from influencing a state's election to ensure that a friendly candidate takes office is clear, it is less clear why a country would expend money and effort to produce political unrest elsewhere (such as by fomenting secessionist sentiment).

Why do countries engage in informational attacks against other countries? One explanation – a modified security dilemma – holds that in an anarchic world, devoid of an external authority, countries are motivated by fear and anxiety that their own information channels might themselves be attacked. This fear drives them to build up their

informational resources. In the realm of information, defensive and offensive resources are frequently the same, so the countries simultaneously build up their defensive and offensive capability. At some critical point, the dangerous spiral results in one country using these resources to attack.

But although this explanation accounts for the fact of an information attack, or its eventual occurrence, it does not explain when, precisely, this dangerous spiral culminates in such an attack. Restated in another way, this question reads, when do countries engage in either propaganda or cyber attacks against one another?

The timing of such attacks is determined by factors inherent in the target state. These are transient or more long-term vulnerabilities that combine in various ways and increase the likelihood that another state might attack. These factors are a polarized political environment, an open mass media market, a pivotal historic moment, and the target state's level of preparedness/awareness of its vulnerability.

In this paper, I examine the final of these factors – the level of awareness and preparedness of the target state. This can determine the likelihood, magnitude, and timing of an informational attack. Two cases examined here demonstrate this well. In 2008, Russia waged an initially aggressive informational campaign in Georgia. But this quickly tapered off when Georgia sought outside assistance with its public relations. By contrast, Russia had a nearly perfect target in Ukraine. This country was not prepared to formulate a coherent informational strategy, and quickly lost the information war with its aggressive neighbor.

LITERATURE REVIEW

The realist framework sees the state as a unitary agent whose core goals are state building and security. Although military security is supremely important within this framework, the meaning of security has expanded with globalization. Thus, security of information networks has assumed a progressively greater importance.

A well-established theory within the Realist framework that could, at least partially, explain informational meddling is the security dilemma. This enduring theory, claim its proponents (see, for instance, Buchanan 2016), offers powerful explanatory power both in situations of rapidly evolving crises, like the US-USSR Cuban missile crisis, and long-term strategic international policy decisions. John Herz, a political scientist, first formulated the idea in his 1951 book *Political Realism and Political Idealism*[vi], and Herbert Butterfield, a historian, outlined a similar causal path in his *History and Human Relations*, although he named the scenario differently.

The sequence of events unfolds in the following order: a state that inevitably and rationally fears for its security begins to acquire resources to guarantee it, such as developing or acquiring weapons, making military alliances etc. As it continues to strengthen itself, this state not only builds up its defensive capabilities, but it also begins to look more threatening to other states. These other states, recognizing their own relative weakness, will invest in their own security resources. As the process develops, it runs the risk of spiraling into an international conflict.

The security dilemma rests on a major assumption that the world order is an anarchic, rather than a hierarchical arrangement. William Golding, a Nobel-prize winning British novelist, allegorically described this arrangement in his 1954 novel *Lord of the Flies.* When a group of previously ordinary, civilized British school boys, accustomed to

living under the external authority of adults, crash on a deserted island in the Pacific Ocean, it does not take them long to devolve into a bloody power struggle, motivated by constant fear of each other and a chimerical monster. In other words, the boys experience a shift from a hierarchical social arrangement, in which their lives are governed by adult authority and school rules, to an anarchic one where no one person or institution prescribes their actions. The outcome is violence and disorder.

An anarchic view of the world dates back to ancient Greek history. Thucydides, commonly considered to be the world's first historian, describes the violent Peloponnesian war, between Athens and Sparta. After executing every adult male on the island of Melos, as a punishment for not joining a military alliance, the Athenians declare, summing up the anarchic view of the world: "the strong do what they can and the weak suffer what they must." In an anarchic world, which lacks a single, central authority that provides arbitration and resolves conflict, life, in the words of the English political theorist Thomas Hobbes is "solitary, poor, nasty, brutish, and short." States sometimes fight for no other reason than their lust for power (Morgenthau 1971; Waltz 1994). In an anarchic world, states do not trust each other and lack the motivation to cooperate (Bull 1994).

