

Georgetown Journal

of International Affairs

FALL 2017, VOLUME XVIII, NUMBER III

International Engagement on Cyber VII

Georgetown Journal

of International Affairs

FALL 2017, VOLUME XVIII, NUMBER III

CYBER STAFF

Tom Hoeffcker *Graduate Editor-in-Chief*
Harrison Goohs *Undergraduate Editor-in-Chief*
Laura Pedersen *Undergraduate Editor-in-Chief*
Mara Goldman *Managing Editor*
Benjamin Brazzel *Managing Editor*

Forum

Section Editor Daniel Wassim
Editorial Assistants April Artrip
Kevin Doyle
Colin Maloney

Business & Economics

Section Editor Olivia Rockwell
Editorial Assistants Kate Hyun
Hannah Nelson
Meghna Sinha

Country in Focus

Section Editor Marie Terrier
Editorial Assistants Summer Lyle-Holmes
Shane Dante Quinn

Dialogues

Section Editor Samantha Wolk
Editorial Assistant Sophia Mauro

Global Governance

Section Editors Sam Gerstle
Joey Stabile
Editorial Assistant Marco Garcia

Law & Ethics

Section Editor Josh Chang
Editorial Assistants Meghan Bodette
Maria Victoria Galarraga
Emma Rhodes

Military Matters

Section Editor Michael White
Editorial Assistant Gary Xie

Safety & Security

Section Editor Beatriz Bechelli
Editorial Assistants Asma Venus Ebadi
Anthony Palacio
Macon Sheppard

Science & Technology

Editorial Assistants Marie-Claire Hazburn
Varun Kota
Mahesh Kumar

Copy Editors

Dineo Brinson
Gustav Honl-Stuenkel

DESIGN

Lille Brown

DEVELOPMENT

Kathleen Guan *Director of Development*
Field Daniel *Associate*
Graham Willard *Director of Communications*
Taylor Fitzgerald *Director of External Operations*
Emily Portuguese *Director of Marketing*
Bessie Zavidow *Director of Finance*
Esther Kim *Director of Finance*
Angela Qi *Director of Internal Operations*
Minas Rasoulis *Director of Sales*
Siddarth Singh *Director of Strategy*
Bella Lu *Social Media Chair*

ONLINE

Mana Mostatabi *Executive Editor*
Peter Metzger *Undergraduate Managing Editor*
Jung Min Yeo *Director of Strategy*
Isabella Lu *Social Media Manager*

SFS DEAN'S OFFICE ADVISOR

Jennifer Long
Irfan Nooruddin (Chair)
Anthony Arend
Joel Hellman

PAST ADVISORY BOARD

Marc Busch
Susan F. Martin
Matthew Carnes
Kathleen McNamara
James Millward
Raj Desai
Daniel H. Nexon
Mark Giordano
Christine Kim
Joanna Lewis
Steven Radelet
Katherine Marshall
Elizabeth Stanley
Catherine Lotrionte

Post-Truth Soft Power

Changing Facets of Propaganda, *Kompromat*, and Democracy

Paweł Surowiec

During the July 2017 G-20 diplomatic summit in Hamburg, one of the discussion points between Donald Trump and Vladimir Putin was Russian *intervention* in the 2016 US presidential election, elevating the issue to multilateral diplomatic setting.¹ This article discusses statecraft behind this type of intervention. In particular, it discusses the advancement of Russian propaganda in cyberspace. The central argument of this discursive article is built on the discussion of unique features in Russia's statecraft, namely, the hybridization of "hard" and "soft" power. Further, this article discusses how *kompromat* (a portmanteau signifying "compromising materials"), a feature of Russia's political culture, underlies its approach to exercising soft power in cyberspace, and drives the advancement of Russia's propaganda in cyberspace to further the Kremlin's diplomatic ends.

