Bot of course Russia Matters!
Russia and Online Politics

Joshua A. Tucker,
Professor of Politics and
Affiliated Professor of Russian and Slavic Studies
Affiliated Professor of Data Science
Director, Jordan Center for the Advanced Study of Russia
Co-Director, NYU Social Media and Political Participation (SMaPP) lab
New York University

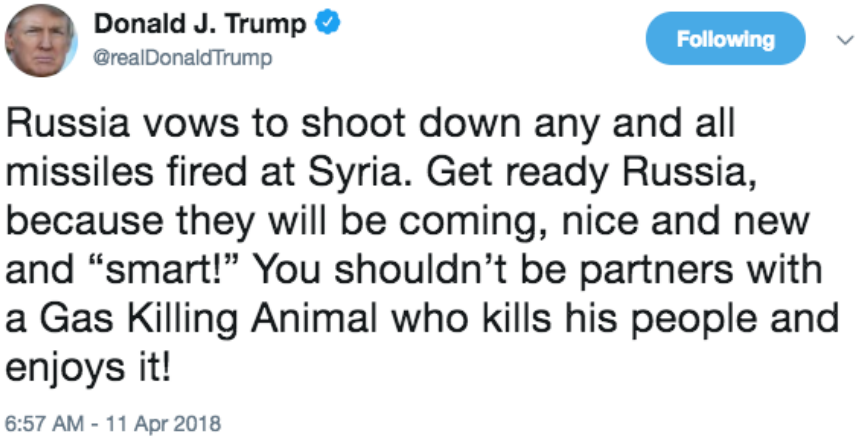
ROUGH DRAFT IN PROGRESS

Paper prepared for presentation for conference on *Regime Evolution, Institutional Change, and Social Transformation in Russia: Lessons for Political Science* at Yale University, April 27-28, 2018. Please do not quote directly from this paper without author's permission, as most of Section III of this paper is reproduced from Sanovich et al. 2018. This paper also draws heavily on Tucker et al. 2017, and is intended mainly to function as a brief synopsis of arguments advanced in those two articles – with on additional section/topic included as well – but applied to the theme of this conference.

Abstract: One of the most pressing questions facing comparative politics today concerns the interaction between social media, democratic activists in authoritarian countries, and illiberal activists in democratic countries. Needless to say, the study of Russia will play a paramount role in all of these endeavors. In Tucker et al. (2017), we argue that two basic factors – the ability of social media to give voice to those excluded from mainstream media and yet simultaneously function as a form of censorship that can be exploited by both state and non-state actors – can explain both of these phenomena. In Sanovich et al. (2018), we lay out a basic framework for classifying the ways in which authoritarian regimes can respond to online opposition and provide a case study of Russia's evolving internet policy. In this paper, I synthesize arguments from these prior works to argue that Russia is actually at the center of important new theoretical component of what is now mainstream political science. Research on Russia can play a role not only in advancing these debates, but also in developing new methodological tools for the field as whole to answer a range of questions that are increasingly demanding attention but with which the field is only beginning to grapple.

1. Introduction

For this conference, we were asked to wrestle with the question of what Russia has to offer the study of political science, and what the study of political science has to offer for our understanding of Russia. I would like to make the argument here that far from having to reach to find ways in which what is happening in Russia can be connected to larger trends in political science, Russia is actual central to some of the most important new developments in the field. More specifically, the field as a whole needs to wrestle with questions regarding the ways in which the digitization of information is transforming the ways both citizens and elites interact with the political world, the way citizens and elites interact with one another, as well as the way in which elites interact with each other. To wit:



In the remainder of this brief paper, I will do the following to advance this argument. First, in Section 2 I will briefly summarize a general framework for thinking about the relationship between social media, pro-democracy movements in authoritarian regimes, and anti-democratic movements in democratic regimes that we laid out in Tucker et al. (2017). Although

Russia's footprints can be found in all aspects of this schema, I will use Section 3 to expand upon a part of the framework – the manner in which authoritarian regimes respond to online opposition – where Russia has been extremely influential in organizing both theory and empirical evidence; this section will be reproducing material just published in Sanovich et al. (2018). In Section 4, I will then address just a few of the many, many questions raised for political science by Russia's purported attempt to weaponize information in Ukraine,[1] the 2016 United State presidential election,[2] and other European elections.[3] The net result should be a clear picture of how Russia is not only instrumental for helping us to study some of the most pressing new questions in political science, it may actually be defining what some of those questions are.

