Russia continues to project its economic, political, and military power across Europe to challenge the U.S. position as leader of the liberal international order and the NATO military alliance. How might Russia use its technological advancements to counter U.S. values and interests? Cyber warfare and new hypersonic weapons are particularly important. As for asymmetrical political warfare, how can the United States respond to Russia’s (dis-) misinformation campaigns and other technological offensives aimed at undermining the U.S. political system and that of its allies? Are there any avenues for the two countries to improve their relationship in the new age of disruptive technology? Does Russia have an Achilles heel regarding disruptive technology, or can it fend off Western attempts to contain its aggressive deployment of technology?

Introduction:
Technological subversion as a commonplace tool of statecraft

Attempts by Russia to use new technologies to undermine the legitimacy of the U.S. political system and the capacity of its economy should come as no surprise to Americans. State and non-state actors have used technological innovations to weaken their opponents for centuries. Russia logically follows this historical pattern in part because weaponizing new technologies is a relatively cheap way to balance against an adversary, particularly one of enormous comparable power. America outstrips Russia in just about every crucial metric of power: population size, favorable demographic trends, technological prowess, economic wealth and productivity, and an enormous military-industrial complex that supplies an advanced military and a world-wide network of bases. Equally important, the allies of the United States, including key countries in Europe as well as Canada, Japan, and Australia, augment American power in significant ways.

By contrast, Russian state power is in decline. The precipitous slide in Russian capabilities caused by the aftermath of the collapse of the Soviet state has ended, but highly negative demographic and economic trends persist and are largely impervious to improvement. Its network of external partners is similarly weak. Russia is left to consort with weak states such as Belarus, Cuba, and Iran. While an important exception is Russia’s strengthening relationship with China, it is still unclear whether their strategic, political, and economic interests will remain aligned over the long term.

Vulnerabilities of American social media and US infrastructure

That Russia has used social media and cyber espionage to divide the American polity and undermine constitutional processes, including national elections, is now common knowledge in the United States. US intelligence services concluded in 2017 that Vladimir Putin had authorized a far-reaching Russian campaign to interfere in the 2016 presidential election to support Donald
Trump’s electoral prospects. In 2020, a bipartisan Senate Intelligence Committee report confirmed the findings of the US intelligence agencies. So too, did Special Counsel Robert Mueller’s investigation into Russian interference which documented an extensive Russian influence campaign to support Donald Trump, disparage candidate Hillary Clinton, and more generally polarize American attitudes and values.

Russia has also attacked American infrastructure with devastating effectiveness. The most dramatic example was discovered in 2021 in connection with a routine software update conducted in 2020 by the technology firm SolarWinds. About 18,000 clients in the private and public sectors were potentially affected. SolarWinds was apparently targeted by the SVR, an arm of Russian intelligence, which installed malicious code in the SolarWinds update.¹ These and other hacks authorized by the Kremlin, either through Russian government agencies or non-state actors, including criminal gangs, are designed to either steal or destroy data on a massive scale. Russia is an effective adversary because it has long developed and tested its cyber strategy in operations against its neighbors, including Ukraine and Estonia. More important, the Kremlin for two decades has used malign cyber tactics against its domestic political adversaries as well as the Russian population as a whole. Some scholars have called Russia and similar states “information autocracies” which combine censorship of the opposition and the mass dissemination of regime-supportive narratives to manipulate public opinion and cripple the marketplace of ideas.²

What is to be done?

While Russia’s cyber threats to America’s infrastructure are serious, the danger to American democracy is likely even greater. One of the most important questions facing the United States is how to counter Russia’s attempts to exploit divisions in American society which make it a soft, inviting target. While these divisions were decades in the making, populism more fully exposed – and deepened -- these social, cultural, economic, and political fissures. Large segments of the American public now feel they are strangers in their own land, or soon to become so due to economic dislocation, unemployment, and social insecurity. Fears of cultural marginalization intersect with these economic concerns, heightening social and political alienation.³ Trust in national institutions as guardians of America’s well-being are now at their lowest ebb in decades.