In the recent years, Russian soft power has been thought of as lacking coherence, while its statecraft enjoys a multilayered architecture. On a surface level, Russia presents itself as magnanimous and pragmatic leader, using its media mouthpieces of RT (formerly Russia Today) and Sputnik, and promoting Russian culture globally through

the agencies Russkiy Mir and Rossotrudnichestvo. More recently, however, global audiences have been learning more about the dark side of Russian influence in international politics: Russia's aiding the proliferation of "fake news," cyberattacks, and *kompromat*.² This article will illustrate how Russia uses these digitalized means of attraction and coercion to create destabilizing effects. It will argue that countering these cyberattacks and *kompromat*-inspired campaigns is complex and requires several types of policy initiatives and responses.

Hybridizing Soft Power

Russia might be perceived as a wonderful state if imagined through the prism of its cultural legacies: it has a rich and diverse fine arts heritage, the Bolshoi Ballet, and an incredible film industry, capable of capturing the imagination of international audiences with films such as *Leviathan* (2015)—all three are truly exciting sources of soft power, which Western liberals usually warm up to. The contemporary Russian soft power draws from the full potential of what it can offer the world: in autocratic Russia, Putin's media is packaged for global audiences in a liberal "sugarcoating of a sweet and sour flavor" through a mimetic mix of strategies, including RT's international broadcasting. Russia has given the West a taste of attraction and coercion as its soft power assets. With government spending on communicative resources of soft power exceeding spending on social policies combating unemployment, Putin's Russia aims to reestablish its global influence and, on the way, reinvent strategies for doing so.³

"Soft power" refers to the means of influence by "non-material capabilities such

Dr. Paweł Surowiec is the senior lecturer of the Faculty of Media and Communication at Bournemouth University. His specializes in the relationships among media, global governance, and public opinion.

Putin's Russia aims to reestablish its global influence and, on the way, reinvents strategies for doing so.

as reputation, culture, and value appeal that can aid attainment of a state's objectives."⁴ Digital media technologies offer new means to pursue these ends as states strive to adopt innovative strategies in the ongoing race for influence.⁵ Given that the future of diplomacy is inextricably linked to digital media technologies,⁶ one of the consequences of this process is the hybridization of soft power statecraft. Hybridization is hardly new in diplomacy: after all, Western public diplomats who are typical front-liners in exercising soft power on behalf of their governments had to adapt to changing media landscapes. Private-sector consultants facilitated the emergence of new trends in statecraft by hybridizing, for example, public diplomacy and nation branding and by advancing the process of corporatization of soft power.⁷

In the case of contemporary Russia, hybridization of soft power is unique because it is made out of a blend of political culture features, such as *kompromat*, and propagandistic strategies that are tailored to specific media landscapes. While the pioneer of the concept, Joseph Nye, argues that propaganda is not the way to advance influence in international relations, communicative resources are integral to soft power.⁸ Russia is one of the players adapting its communicative capabilities to match its ambitions and treating contemporary international relations as a playground for state-facilitated or state-sponsored articulations of soft power strategic narratives in cyberspace. The uniqueness of Russia's approach to soft power is consistent with Putin's views on making foreign policy "through information and other means of influence," further

recognizing that "these methods are often used to encourage and provoke extremism, separatism, nationalism, manipulation of public sentiment, and outright interference in the internal affairs of sovereign states."⁹

The uniqueness of Russia's approach to soft power is consistent with Putin's views on making foreign policy "through information and other means of influence."

Perhaps not coincidentally, there is no adequate translation of the term "soft power" into the Russian language. The phrase "мягкая сила" translates *ad litteram* as "soft force" and arguably captures what Russia aims for in international politics: a hybrid of "forceful persuasions," articulated less to be "liked" by the West and more so to be seen as an "equal" player. Russia's approach to diplomacy and statecraft favors security over democracy, uses soft power capabilities instrumentally by adopting destabilizing strategies and tactics, and often deploys them to cover up its information warfare in cyberspace. Russia is turning into a "spoiler power,"¹⁰ pushing the boundaries of the application of digital media technology in statecraft and advancing digital espionage. While the revelations about Russian intervention into the 2016 US election are still open to scrutiny, this event, combined with Donald Trump's foreign policies, carries beneficial propaganda value for Russia: it undermines liberal democracy and reveals weaknesses of the United States as a global power.