2. Social Media and Democracy: From Liberation to Turmoil

One vexing question facing the field of comparative political science today is how social media could have gone from being "Liberation Technology" (Diamond 2010) to "Can Democracy Survive the Internet?" (Persily 2017). In other words, how did social media go from forming a backbone of the Arab Spring – and the 2011 Russian Duma Elections (Enikolopov, Makarin, and Petrova 2017) – to threatening the quality of democratic elections in one of the world's oldest democracies in 2016?[4]

In a recently published article in *The Journal of Democracy* (Tucker et al. 2017), we advanced a parsimonious explanation that I will briefly summarize here. The reason I do so is

[1] http://cepa.org/index/?id=6060d322713797e84f598ea25c812cab.
[2] https://www.theguardian.com/us-news/2018/feb/16/robert-mueller-russians-charged-election.
[2] https://www.theguardian.com/us-news/2018/feb/16/robert-mueller-russians-charged-election.
[3] https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/?utm_term=.007899ecea7e.
[4] This is section draws heavily from Tucker et al (2017), although does not reuse text verbatim from that article.

two-fold within the context of this conference. First, it is a good example of how a new, general argument about the relationship between online information and politics can give us insight into Russian political developments. But at the same time, it is also an illustration of a case where Russian political developments have played a crucially important role in theory development.

At the heart of our argument lies two simply assumptions. First, we assume that social media gives voice to those who are excluded from access to mainstream media. This voice can, in turn, be used for a wide variety of political purposes, but most importantly it can be used to overcome barriers to collective organization. Our second assumption, however, is despite the fact that social media democratizes access to information, it is also a tool that can be used for censorship.

How do these two assumptions answer the question of how we get from liberation technology to can democracy survive the Internet? Consider first the situation in authoritarian, or competitive authoritarian, regimes like Russia. Who is excluded from access to mainstream media? This may include many other anti-regime but also anti-democratic forces, but it will almost certainly include pro-democratic forces. Thus if a tool emerges that will help those excluded from access to mainstream media in authoritarian states, one set of actors likely to benefit will be pro-democratic forces. Thus we get "liberation technology", with, if one is convinced by the arguments presented in Enikolopov, Makarin, and Petrova (2017), Facebook helping to fuel the 2011 anti-fraud protests in Russia following the 2011 Russian Duma elections.

Of course such developments do not happen in a vacuum. And while there might be reason to think autocrats surrounded by people dependent on staying in the autocrat's good graces might be hesitant to raise the specter of new threats to the regime, eventually we are going

to expect to see autocratic regimes respond to these emerging threats (Morozov 2012). In the following section, I will lay out in more detail a theoretical framework for conceptualizing the response options that regimes face for dealing with online opposition as well as a brief summary of how Russia has utilized these different options as the internet has evolved, but suffice it to say that Russia was instrumental in pioneering methods by which regimes were able to respond to online oppositions, including by using the internet as a tool of censorship.

Before turning to that discussion, I want to just address how this simple framework gets us to "can democracy survive the internet?" as well by 2016. Turning again to the concept of who is excluded from access to mainstream media, in democracies we can also think of multiple actors who might benefit from a tool that gives voice to those not generally afforded to mainstream media. On the one hand, if we want to think of "corporatized media" as excluding more progressive voices, we can point to movements such as Occupy Wall Street or Black Lives Matter as benefiting from the affordances of social media. At the same time, it is clear (at least until very recently) that main stream media in democracies also has tended to for the most part exclude voices that were especially noxious to the very tenants of liberal democracy. Thus the same exact technology that helps pro-democracy advocates organize in authoritarian systems can help anti-democratic forces organize in democracies. Moreover, as we have begun to learn, sometimes these forces don't even have to be present in the country in question, or, at the very least, they can be aided by forces outside the country. This aid can come in traditional forms, such as financial support,[5] but also in the form of support online through the use of new tools to amplify messages, a topic to which I turn in the following section.

[5] http://www.bbc.com/news/world-europe-39478066.

3. Responding to Online Opposition: Theory and Empirical Evidence From Russia[6]

In Sanovich et al (2018), we introduce a tripartite system for classifying government responses to online opposition. We begin with *offline responses*, which primarily refer to changing a country's legal Internet regulations, but also includes attempts to change the ownership structure of online media and intimidate particular users. The second category encompasses various ways to technically *restrict access* to online content, from firewalls to Distributed Denial of Service (DDoS) attacks to sophisticated online censorship systems. The final category also involves online activity, but instead of focusing on restricting access to content, this tactic involves creating content to *engage* with users online.

3.1. Offline Responses

The first set of options at any government's disposal is based on digital age implications of traditional governing advantages: nodality ("network centrality"), organizational capacity, legal authority to enforce the law, a monopoly on the legitimate use of violence, the right to regulate human activity, and the ability to expend large financial resources through taxation.[7] The actions facilitated by these advantages could have a huge impact online, but take place offline; thus end-users either observe the consequences online after-the-fact or encounter these actions in person, but offline. The latter case includes legal prosecution and violence, but can also include actions such as having commenting functionality turned off by their favorite news websites after readers' comments become legally designated as media content.