With the decline in the ability of political institutions to address societal grievances and mediate political conflict, sectarianism approaching tribalism has grown quickly in the United States. That the major political parties in recent decades have increasingly sorted along racial, educational, and geographic lines has worsened this condition. Distrust of the motives and morals of members of the other party strongly incline voters to value partisan purity over bi-

---

³ For an excellent study on these issues, see Pippa Norris and Ronald Inglehart, Cultural Backlash (New York: Cambridge University Press, 2019)
partisan compromise. A 2020 public opinion survey found that 57% of respondents agreed with the statement that the “US is in the midst of a cold civil war.”

Healing these social wounds, thereby reducing America’s vulnerability to Russian influence campaigns, will take years of efforts. But of what kind? Reforms that check or roll back gerrymandering of congressional districts would increase political competition – essential to exposing voters to authentic political competition and the marketplace of ideas. More immediate steps are contained in current legislation before Congress. Whether or not you agree with the current budgetary priorities of the Biden Administration, these measures are likely to address key social problems and help reduce the extreme polarization and populist grievances that challenge American democracy. For example, providing greater access to higher education, re-training, affordable health care, childcare, and other social services will weaken widespread feelings that the American dream is a myth and help restore the belief that the American experiment is based on fairness, equity, and justice. American politicians who feel that the cost of Biden’s program is too high, in ideological or economic terms, must offer a coherent alternative vision and policies to restore trust in American institutions. The more US public policy effectively addresses populist grievances; the weaker Russia will be to divide American public opinion.

Other, more direct measures can be taken to reduce the effects of malign influence campaigns such as Russia’s. While platforms like Facebook, YouTube, and Twitter are not the primary source of the political divisions in America, they clearly stoke divisiveness and sectarianism. Such platforms could employ crowdsourcing to identify false or hyper-partisan content and incorporate such information into algorithmic rankings on a permanent basis to reduce its presence in people's news feeds. Similarly, they could devote greater effort to confirming the true identity of the sources of online information, thereby denying access to foreign actors with malicious intent. Measures such as these would help reduce the size and effect of sectarian echo chambers at major points on the American political spectrum.

It is unlikely that popular and powerful social media platforms will embrace these and similar measures to effectively police themselves. Here judicious political intervention may be necessary. Legislation that enables the government to engage in consistent and effective oversight of social media could empower the Federal Trade Commission to develop and enforce a social media code of conduct. Such rules of behavior and their enforcement would fall under the FTC’s capacity to monitor and proscribe “unfair or deceptive” commercial practices. Efforts in this direction have recently been taken. For example, one of the tasks of the investigation opened by the US House of Representatives into the January 6th insurrection is to determine the role of social media in fomenting the violence. Another effort is the proposed Online Consumer Protection Act which would increase the accountability of social media companies which, according the bill’s fact sheet, “for too long…have allowed harmful content to spread across


Believing that transparency is an essential first step to reducing the political pathologies associated with social media, some experts have proposed that the largest platforms, including Facebook and Google/YouTube, be required to disclose how their algorithms rank, recommend, and remove content. The dangers to privacy and free speech that might arise from such government intervention cannot be taken lightly. Americans hopefully share enough in common to responsibly debate and propose policies that react to external threats while defending domestic freedoms. A debate of this kind would necessarily educate Americans as to the nature of the threat and what the agencies of the US government are now doing to confront hostile external actors like Russia. Responses by the US government are at hand. Congress established the Cyberspace Solarium Commission in 2019 to identify and understand the threats against the United States and to generate proposals on how best to protect the US in cyberspace. Frontline US government agencies have already adopted a proactive strategy and a forward defense that seeks to confront, not react to, cyber threats from abroad and perhaps engage in preemptive behavior.