Perhaps not coincidentally, there is no adequate translation of the term "soft power" into the Russian language.

Digitizing Propaganda and Soft Power

I belong to the transitional generation of Europeans who, during the final stages of the Cold War, were exposed to the Soviet-styled propaganda in our everyday lives. As a citizen, I witnessed systemic changes in Central and Eastern Europe, including shifts in the ways in which the Soviet Union interacted with citizens of the “bloc” and the way the influence of its communication, arts, cultures, and political ideas faded after 1989. I then went on to study propaganda in Britain, and after a while I realized that my experience gave me an advantage in terms of detecting iterations of propagandistic practices and different propaganda styles, including those exercised across national boundaries. In the past year or so, I have been strangely alerted to the news media reports about the growing amount of Russia’s “soft power-styled” activities in Europe. More recently, the revelations about Russia’s interference in the 2016 American presidential election felt like a flashback to my youth. I immediately recognized the use of *kompromat* as the cultural underpinning of this complex foreign policy issue. The scope and style of Russia’s soft power is becoming increasingly problematic for democratic governance in liberal parts of the world. As a professional, I found it fascinating. As a European, I was deeply worried.

In its soft power, Russia has been increasing its digital media technology capabilities, and its statecraft has been responding fast to changes in global media landscapes. According to Alexander Yakovenko, Russia’s ambassador to the United Kingdom, his state has joined the club of “Twiplomacy of great powers” relatively recently, but in terms of adoption of its capabilities and levels of public engagement, Russia matches activities of the US and Israel. The Russian Foreign Ministry came up with

its own term—“innovative diplomacy”—which it interprets as a “tool of Russian foreign policy to exert influence on public opinion through the use of ICT.” Putin himself urged Russian diplomats to use digital media technologies across multiple platforms, including in social media, to explain Russia’s foreign policies.¹¹

The speed with which Russian soft power statecraft adapted to an increasingly dynamic and flux global media landscape is impressive. For example, investing in communicative resources such as the “Kremlin School of Bloggers,” expanding the social media capabilities of RT, growing networks aiding cyberspace campaigning, advancing IT expertise, and shifting cyberspace strategies toward attacks and espionage¹²—all are powerful indicators that Russia is a highly capable actor. Correspondingly, there is a growing amount of foreign media coverage, policy reports, and scholarship (e.g., *Reframing Russia for Global Media Sphere* at the University of Manchester) revealing the inner workings of Russian soft power in cyberspace. For example, in an article titled “Russia Is Attacking Western Democracies,” Gerodimos and his colleagues collated some evidence of media stories on Russian cyberattacks and strategic interventions in domestic politics.¹³ Among the listed target locations of Russia’s cyberattacks are Germany, France, the Czech Republic, the United Kingdom, Finland, Greece, Poland, Estonia, Ukraine, Georgia, Moldova, Hungary, Austria, Montenegro, Bulgaria, and, finally, the United States. The intervention in election campaigns has been reported in Germany, France, Bulgaria, and the United States and often has the intention to aid certain political parties, often seen as fringe movements. According to the European Council on Foreign Relations, these parties tend to adopt pro-Russian foreign policy stances.¹⁴ Among examples of political party

vehicles for such policies is *Alternative für Deutschland* in Germany. While Russia and the targeted group of European parties enjoy different depths of relationships, their campaigning tends to have polarizing effects on politics in Europe.