Because of this, the security dilemma is a psychological problem. The dangerous spiral of events that eventually leads to conflict is motivated by fear which is commonly unfounded (for instance, the chimerical monster in *Lord of the Flies*). The misunderstanding works in both ways: not only do states exaggerate their own fear of the other states that are increasing their defensive resources, misinterpreting the buildup as offensive and threatening, but they also misperceive how others will interpret their own

strategic resource buildup (Jervis 1994; Booth and Wheeler, 2008). Herbert Butterfield wrote, for instance: "It is the peculiar characteristic if the situation I am describing -- the situation of what I should call the Hobbesian fear -- that you yourself may vividly feel the terrible fear you have of the other party, but you cannot enter into the other man's counter-fear, or even understand why he should be particularly nervous." This is problematic for a political scientist who is grappling with the problem that could be explained by the theory, must also think like an armchair psychologist and attempt to understand and account for emotions like anxiety, worry, fear and nervousness.

More recent work on informational warfare, specifically cyber security, has adapted the security dilemma to explain cyber attacks. Buchanan (2016) argues that the theory explains the fear that states feel when they experience network intrusions and their subsequent actions.[vii] According to his argument, states build up their offensive capability because a lack of borders in cyberspace and the nature of network intrusions mean that they can do so in stealth and well in advance of when they actually decide to intrude. But they also have a constant fear of intrusion, which means that they will proactively try to collect intelligence (sometimes by breaking into the networks of other states) that would indicate the presence or absence of a threat. This, coupled with technological difficulties in assigning blame in cyber threats (Rid and Buchanan 2015), results in the blurring of the line between offensive and defensive actions, and might effect the cybersecurity dilemma.

THEORY

Although the cyber-security dilemma explains the eventual occurrence of some information attacks, it has more limited explanatory power when it comes to their timing

or magnitude. For example, Russia's campaign to influence the U.S. 2016 presidential election, as well as informational campaigns related to some Western European elections, and the referendum on Brexit, were timed strategically to coincide with important events in the history of the nations under attack. If they were the culmination of a pernicious cycle effected by the security dilemma, this was not immediately obvious in the sequence of events.

Thus a complete explanation for information attacks must account for two sets of factors. States perpetrate information attacks against other states when

1. their *information power resources* allow for this. This follows from the logic of the security dilemma. Information power resource endowment is a variable that includes things like the know-how, institutions and organizations to engage with foreign recipients of information. In Russia, for instance, organizations like the Internet Research Agency, Russia Today, and Sputnik relied on decades of experience crafting propaganda under the Soviet state. Information power resource endowment is thus a necessary but not a sufficient condition for a state's engagement in an informational attack.
2. the defensive states exhibit changes or vulnerabilities in their *informational structure.* These vulnerabilities include factors like a polarized political environment (for example, the political environment in the U.S. leading up to the 2016 presidential election), an open mass media environment that frequently gives voice to marginal opinions (relatively free Western mass media markets), the target nation undergoing a pivotal historic event in which an intervention could make a difference (like an election), or the degree of awareness or

preparedness of the target state. These factors can exist independently or in combination, and some might be more prominent than the others. The various ways in which they combine affect the calculated payoff for the attacking state and the resulting timing and intensity of the informational attack. For instance, the U.S. presidential election was a combination of all three factors, but many of the Western European elections, where Russia interfered to a lesser degree weren't.

Unlike the security dilemma alone, this theory does not hold that states will orchestrate informational attacks when they fear other states' buildup of informational resources. Their actions are only partially motivated by fear, anxiety, or moral considerations. They do not wait to strike until their adversary has indicated that they are about to launch a propaganda campaign in their own nation. Instead, they launch informational attacks when their own power resources allow them, and when they find vulnerability in the politics of the defending nation.

GEORGIA AND UKRAINE: VULNERABILITY OF THE TARGET STATE

Vulnerabilities in the target state include a polarized political environment, an open mass media market that gives voice to marginal opinions, the presence of a pivotal historic event in which an intervention can make a difference, and a lack of awareness and preparedness within the target state. These individual factors can be more or less prominent, but combine together to determine the eventual outcome – the timing of the information attack.