[6] This section is almost entirely composed of text from Sanovich et al. 2018, a recently published article in *Comparative Politics* co-authored with Sergey Sanovich and Denis Stukal. Anyone wishing to quote text from this section should therefore quote directly from Sanovich et al. 2018, and not from this paper.

[7] See a detailed discussion in Robert Ackland, *Web Social Science: Concepts, Data and Tools for Social Scientists in the Digital Age* (SAGE Publications, 2013).

Another option is to require popular bloggers to register with the government, making each individual blogger responsible for her own content, on a par with actual commercial media outlets, as it has recently been done in Russia.[8] Additionally, governments can attempt to change the landscape of digital media markets and alter the choice of online platforms available to users. Relying on their authority to regulate commerce, autocrats around the world designate certain companies and industries, including telecommunications, as "strategic", upon which they start to enforce various restrictions, such as banning foreign ownership and/or investments, appointing state representatives to the board, etc. For example, in late 2013, the publicly-owned – but heretofore relatively independent editorially (especially, in its popular social media operations) – major Russian news agency *RIA Novosti* was stripped of its leadership, restructured, renamed, and put under the leadership of a fervent regime supporter.[9] Then, in order to ensure the complete control, it was included in the list of "strategic enterprises" in early 2014, along with the second largest Russian news agency, *ITAR-TASS*.[10]

If control over digital media is challenging or costly to legislate or order, especially in the case of private companies, then governments can use other means, in particular purchasing power and extra-legal pressure, to assume control over important Internet platforms. The so-called "Russian Google", Yandex, sold a "golden share" to state-owned *Sberbank* in 2009, allegedly after negotiations with Dmitry Medvedev and multiple proposals to designate companies such as Yandex as "strategic", which would have forced them to re-register in

[8] Neil Macfarquhar, "Russia Quietly Tightens Reins on Web With 'Bloggers Law,'" *New York Times*, May 6, 2014, available at http://www.nytimes.com/2014/05/07/world/europe/ russia-quietly-tightens-reins-on-web-with-bloggers-law.html. See also Appendix B.3.

[9] Sergej Sumlenny, "Bad News: What Does the Closure of RIA Novosti Mean for Media in Russia?," *Calvert Journal*, December 12, 2013, available at http://calvertjournal.com/comment/show/1837/ RIA-novosti-putin-russian-media-kiselyov.

[10] Gabrielle Tetrault-Farber, "RIA Novosti Begins Cutting 1/3 of Staff," *Moscow Times*, March 12, 2014, available at http://www.themoscowtimes.com/news/article/ria-novosti-begins-cutting-13-of-staff/495980.html.

Russia[11] and severely diminish their appeal to international capital markets.[12] A similar attempt was made in the case of VKontakte, known as the "Russian Facebook", which resulted in the hostile takeover of the company by business groups loyal to the Russian government[13] and founder and former owner and CEO Pavel Durov fleeing the country with many members of his team.[14]

3.2 Online Responses: Restrictions

The rapid growth in Internet penetration rates and the emergence of the Internet as a principal source of information for increasing numbers of people creates challenges even for autocrats who are able to successfully employ offline tools of control. To begin with, information can be produced and distributed by foreign citizens and entities that are out of reach of the autocrat's security apparatus. Second, some local activists and/or journalists can use their digital proficiency to distribute information anonymously and therefore avoid offline prosecution. Moreover, autocrats may simply prefer putting flows of information under their control rather than going after its producers. If, for example, an autocrat wants to avoid taking responsibility for the government's actions, a DDoS attack on a popular oppositional blog can be blamed on

[11] Yandex is incorporated in the Netherlands as Yandex N.V. – a fact that in 2014 was publicly condemned by Vladimir Putin at his meeting with the All-Russia People's Front. See Christopher Brennan, "Putin Says CIA Created the Internet, Cites Foreign Influence at Yandex," *Moscow Times*, April 24, 2014, available at http://www.themoscowtimes.com/news/article/ putin-says-cia-created-the-internet-cites-foreign-influence-at-yandex/498903.html.

[12] Nikolay Grishin, "Yandexed Everything," *Kommersant – Trade Secret*, March 12, 2012, available at http://www.kommersant.ru/doc/2065978.

[13] Nickolay Kononov, "The Kremlin's Social Media Takeover," *New York Times*, March 10, 2014, available at http://www.nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html; Joshua Yaffa, "Is Pavel Durov, Russia's Zuckerberg, a Kremlin Target?," *Bloomberg Businessweek*, August 1, 2013, available at http://www.businessweek.com/articles/2013-08-01/is-pavel-durov-russias-zuckerberg-a-kremlin-target.