It is worth noting that innovations in media technologies led to the redefinition of the way we think about soft power statecraft: for example, in the 1990s, the “CNN effect” underpinned the theory and practice of public diplomacy. Nowadays, digital diplomacy is being recognized as a semiautonomous practice, but as a field of inquiry, it has some way to maturity.¹⁵ The proliferation of digital media technologies has created new, often pathological, opportunities for advancing influence in international politics. The widespread usage of blogs, bots, and trolling mixed with “fake news” underpins a propagandistic offensive that has used digital media to position Russia as a threat to Western liberal governance.¹⁶ In its soft power, Russia uses digital media to project its stance on socioeconomic development, culture, and military operations. Given the skillful hybridization of foreign policy statements with digital activities in cyberspace, Russia’s soft power carries an assertive strategic narrative visible, for example, in Ukraine where a “pro-Russian, anti-Western” narrative competes with a “pro-Western, anti-Russian” narrative projected from Kiev.

Risks for Liberal Democracy: *Kompromat*-Inspired Propaganda

It took post-Cold War Russia a while to centralize its soft power capabilities, but by 2014, as noted in a Chatham House report, “Russian information campaigns displayed close coordination of messaging as well as an impressive range of alternative outlets to address all sectors of the target audience.”¹⁷

RT, Sputnik, Russia Direct, and others each tailored their level of argument. In the light of the cyberattacks on the White House, the Clinton-DNC attack, and the WikiLeaks release of 20,000 emails before the Democratic National Committee, the cyberhacking group APT28 was believed to act on behalf of Russian state principals.¹⁸ These activities show how, on the one hand, Russia centralizes its soft power on the level of governance and how, on the other hand, it decentralizes its tactical propaganda operations. Consequently, the intervention of Russia, or any other actor, into domestic politics should be analyzed as digital espionage instead of digital diplomacy.

These kinds of cyberattacks find roots, I argue, in Cold War-style espionage and political blackmail. What makes the key difference between traditional espionage and digital espionage is *kompromat*, which, thanks to the recent dossier on Donald Trump, has gained widespread media attention. This peculiarity of Russian political culture illustrates the strong public dimension of digital espionage that is absent from traditional espionage. *Kompromat* is a flexible and powerful concept. It enables denial (rarely apologia) of any wrongdoing when uncovered. Additionally, it often reveals falsehoods and lies about political or business opponents along with truthful negative information, blending accuracies and misinformation, thus allowing it to damage its targets in a highly sophisticated manner. With the hacking of the Democratic National Committee, the undercurrents of *kompromat* were also explicit in the 2016 US election campaign.¹⁹ Furthermore, President Trump’s tendency to promote theories that are not supported by evidence might explain why *kompromat*-inspired propaganda resonates well among his supporters. It is clear that *kompromat* has entered the news media cycles of liberal democracies,

but what is not clear is how these countries will respond to it.

Furthermore, President Trump's tendency to promote theories that are not supported by evidence might explain why *kompromat*-inspired propaganda resonates well among his supporters.

How Should Liberal Democracies Respond?

A starting point for the development of responses to the wave of *kompromat*-inspired propaganda is policymakers' and citizens' awareness of Russian political culture and the effects digital media technology might have on soft power. In cultural terms, Russia displays clear-cut attitudes on foreign policy toward the West, highly polarized domestic politics, and instrumentalization of the value of public opinion in governance—all of which enable *kompromat* to function with ease. In this cultural milieu, Russian media autocracy oftentimes resorts to communicative practices rooted in the Soviet past. Because the Russian state plays a powerful role in citizens' lives, there is a tendency among its citizens to take government's communication practices for granted or oppose it all together. This aspect of Russian political culture translates to strategic communication for soft power: in responding to Russia's *kompromat*-inspired propaganda, the United States and other actors need to develop strategies for enhancing *credibility* instead of engaging in hybridized propaganda wars.