In particular, in the past years, Russia has been more likely to orchestrate an informational attack, or dedicate more resources to one, when it has perceived the target state to be either unaware or unprepared for the attack. In cases where the target state has

demonstrated a robust informational defensive strategy, or was able to quickly demonstrate the ability to notice and reverse offensive actions, Russia's calculus of its involvement changed and has sometimes resulted in abandoning the course of an informational attack. The cases of Georgia and Ukraine illustrate this well.

Russia engaged in informational warfare against both countries in the recent years. In both cases, Moscow was confronted with separatist sentiment in the two former Soviet republics. In both cases, the Kremlin engaged in a concerted propaganda effort against the two nations that meant to promote its own narrative and subsume theirs.

In 2008, the regions of Abkhazia and South Ossetia that had, in the 1990s, declared independence from Georgia began to experience more and more tensions and belligerent incidents. The government of Georgia started to indicate that the presence of Russian "peacekeepers" there was more and more unbearable. In early August of 2018, the two sides, probably beginning with Georgia, engaged in a series of military provocations.[viii] The actual military campaign was brief – 5 days – but the informational aspect of the military encounter was substantial and deserves analysis.

The most proximate cause of the Ukraine crisis might be found in the November 2013 decision by Victor Yanukovich, then President of Ukraine, to renege on a trade deal with the European Union in favor of another one with Russia. Public protests followed the announcement - first with hundreds of people, then thousands, then hundreds of thousands. A forceful, deadly response from the Ukrainian police brought more protesters out into the streets, and by January the situation turned into a full-blown crisis.[ix]

In February of 2014, following more deadly confrontation between the protesters and the authorities, Yanukovich is deposed and flees, while Russia puts troops on high

alert. On March 1st, armed men, identified by Ukraine as the Russian military, seize key points of the Crimean Peninsula as the predominantly Russophone region begins the process of secession from Ukraine. Amid broad international condemnation and accusations of illegal and aggressive actions, undaunted by the threat of sanctions, Russia absorbs Crimea.

By early April, pro-Russian protesters occupy several key cities in Eastern Ukraine. Donestk and Luhansk become the hottest points of separatism. As clashes between rebels and Ukrainian government forces continue, a civilian passenger airliner with 298 international citizens on board is shot down killing all passengers and crew. The two sides vigorously accuse each other of the act of aggression.

These two cases are an appropriate choice for this analysis, because they conform to a well-accepted method of case selection - Mill's Method of Comparison. When two cases are similar in all aspects but one, that one aspect is likely to be causal of the different outcomes. Ukraine and Russia are both former Soviet Republics. They are similarly important to Russia in geopolitical terms. Both have had a back-and-forth relationship between loyalty to Russia and interest in integration with the West. Both have had internal tensions where regions heavy in Russian speakers were interested in breaking away and joining Russia. Both have had Russian support for this.

Russia's initial informational offensive in Georgia in 2008 was both proactive and aggressive. Several weeks before the military operations of the five day August war, Russian hackers subjected the unprepared nation's Internet infrastructure to D.D.O.S. attacks, while simultaneously taking down the website of then Georgian President, Mikheil Saakashvili. Several other state computers were hacked too, the Ministry of

Foreign Affairs and the Ministry of Defense among them.[x] As if in anticipation of hostilities to come, Moscow sent journalists into the region – by some accounts, as many as 48[xi] – to ensure that its version of events to come will be thoroughly covered.

Orchestrating a cyber attack requires specific informational resources - trained hackers and advanced networks, among others. Georgia's Internet was partly supplied by Russia, and partly by Turkey. Its Internet infrastructure was dwarfed by the considerably more vast Russian information power resources. Possessing these resources enabled the Kremlin to begin the information war.

The resource differential also meant that at least in the beginning, Russia was on the offensive, and Georgia – playing defense. This reactive policy was not always wise. For instance, one measure that the Georgian government resorted to in an attempt to limit the damage of the aggressive Russian information campaign, was censoring Russian media sources and the Russian Internet.[xii] This gave Moscow more reason to accuse Georgia of not being an "open" and "democratic" society it had purported to be. As a Ministry of International Affairs representative said at the time,

> "The informational blockade of the Russian media in Georgia represents a crude violation of international standards of press freedom that guarantee the obligation of the government to provide citizens the right to freely access information, and the ability of the press to disseminate such information. […] Such policy of the Georgian authorities has nothing in common with democracy."[xiii]

But although Georgia lacked the technical capability to respond in kind, the country quickly mobilized their PR resources. In other words, the target state of the information attack in this case was prepared to respond. And it responded as actively as it could.