[14] Ingrid Lunden, "Durov, Out for Good from VK.com, Plans a Mobile Social Network Outside Russia," *Techcrunch*, April 22, 2014, available at http://techcrunch.com/2014/04/22/durov-out-for-good-from-vk-com-plans-a-mobile-social-network-outside-russia/.

"unidentified" hackers, while most types of offline response require at least some involvement of the state apparatus.

Of course, there option also to completely monopolize the telecommunication infrastructure inside the country and cut any connections with international networks. North Korea did just that: it maintains *Kwangmyong*, a national intranet, and a national mobile phone service *Koryolink*, both of which can be controlled and monitored. Communications with the outside world through both channels are prohibited (except for the ruling elite and foreign tourists). However, such a system imposes a heavy toll on the national economy.

A step removed from this extreme approach – albeit still with non-trivial costs – is the highly sophisticated Chinese "Great Firewall", probably the best example of blocking sensitive information without fatally hurting either government communications or commercial activity.[15] This form of targeted Internet-censorship is well documented by King, Pan, and Roberts, who describe the immense Chinese system of monitoring and censoring of user-generated content across the country's dispersed social media platform and estimate that around 13% of all social media posts get censored.[16]

Two primary technological options for regimes are filtering/blocking of particular websites or segments of the web and DDoS attacks. The former has the advantage of being permanent and customizable. China, for example, blocks only certain platforms and content (by keywords), while North Korea famously maintains its local web segment in complete isolation from the outside web. Both policies, though, share a common disadvantage of this approach: high

[15] *The Economist*, "The Art of Concealment," April 4, 2013, available at http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated.
[16] King, Pan, and Roberts.

transparency for local users and susceptibility to documentation by outsiders (including other governments, human rights organizations, etc.).[17]

DDoS attacks, on the other hand, are usually hardly traceable, relatively cheap, can be deployed during particularly sensitive political events such as elections or protests and can be more easily outsourced to loyal but independent groups, such as the Syrian Electronic Army.[18] On the other hand, their ability to break up online communications is limited in time and web space, i.e., a small set of websites at best. Moreover, the most popular platforms, such as Google and Twitter, are highly protected from DDoS attacks.

3.3 Online Responses: Engagement

Establishing a government presence on the web and using it to promote its agenda constitutes the third and final option at a government's disposal. This type of government response actually takes place online and users encounter it in the course of their online activity. Mainly, it includes the government creating content, either through automated processes or real human effort.[19] The most obvious and increasingly popular tool employed to alter political conversations on social media is using either "bots" (i.e. computer programs) or "trolls" (i.e. real

[17] Morozov.
[18] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," *Information Warfare Monitor*, May 30, 2011, available at http://www.infowar-monitor.net/2011/05/7349/.
[19] However, hacking and publishing bloggers' personal communications (such as emails, instant messages, etc.) could allow the government to expose and implicate the opposition and shape the conversation that way. A typical example of the latter is the case of Russian blogger and hacker known online as *Torquemada Hell*, a Russian-speaking person allegedly living in Germany. In 2010-11, he successfully hacked the email accounts of multiple Russian opposition politicians and released potentially damning information to the public. See Alexey Sidorenko, "Russia: Analysis of Hacker Attacks on Bloggers," *Global Voices*, June 20, 2010, available at http://globalvoicesonline.org/2010/06/20/russia-analysis-of-hacker-attacks-on-bloggers/.

people) to advocate pro-government positions, turn conversation meaningless or prohibitively divisive, or distract users from sensitive political issues altogether.[20]

Bots can perform two key functions: cluttering conversations with "digital dust", which could be pro-government, anti-opposition, or simply aimed at "flooding the zone" with distracting information in order to detract attention from opposition voices[21]; or altering search results, Internet rankings, top lists, and other automated tools for sorting, sharing, discovering, and consuming online content. As such, bots could be used to support real people. For instance, a ranking of the most popular Russian blog posts maintained by Yandex was closed in 2009, inundated by bots promoting mostly pro-government posts.[22]

The possible functions of humans acting on the government side are much more diverse. It is useful, therefore, to provide a basic classification of *pro-government content producers*. This classification does not look into users' honesty, consciousness, or beliefs. Instead, it is based on formal or informal ties with the government (or the lack of thereof).