For example, US Cyber Command, headed by GEN Paul Nakasone, has embraced a “defend forward” strategy that is implemented through a doctrine of “persistent engagement.” In brief, this approach advocates that the US be proactive in meeting existing challenges and anticipating hostile cyber strikes. According to Nakasone, the “country cannot afford to wait for attacks to come its way.”

But no matter how capable and willing they may be to pursue engagement with malign actors, US agencies may be constrained by the US president, who must balance competing imperatives. For example, while the Administration of President Joe Biden has imposed new sanctions on Russia in connection with its election interference and cyber hacking, it has also stated that the US does not want to be drawn into an “escalatory cycle” with Russia, and that its responses to the Kremlin’s malign behavior would be “proportionate and tailored.” In short, the current Administration wants its relationship with Russia to be “stable and predictable.” According to Nakasone, his agency can guard against miscalculation and escalation even as it competes “proactively in cyberspace.”

Can the US and Russia just get along?

As the United States works to develop strategies to counter Russian technological hacking and subversion, it is important to keep the dimensions of the threat in mind. While the Kremlin clearly values disruptive technologies as “weapons of the weak,” it is likely sensitive to the limitations on their use. If history is any guide, the targets of technological subversion often

9 For the Commission’s 2021 report on recommendations see https://www.solarium.gov/
develop effective counter-measures. Equally important, the Kremlin is aware that its subversive tactics via social media, hacking, and other technologies must stay below the threshold of war if it is to have a margin of safety against the United States, as a much more powerful state, engaging in devastating retaliation. One problem, of course, is the difficulty in determining the location of that threshold particularly when cost-benefit analysis on the part of a state is conducted in conditions of significant power imbalances.

The Kremlin may also temper its risk-taking strategy because the Russian political system and the Russian state itself is relatively fragile. The Russian state is weak not only because the economy is wracked by dependence on fossil fuel exports and a developmental model that relies heavily on ineffective state management. Widespread corruption also cripples Russia, with efforts at authentic modernization undermined by incumbent elites interested primarily in self-aggrandizement. According to a leading Russian analyst,

Russia is governed by a class of people who are, for the most part, self-serving, and do not care at all for ordinary people or the country, instead focusing single-mindedly on making themselves rich on the job. Money—or rather Big Money—has become that group’s top value, and the most corrosive element in today’s Russia. Therein lies perhaps the biggest vulnerability of modern Russia.12

The weakness of the regime is heightened by the powerful grip of one-man authoritarianism, which undercuts its capacity for self-adjustment in the face of political and socio-economic challenges. The dramatic assessment in 2014 by Vyacheslav Volodin, a leading Russian politician, that “there is no Russia if there is no Putin” points to how insecure the Russian regime is potentially.13 That the Kremlin understands its vulnerability is demonstrated by the intensification over the past two years of crackdowns on even modest forms of political protest and other forms of organized political activity outside the control of the government. The independence of the Russian internet has been curtailed and the operation of foreign human rights organizations all but eliminated. Further, the regime has ramped up its domestic propaganda machine, underscoring it designation by scholars as an “information autocracy.”14

Russia may also restrain its covert meddling in American politics because it needs the cooperation or at least the acquiescence of the United States in its pursuit of important goals. These include Russia’s continued access to international flows of capital and investment despite existing sanctions imposed by the West as well as collaboration on agreements related to climate change and arms control.

**Uncertain futures and the need for vigilance**

While these factors should caution the Kremlin against relying too heavily on cyber operations against the West, Russia may still balk at moderating its subversive behavior and may even

---

13 *Moscow Times* 23 October 2014.
choose to escalate. Much depends on Moscow’s threat perception and how it might lead to miscalculation. The Kremlin has long feared the meddling of foreign powers in Russia and in its immediate region. These are powerful themes that resonate far into Russia’s past and include such episodes as Imperial German support for Vladimir Lenin to travel in 1917 from exile in Switzerland to the Finland Station in St. Petersburg in order to foment revolution.