The Russian cyberattacks in the United States and in Europe bring us to the issue of the role of technology in responding to particular negative effects of digitalized propaganda. A report by Chatham House states, "Misconceptions about the nature of Russian information campaigns, and how

best to counter them, remain widespread—in particular, the notion that successful counter-measures consist in rebutting obvious disinformation wherever possible."²⁰ This approach is problematic for at least two reasons: organizational and efficacy issues. There is a risk that countering *kompromat*-inspired propaganda head on will lead to the proliferation of the very information one is trying to counter in cyberspace. Because reports about Russia's involvement in destabilizing cyberspace emerged among multiple states and locations, challenging these actions require cyber diplomacy—that is "the use of diplomatic tools, and the diplomatic mindset—to resolve issues arising in cyberspace."²¹ The first lesson in responding to Russia's propaganda campaigns is the internationalization of this issue by, for example, the formation of a diplomatic coalition to counteract Russia's actions.

Unfortunately, while some governments have already introduced institutional measures to unravel the dynamics of Russian disinformation campaigns, they still seem to operate in silos. For example, in early 2017 the Czech governments set up the Centre Against Terrorism and Hybrid Treats and entrusted it with the task of challenging radicalization and destabilization campaigns. The agency is seen as an example to follow for other democracies in Central and Eastern Europe. Similar governmental units are needed, especially among states in which Russia is looking to revisit its political, economic, or security priorities. Whether the United States can be a credible leader of this type of coalition depends on political developments at home so that they don't overshadow cyber-diplomacy efforts.

Apart from the formation of a diplomatic network, the EU External Action Service's East StratCom Task Force should be strengthened by additional capacity and capabilities. While this EU diplomatic body declares that

it “corrects information,” the approach of this group (and similar national bodies) should focus on unraveling the ways in which Russian *kompromat*-inspired campaigns have been designed and on using media relations to report on them rather than fighting falsehoods head on. In this approach, knowledge exchange between security services, NATO, government agencies such as the one in the Czech Republic, and think tanks (e.g., Chatham House) is critical in discrediting theories of conspiracy and personalized cyberattacks on politicians. In addition, the US and EU policymakers should be proactive in the development of transparent media relations response strategies. After all, their reputations are at stake if they fall victim to *kompromat*-inspired propaganda.

Apart from cyber-diplomacy efforts, the American media and its regulators can play a proactive role in counterbalancing Russian campaigns. US media broadcasters should monitor the media landscape and facilitate gaining information access to news sources. National broadcast regulators can also play a significant role in ensuring that information carried in national media markets by the external media is produced in accordance with professional journalistic standards. In the case of the United Kingdom, Russia’s RT has been a subject of the investigation by a national regulator, Ofcom, and it has been sanctioned for misleading reporting. The existing evidence suggests that national regulators certainly can do more to inform media audiences about the ownership of external media—for example, the fact that RT is owned by TV-Novosti and hence the Russian state.²²

To challenge the speed with which propaganda is disseminated, investigative journalism should be more proactive. While Western broadcasters report on Russian campaigns, those news media stories tend to be reported as isolated cases, and given

the complexity of the issue, their analysis should be aided with extra resources. Consequently, national media regulators, media organizations, and journalists should pay more attention to cybersecurity. Apart from policy-focused measures, professional standards should be encouraged: for example, initiatives bringing together Western journalists, public diplomacy experts, and Russian diplomats should be facilitated by governments and media organizations as a policy measure for advancing dialogue between the two environments.

Finally, it has to be noted that Russia’s soft power is relational, and so far, it has been difficult to talk about Russian grand soft power strategy. Undeniably, although with varying levels of success, Russia has managed to make some inroads into capturing the attention of some of the international public thanks to nationally focused strategic narratives about a shared past, challenging the features of the liberal international system, fueling polarizing populist agendas and actors, and appealing to the sense of religious and economic ties of Slavic nations. As the powerful strategic narrative of the “transformation” of Central and Eastern Europe is slowly fading away and Russia reemerges to the position of a global player in propaganda games, new attractive strategic narratives should be developed by the Western democracies to challenge Russia’s military posturing and destabilizing propaganda attacks.