To begin with, the government could hire students or other low-paid workers to submit rather simple messages, which would nevertheless pass the human intelligence tests integrated in many modern social media platforms. One particular example of this type of bloggers are the so-called Chinese 50-centers.[23] Russian pro-government youth movements, such as *Nashi* and *Young Guard of United Russia* were sometimes accused of running a similar network of 11-

[20] See as well Tucker et al (2018).
[21] Roberts.
[22] Alexey Sidorenko, "Russia: Major Search Engine Closes Its Blog Rating," *Global Voices*, November 6, 2009, available at http://globalvoicesonline.org/2009/11/06/russia-major-search-engine-closes-its-blog-rating/. The more pressing concern for Yandex, though, was government outrage in the cases when, instead, anti-government posts got traction in the ratings, see Alexandra Odynova, "Yandex to Close List That Annoyed State," *Moscow Times*, November 6, 2009, available at http://www.themoscowtimes.com/news/article/yandex-to-close-list-that-annoyed-state/388969.html.
[23] Sarah Cook, "China's Growing Army of Paid Internet Commentators," *Freedom At Issue Blog*, October 11, 2011, available at http://www.freedomhouse.org/blog/china%E2%80%99s-growing-army-paid-internet-commentators.

rublers.[24] Leaks released by the Russian arm of Anonymous in 2012 indicated that *Nashi* paid hundreds of thousands of dollars in fees for comments, statuses, Facebook likes, YouTube dislikes, etc.[25]

Cheap bloggers paid per comment are not the only group of friendly users that could be put on the government payroll. Bribing prominent and trusted bloggers, celebrities, or journalists – although potentially much more expensive – could turn out to be a better investment in terms of persuading the public. The same leaks noted previously revealed that along with paying small fees to thousands of low-skilled bloggers, *Nashi* also put aside tens of thousands of dollars to be paid to a small group of popular and, heretofore considered, independent bloggers for highly sophisticated positive publicity for the Russian leadership.[26]

The next group consists of government supporters whose social media activity is not paid *per se*, but is facilitated through participation in various political projects or actual employment by the government. These sets of bloggers range from members of various youth political movements to the MPs from the ruling (or affiliated) parties to relatively prominent politicians (ministers, party leaders) who are encouraged to take on the challenge of representing the government's point of view in an often-hostile social media environment.

Finally, the government could also try to mobilize genuine supporters with no formal or informal ties to the government or ruling party. If famous people volunteer to support the government agenda, it could help the autocrat both directly and indirectly through endowing the

---

[24] Anton Nossik, "11 Rubles and 80 Kopecks per Comment," *Echo of Moscow*, September 10, 2013, available at http://www.echo.msk.ru/blog/nossik/1154616-echo/.

[25] Miriam Elder, "Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers," *The Guardian*, February 7, 2012, available at http://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers; Miriam Elder, "Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Group," *The Guardian*, February 7, 2012, available at http://www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi.

[26] Miriam Elder, "Emails Give Insight into Kremlin Youth Group's Priorities, Means and Concerns," *The Guardian*, February 7, 2012, available at http://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities.

ideas already promoted by the armies of bots and paid bloggers with the weight of fame, reputation and personal independence.

3.4. Russian government online: a constantly evolving strategy

The reason why I have taken the time here to dive into this theoretical framework in the context of how Russia matters for political science is precisely because Russia has played a crucial role in many of the developments the gave rise to our conceptualization of this framework. Also in the spirit of this conference, we can demonstrate the value of the framework by showing how it sheds light on the online policies of the Russian government over the past two decades.

Russian government activities online first gained serious international attention when they were redirected towards aiding the Russian offensive in Ukraine in the wake of the 2014 Euromaidan Revolution. The resourcefulness and inventiveness of these actions as well as their reach were all the more surprising for Western observers and policy makers since until then Russian authorities were not considered to be particularly artful in their digital operations, even for domestic purposes.

However, a closer examination of the evolution of Russia's Internet policy reveals that perhaps such surprise was unwarranted. Vladimir Putin is famously old-fashioned when it comes to digital tools: he rarely uses a computer and has never had any personal online presence. However, policy-wise he showed both interest in new technologies and awareness of potential government strategies regarding them. Even before he became acting President, in late 1999, he convened the leaders of the nascent Russian IT industry and online media and made a clear commitment to protect their freedom and avoid Chinese-style filtering. While it is unclear

whether he was concerned with the Russian image abroad or had other intensions, his choice was very politically expedient.

At only 2% Internet penetration in 2002 (and 16% at the end of Putin's second term in 2008), online media were a medium for personal communication more than of mass persuasion and as such were hardly an asset of any political significance. Following an old Soviet tradition, Putin avoided direct interference with personal communication channels.[27] This resulted in the emergence of a thriving and competitive Internet industry, whose leading companies – Yandex and VKontakte – won the competition for local users over Google and Facebook, respectively, and did it without the aid of any protectionist measures, a rare achievement for any country. Years ahead of most Western countries, Russian online news media that had been created from scratch overtook the websites of traditional media in popularity and began doing their own original reporting (instead of relying on existing offline news agencies and outlets). Meanwhile, the Russian public created a vibrant blogosphere that was large enough to completely overtake the major blog platform of the time, LiveJournal, which was eventually purchased by a Russian company.