The Georgian government quickly sought professional public relations help. Some accounts related that it approached foreign firms for help in crafting an image.[xiv] It rapidly increased the number of its political blogs – in some cases transforming existing websites into blog format, and in others – crafting new content. Its strategy changed from defensive to offensive. The new informational campaign featured carefully chosen language that characterized Russia as the aggressor. It compared the invasion on the ground with the military occupation of Prague in 1968. It issued claims of genocide.

This heavy barrage of allegations against Russia raised the cost of involvement for the Kremlin and caused it to reduce the intensity of informational war dramatically. The conclusion of the international community, as well as many Russian observers, was that Georgia won the information war. As Russian dissident poet Lev Rubinstein poignantly noted when comparing Soviet propaganda with the informational tactics of the Kremlin in August 2008,

> "A [Soviet] common man, even one without access to information, firmly knew: the case is directly opposite that which has been painted for him by the newspaper or the television. But if the Soviet magician worked with a screen, using all sorts of smoke to obscure the mysteries of his profession, those of today saw the lady in the golden dress in half right in front of the respectable citizenry, without any mysterious smiles, without the pink smoke, without a turban and other abracadabras."[xv]

What Rubinstein is saying in his colorful way is that Russian propaganda in the early stage of the war was intense and crude. The international community, represented by the Western press, covered Georgia sympathetically. This indicates that Georgia eventually managed to advance its narrative of events.

On the other hand, Ukraine, which, in the words of Peter Pomerantsev, lacks "an international voice or image", was a far better target for a sophisticated and sustained

information attack when Russia annexed Crimea. Russia's informational strategy was more advanced, constantly evolving and adapting to new challenges.

Although the information campaign was aimed at the international community as much as at the domestic audiences, the Kremlin began their work at home. Systematically, it eliminated or reorganized the remaining independent press outlets, one by one. RIA Novosti, Dozhd, Ekho Moskvy, and Lenta.ru were all experienced Kremlin-directed "restructuring" that installed Putin-friendly professionals in place of liberal-minded ones.[xvi]

A strongly promoted narrative featured in this information war was characterizing any pro-Ukranian forces as "fascist."[xvii] As this Kremlin story goes, far-right groups high-jacked the protests and has been busy harassing the country's Jewish and Russian populations. Although these claims were repeatedly debunked[xviii], the mere fact of their existence and persistence in the public narrative is indicative of the success of the Russian strategy. As scholars and practitioners of political campaigns are well aware, a small amount of untruthful information is exceptionally difficult to counteract, even with copious amounts of factual data.

These kinds of claims illustrate the distinction between misinformation and disinformation. The former is quite easy to spot. Misinformation is outright lies. When Russia claimed thousands of Georgia-inflicted casualties in the August 2008 war, it was engaging in misinformation. Disinformation, however, takes half-truths and spins them further, retaining just a small portion of the original fact. This remaining kernel of truth is what makes disinformation so difficult to reject outright. In the Ukraine informational

campaign, Russia's sophisticated disinformation techniques were a vast improvement on the crude misinformation campaign it had orchestrated in Georgia only a few years prior.

Kremlin-promoted narratives about Ukraine did not stop at the fascism accusation. Indeed, the full set of untruths is impressively rich. The Russian media proactively accused the West and Ukraine of waging an information war against Russia.[xix] The Kremlin claimed that it had no intention of using military force in Crimea.[xx] Deriding Western journalists, Putin asserted that Russian soldiers were really Ukrainians who purchased their Russian military uniforms: "Why don't you have a look at the post-Soviet states […] There are many uniforms there that are similar. You can go to a store and buy any kind of uniform."[xxi]

In addition to propagating a rich and expanding array of untruths, the Russian propaganda machine used considerably more ways to reach their targets, like blogs and social media. It had multiple target audiences - Ukrainian separatist fighters, Russian domestic population, and the international community. By comparison with the Georgian case, its reach in Ukraine, a state that was not prepared to put up a fight, was vast, and the effects considerably more dramatic.