Applebaum has argued that the consensus over the acceptance of the narrative of Russian decline meant that the West has found it difficult to respond to Kremlin’s assertiveness.²³ Yet Russian *kompromat*-inspired propaganda has a multiplayer effect—it falls on the fertile ground of nationalism, populism, and illiberal tendencies in which “post-truth politics” or declining respect for facts causes cracks in liberal democracies and deepens divisions in transatlantic diplomatic relations.

Keeping in mind the scale of media capture in Russia as well as the changing global media landscape, Western strategic soft power narratives should have a strong digital dimension. The United States' public diplomacy needs further investment in digital capabilities, and policymakers in the West must amplify a strategic soft power narrative about their relationship to Russia and highlight the role of liberal governance within that narrative.

Notes

1. Wintour Patrick and Asthana Anushka, "Trump-Putin Meeting Dominates G20 as Russia Denies Interfering in US Elections," *The Guardian*, July 7, 2017, <https://www.theguardian.com/world/2017/jul/07/trump-putin-meeting-dominates-g20-as-russia-denies-interfering-in-us-election>.
2. Craig Timber, "Russian Propaganda Effort Helped Spread 'Fake News' during Election, Experts Say," *Washington Post*, November 24, 2016, https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html?utm_term=.35e624918979.
3. Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lanham, MD: Rowman & Littlefield, 2016), 47–65.
4. Paul R. Viotti and Mark V. Kauppi, *International Relations and World Politics*, 5th ed. (New York: Pearson, 2013), 207.
5. John Holden, *Influence and Attraction: Culture and the Race for Soft Power in the 21st Century* (London: British Council, 2013).
6. Philip Seib, *The Future of Diplomacy* (Cambridge: Polity Press, 2016).
7. Pawel Surowiec, *Nation Branding, Public Relations and Soft Power: Corporatizing Poland* (London: Routledge, 2016).
8. "Information Warfare Versus Soft Power," *ProjectSyndicate.org*, May 9, 2017, <https://www.project-syndicate.org/commentary/cyber-warfare-weakens-russia-soft-power-by-joseph-s-nye-2017-05>.
9. Herpen, *Putin's Propaganda Machine*, 27–28.
10. Nadia Kaneva, "Russian Appropriations of Soft Power." Paper presented at the International Communication Association Conference, San Diego, May 24–29, 2017.
11. Olubukola S. Adesina, "Foreign Policy in an Era of Digital Diplomacy," *Cogent Social Sciences* 3, no.1 (2017): 1–13.
12. Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nations Cope in the Future Conflicts?" *Journal of Slavic Military Studies* 27, no. 1 (2014): 101–30.
13. "Russia Is Attacking Western Liberal Democracies," *Medium.com*, n.d., <https://medium.com/@romangerodimos/russia-is-attacking-western-liberal-democracies-4371ff38b407>.
14. European Council on Foreign Relations (ECFR), *The World According to Europe's Insurgent Parties: Putin, Migration and People Power* (London, 2016), 17.
15. Corneliu Bjola and Marcus Holmes, *Digital Diplomacy: Theory and Practice* (New York: Routledge, 2015).
16. Herpen, *Putin's Propaganda Machine*, 90–94.
17. Chatham House, *Russia's New Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (London: Royal Institute of International Affairs, 2016), 30.
18. Nicole Perlroth, "Russian Hackers Who Targeted Clinton Appear to Attack France's Macron," *New York Times*, April 24, 2017.
19. Sarah Oates, "How Russian 'Kompromat' Destroys Political Opponents," *Chicago Tribune*, January 17, 2017.
20. Chatham House, *Russia's New Tools for Confronting the West*, 3.
21. "Cyber-diplomacy Versus Digital Diplomacy," *USC Center on Public Diplomacy*, May 12, 2016, <https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>.
22. Chatham House, *Russia's New Tools for Confronting the West*, 53.
23. "How He and His Cronies Stole Russia," *New York Review of Books*, December 18, 2014, <http://www.nybooks.com/articles/2014/12/18/how-he-and-his-cronies-stole-russia/>.