As Internet penetration continued to rise steadily in the late 2000s and most traditional media became completely sanitized of any alternative opinion, online news media, most of which were rather critical of the regime, became increasingly influential. However, the government first saw this as an opportunity rather than a threat. To a large extent, this attitude was the result of a change in the government.[28] In 2008, freshly installed into the Kremlin, Dmitry Medvedev and his team were looking for ways to build their own support base.

[27] However, again in line with the Soviet blueprint, an elaborate system of digital surveillance called SORM was established. See Ivan Zasursky, *Media and Power in Post-Soviet Russia* (New York: M.E. Sharpe, 2004), 181–183.
[28] That it became one of Medvedev's government's defining policies suggests how limited was the change overall (see on limits of Medvedev's modernization Jonson and White 2012).

Medvedev published his modernization manifesto "Go Russia" in the online-only liberal newspaper *Gazeta.ru*. Medvedev and his team made a serious attempt to engage Russian online public in a genuine discussion of the country's future. Both he and his aids created digital presences on multiple platforms, which earned Medvedev the nickname "Blogger-in-Chief". Most crucially, they sought, received, and responded to critical feedback from the audience, a practice unheard of for years in the traditional media, but necessary to get any attention in the vibrant Russian blogosphere at the time. Pro-government youth movements were mobilized to spread Medvedev's message to every corner of the Russian segment of the Internet. While their activities were not without controversy (more due to corruption and incompetence than ideological zeal[29]), even they had to engage in genuine discussion with bloggers critical of the government, thus facilitating public debate on important issues. While the government did occasionally use DDoS attacks, particularly in relation to the 2008 Russo-Georgian war, the Russian Internet remained remarkably free (in a growing contrast with the traditional media) and the government activities there were primarily targeted to mobilize genuine support based on the compelling message and (limited) interaction with the public.

This engagement came to the abrupt end in the wake of the 2011 – 2012 Russian popular protests, which coincided with Putin's return to the Kremlin.[30] Given the role of media, and social media in particular, in coordinating and sustaining the largest and the longest wave of protests in Russia in two decades, it was also impossible for Putin to go back to the "disengagement strategy" he used during his first two terms in office.

[29] Miriam Elder, "Emails Give Insight into Kremlin Youth Group's Priorities, Means and Concerns".

[30] According to most observers, protest, triggered by the alleged major irregularities in vote count during Duma elections, did not just coincide with Putin's return to Kremlin, but were largely caused by the perceived undemocratic nature of the deal between Putin and Medvedev, which was announced just a few weeks before elections at the ruling party convention, and was kept secret until the last minute even from the convention delegates. See Richard Sakwa, *Putin Redux: Power and Contradiction in Contemporary Russia* (London: Routledge, 2014), 111–134.

Instead, Putin began to actively employ both offline means of controlling media production and online means of controlling access to it. The first included pressuring media moguls into either replacing the editorial stuff of online media they owned (*Lenta.ru*, *Gazeta.ru,* and *RBK* are the most prominent among dozens of examples) or into selling them to more loyal owners (Russian Forbes and *VKontakte*).[31] The government also adopted laws making online media liable for the content of comments posted by their readers, thus requiring these websites either to actively police user-generated content, or shut commenting tools down altogether. In addition, various laws were adopted to prosecute individual bloggers for alleged extremism and other content deemed inappropriate.[32] Since 2012, these laws have been applied in an increasingly wide-ranging manner, punishing with large fines and real prison terms not only the original authors of messages, but also those who reposted them.[33] Finally, many prominent bloggers and online media journalists have faced threats and (at times life-threatening) assaults, which are rarely if ever investigated.

Online tools of controlling access to content include the creation of the Russian Internet Blacklist, maintained by the dedicated government agency, *Roskomnadzor*. Blacklisting initially required a court order, but later was also allowed on a simple request from the Office of the Prosecutor General. While theoretically it is supposed to be easy to exit the blacklist (after removing the content deemed unlawful), after several prominent opposition news websites and opposition leader's blogs were blocked in March 2014, in the midst of the Russian-Ukrainian conflict, they were not informed what content they would have to remove to exit the Blacklist.[34]

---

[31] Lunden.
[32] Human Rights Watch. *Online and On All Fronts. Russia's Assault on Freedom of Expression* (July 18, 2017), available at https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression.
[33] Ibid.
[34] *Human Rights Watch*, "Russia: Halt Orders to Block Online Media," March 23, 2014, available at https://www.hrw.org/news/2014/03/23/russia-halt-orders-block-online-media.