PRACTICAL IMPLICATIONS

In the years leading up to the 2016 U.S. presidential election, the Russian government, relying on decades of Soviet experience with propaganda, created outfits like the Internet Research Agency that were tasked with conducting a disinformation campaign and sowing "political discord" in the U.S. The Kremlin is doing this again. In June of 2018, Russia founded a new media outlet in the United States, called USA

Really. The newest outlet, much like its predecessors, reports on divisive political issues like press freedom, death penalty, race, LGBTQ+ rights and others.

These actions are indicative of growth in the information resource endowment. They may indicate that another spiral of the security dilemma is underway. The theory presented here indicates that this buildup of resources will culminate in an information campaign that happens when a set of vulnerabilities in the target state, the U.S. aligns. The U.S. will once again be undergoing a pivotal historic event – midterm elections in the age of Trump, its society is divided along partisan lines, its media market is open enough to allow the Russian narrative to enter. The only factor that is different this time is that the U.S. intelligence community is aware of the Russian threat. This will make a difference in the intensity and the timing of the eventual information attack.

[i] Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution, Office of the Director of National Intelligence, 6 January 2017. Found at https://www.dni.gov/files/documents/ICA_2017_01.pdf Last accessed 18 September, 2018.

[ii] Stamos, Alex, "An Update on Information Operations on Facebook," *Facebook Newsroom*, 6 September, 2017. Found at https://newsroom.fb.com/news/2017/09/information-operations-update/. Last accessed 17 March, 2018.

[iii] Graham, David "Why Would Russia Try to Foment Protests in the U.S.? *The Atlantic*, 12 September, 2017. Found at https://www.theatlantic.com/politics/archive/2017/09/russian-facebook-events/539565/. Last accessed 17 March, 2018.

[iv] Herszehnhorn, David and Barry, Ellen, "Putin Contends Clinton Incited Unrest Over Vote," *The New York Times*, 8 December, 2011. Found at http://www.nytimes.com/2011/12/09/world/europe/putin-accuses-clinton-of-instigating-russian-protests.html?mcubz=0. Last accessed 17 March, 2018.

[v] Ayres, Sabra, "Russia's Answer to Charges of Meddling in U.S. Elections: You're Messing with Ours, Too," *LA Times*, 23 June, 2017. Found at http://www.latimes.com/world/europe/la-fg-russia-us-meddling-20170623-story.html. Last accessed 17 March, 2018.
[vi] Herz, John, *Political Realism and Political Idealism*, Chicago: University of Chicago Press, 1951.
[vii] Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford: Oxford University Press, 2016.
[viii] "Independent International Fact-Finding Mission on the Conflict in Georgia," Council of the European Union publication, September 2009. Found at https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf
[ix] "Ukraine unrest: Protesters storm regional offices." *BBC News.* 24 January, 2014. Found at http://www.bbc.com/news/world-europe-25876807.

[x] John Markoff, "Georgia Takes a Beating in the Cyber War With Russia," The New York Times, 11 August 2008.
[xi] Starr 2009, p. 186.
[xii] Starr, Frederick S., The Guns of August 2008: Russia's War in Georgia, Armonk, NY: Routledge, 2009, p. 186.

[xiii] Here, and throughout, author's translation. "Naseleniie Gruzii Izolirovano ot Pravdivoi Informatsii – MID Rossii [The Population of Georgia Has Been Isolated From Truthful Information – MIA of Russia]", *RIA Novosti*, 03 September, 2009. Found at https://ria.ru/osetia_news/20080903/150923328.html
[xiv] Starr 2009, p. 191.
[xv] https://graniru.org/Society/Media/m.141302.html
[xvi] https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media
[xvii] https://ria.ru/world/20141203/1036335888.html
[xviii] https://www.nybooks.com/daily/2014/03/07/crimea-putin-vs-reality/?insrc=wbll
[xix] https://www.pravda.ru/politics/parties/other/13-08-2014/1221213-infowars-0/
[xx] https://www.mk.ru/politics/article/2014/03/04/993621-presskonferentsiya-putina-po-ukraine-myi-ne-sobiraemsya-voevat.html
[xxi] https://lithub.com/russia-is-winning-the-information-war/