To be sure, the Kremlin is properly blamed in the West for crafting misinformation campaigns—such as its actions during the 2016 U.S. presidential election—as part of a strategy of hybrid warfare that seeks to weaken America as an adversary. Yet Russia has long accused the United States of using subversive methods of its own to challenge Russia’s regional power and threaten the legitimacy of Putin’s government in Russia itself.

In a society where conspiracy theories are more prevalent than in the West, Russian mass and elite opinion often hold the United States responsible for the collapse of the Soviet Union and the decade of socio-economic and political turmoil that followed, all under the guise of assisting the creation of market democracy in Russia. After gaining power in 2000, Putin increasingly embraced the long-standing mistrust of the US held by Russia’s ruling elites. In the coming years Putin, his political elites, and much of Russian society viewed the political turmoil of the Arab Spring (2010), the mass demonstrations in Russia against Putin in 2011 and 2012, and then the 2014 overthrow of Viktor Yanukovych in Kyiv as more evidence of America’s regional ambitions and subversive tactics. Today, many in the Kremlin and elsewhere in Russia consider Alexei Navalny, Putin’s committed political opponent, to be an American agent of some sort.

The actions of the West since the Soviet collapse noted above, as well as the gradual expansion of NATO to Russia’s borders, have provided the Kremlin with ample raw material to craft a narrative of American duplicity and aggression. For these reasons, Putin likely views Washington’s protests against Russian cyber attacks and subversion against the United States and its allies as hypocritical. If so, this perspective may leave him less unwilling to dial back the use of hybrid warfare, particularly if he feels that confrontation with the West is likely to increase for the foreseeable future. Events would seem to support such a viewpoint. Russia’s seizure of Crimea in 2014 accelerated America’s turn from the War on Terror toward Great Power Competition as the new national security paradigm for the United States. Whether this new framework, with its focus on long-term competition with a resurgent Russia (and an ascendant China), provides a sound basis for US foreign policy will depend on whether it properly assesses the complex sources of that rivalry. For the foreseeable future, however, the United States should expect that Russia will continue to use disruptive technologies, but with uncertain intensity, to weaken the political cohesion and economic capacity of the United States, its primary rival.

**Questions for Discussion**

- On balance, how serious a danger does Russia pose to the security of the United States? Are Russian threats to US infrastructure and the Kremlin’s misinformation campaigns the

---

main dangers? Or is the threat of hybrid warfare against our allies and partners in Europe equally serious?

- Under what conditions should the United States use its considerable cyber capability against the Russian homeland? Should it employ tools and tactics similar to those used by Russia against the United States? Or should the US focus primarily on sanctions as a response to Russia’s hostile behavior?

- Is it possible, and desirable, for the United States and Russia to come to an agreement not to use cyber weapons and misinformation campaigns against each other? Is there utility in contemplating bi-lateral or multi-lateral agreements to enhance American security?

- What are the prospects that Russia and China, both “information autocracies,” will align more closely to confront US global power? What are the factors that draw both countries together? What might keep them apart?

**BIBLIOGRAPHY AND SUGGESTIONS FOR READING**

- Paul Barrett, Justin Hendrix, and J. Grant Sims, *Fueling the Fire: How Social Media Intensifies U.S. Political Polarization* New York: NYU/Stern Center for Business and Human Rights, 2021. [https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/613a4d4cc86b9d3810eb35aa/1631210832122/NYU+CBHR+Fueling+The+Fire_FINAL+ONLINE+REVISED+Sep7.pdf](https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/613a4d4cc86b9d3810eb35aa/1631210832122/NYU+CBHR+Fueling+The+Fire_FINAL+ONLINE+REVISED+Sep7.pdf)

- Cyberspace Solarium Commission, Reports, at [https://www.solarium.gov/](https://www.solarium.gov/)