Instead, the government refused to respond to their requests even after they sued for an answer, and they remain blacklisted to this day, thus illustrating the ways in which formal rules and informal power relations are applied in tandem.[35]

Still, neither offline nor online tools allowed the government to shut down hostile activity online completely. While a long period of unrestricted development of domestic alternatives diminished the market share of Facebook and Google in Russia (which makes the government's job easier, as local platforms are easier to coerce into compliance), Facebook and Google are still used by millions of Russians on a daily basis. And when VKontakte, immediately after getting a request, removed the event page of pro-opposition rally, Facebook (after some uncertain moves) refused to comply.[36] Journalists fired by the pressured owners could move abroad and set up a news media there (as *Meduza.io* did).

Therefore, the space for the engagement strategy remains, but instead of playing the leading role, the government is using it to support offline and online restrictions. Rather than trying to engage in a dialog or persuade, the government simply attempts to hammer down the official message, artificially increase the indicators of its take-up (propelling politicians into lists of top bloggers and their messages into lists of top posts), while simultaneously cluttering communication channels used by the opposition. This created a huge demand for various troll and bot factories, which produce pro-government content in volumes, caring about the quantity much more than quality and persuasion capacity. This content requires a new set of tools to study it properly, which we have been working on developing as well (Stukal et al. 2017; 2018).

---

[35] "Grani.ru v. Office of Prosecutor General," *Global Freedom of Expression, Columbia University*, September 2, 2014, available at https://globalfreedomofexpression.columbia.edu/cases/grani-ru-vs-office-of-prosecutor-general/. Alexey Navalny was able to successfully set up a free-standing blog that is not blocked, but he had to regain the audience he lost on LiveJournal before being able to expand it.

[36] Sergei Guriev, "Facebook Faces Down Putin," *Project Syndicate*, January 9, 2015, available at http://www.project-syndicate.org/commentary/facebook-versus-putin-by-sergei-guriev-2015-01.

4. Unanswered questions raised by recent Russian online activity

While there are of course still many questions to be answered regarding the use of bots and trolls in the context of Russian domestic politics, where Russia has really caught the world's attention in the past 18 months has been in using these tools to interfere in the politics of other countries. We are just beginning to see the first papers appear that attempt to systematically analyze this behavior using social media data by relying on the list of Russian Troll accounts released by Twitter as part of a US Congressional Investigation (Badawy et al., 2018; Steward et al., 2018; Zannettou et al., 2018, LLewellyn et al 2018). Reviewing the now rapidly expanding literature on the general question of Russian propaganda efforts in recent Western elections, including especially the 2016 US election, is far beyond the scope of this current short paper, but interested readers are invited to see Tucker et al. (2018) and Marwick and Lewis (2017) for reviews.

Instead, in the spirit of this conference, what I would like to do instead in this section is highlight five questions that Russian attempts to interfere in Western elections raises for the field of political science:

(1) *Can we actually identify foreign interference when it occurs?* As I mentioned previously, the first four papers we've encountered that systematically attempt to analyze the behavior of Russian trolls are all based on a list of accounts provided to the US Congress (and therefore entered into the public record) by Twitter. But we do not know how Twitter came up with this list. Other scholars have investigated trolling behavior in Russia (Ananyev and Sobolev 2017) and China (King et al. 2017) using leaked data. But can we develop methods that will allow us to identify foreign intervention in online news, communication, and social media that do not rely on these kind of idiosyncratic events to deliver data? Even if we can use machine learning to identify bots (Stukal et al. 2017) and classify their political orientation (Stukal et al. 2018), will we be able to conclusively identify these bots as *foreign* absent these kind of leaks or platform-provided information?

(2) *What is the micro-level impact of being exposed to foreign propaganda*? Do individuals actually change opinions or behavior on the basis of being exposed to

foreign propaganda? If so, at what levels? Is one tweet of one *RT* news story enough to convince a disgruntled Bernie supporter to not turn out in an election? Seems doubtful. How about 100? Or how about changing one's vote?

(3) *What is the macro-level impact of foreign electoral interference*? Even if countries are attempting to interfere in the election processes of other states using online propaganda and disinformation, can this actually change outcomes? If so, what would be the mechanism? Increasing or decreasing turnout among particular groups? Changing people's political preferences? Undermining general faith in the democratic process?

(4) *What are the implications of interstate relations for the types of electoral interference we've witnessed recently*? While a little out of my normal theoretical bandwith given that this is essentially an international relations question, I find myself wondering a lot these days whether Russian attempts to interfere in Western elections is a sign of strength – as it is often cast in media reports – or a sign of weakness? How are states in the future likely to respond to these types of propaganda efforts? Will they be treated as attacks on a sovereign state, warranting an actual military response? A cyber response? Counter-propaganda?

(5) *Finally, is any of this really new*? Both the United States[37] and Russia[38] have a long history of meddling in other countries' elections. So is what has been happening in the last 24 months really all that new? If so, what is it about this kind of (potentially) micro-targeted online activity that makes it systematically different from previous attempts by major powers to influence elections in other countries? And are there lessons we can learn from history here?

All these questions strike me as quite important, but they also represent big picture questions for the field of political science that have been raised by recent Russian political behavior.

5. Concluding Thoughts

The purpose of this essay has been to argue that not only is Russia still relevant for the study of political science, in many important new fields of study Russia is actually driving the conversation, both in terms of empirical analysis and theoretical development. The areas I have

[37] https://www.washingtonpost.com/news/monkey-cage/wp/2016/12/23/the-cia-says-russia-hacked-the-u-s-election-here-are-6-things-to-learn-from-cold-war-attempts-to-change-regimes/
[38] https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/

focused on here are in regard to what could loosely be called "digital politics", or the intersection of social media and politics. Within this general field, Russia has provided both a great deal of motivation for theory building as well as increasing evidence for theory testing. I have specifically provided three examples, which I will very briefly recap.

First, we have tried to develop a general theoretical framework for thinking about the relationship between social media and democracy (Tucker et al. 2017). A crucial component of that framework is that pro-democracy activists in authoritarian and competitive authoritarian regimes can use social media to advance their cause, but that regimes are likely to try to respond to these activities by harnessing various tools of censorship. Russia played an important role in our understanding of both of these processes.

Secondly, Russia was crucial to our attempt to develop a taxonomy of the different options available to regimes in how to choose to respond to online opposition, including offline responses, online attempts to restrict access to content, and online attempts to engage with content and shape the tenor of the discussion. Again, Russia was crucial to developing the entire theoretical perspective, and, as I demonstrated at the end of the section, the framework gives us an important lens through which to view Russian political developments.

Finally, the topic of Russian interference in US (and other) elections in the digital realm has rapidly become its own separate area of study, both in academia and beyond. Here one might be tempted to call this tautological – of course Russia matters when trying to study Russian behavior – but there is a growing consensus that Russian behavior in 2016 is simply a harbinger for a much larger class of political activities that are likely to become increasingly prevalent in the coming years: the deliberate promulgation of disinformation, the injection of hyper-partisan content into civic discourse, the use fake news, images, and even videos, etc. In the future, this is

likely to be the realm of domestic and foreign actors around the world (and indeed to some extent already is). In this realm, Russia is not likely to be a potential peripheral actor in terms of our political analyses of global political phenomena, but rather a very central one.

Works Cited Using International Citations:

Ananyev, Maxim, and Anton Sobolev. (2017). "Fantastic Beasts and Whether They Matter: Do Internet 'Trolls' Influence Political Conversations in Russia?". Paper presented at Midwest Political Science Association Annual Meeting, April 6–9, 2017. Chicago, IL.

Diamond, Larry. "Liberation Technology," *Journal of Democracy* 21 (July 2010): 69–83.

Enikolopov, Ruben and Makarin, Alexey and Petrova, Maria, Social Media and Protest Participation: Evidence from Russia (April 7, 2017). Available at SSRN: https://ssrn.com/abstract=2696236 or http://dx.doi.org/10.2139/ssrn.2696236

King, Gary, Pan, Jennifer, and Roberts, Margaret E. 2017. How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, *111*(3), pp.484-501.

Marwick, Alice, and Rebecca Lewis. (2017)."Media Manipulation and Disinformation Online." *Data & Society Research Institute*.

Morozov, Evgeny. 2012. *The Net Delusion.* New York: Public Affairs.

Persily, Nathan. 2017. Can democracy survive the Internet?. *Journal of democracy*, *28*(2): .63-76.

Sanovich, Sergey, Denis Stukal, and Joshua A. Tucker. 2018. "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia." *Comparative Politics* . 50(3): 435-54.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. 2017. "Detecting Bots on Russian Political Twitter". 5(4): 310-324.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. 2018. "For Whom the Bot Tolls". *Manuscript in progress*.

Tucker, Joshua A., Yannis Theocharis, Margaret Roberts, and Pablo Barberá. 2017. "From Liberation to Turmoil: Social Media and Democracy", *The Journal of Democracy*. 28(4): 46-59.

Tucker, Joshua A. and Guess, Andrew and Barbera, Pablo and Vaccari, Cristian and Siegel, Alexandra and Sanovich, Sergey and Stukal, Denis and Nyhan, Brendan. 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature". Available at SSRN: https://ssrn.com/abstract=3144139