Are the Russians Coming in Cyberspace this Election Day?

Eric W. Orts*

On November 2-3, the Center for Ethics and the Rule of Law held a timely conference on "Democracy in the Crosshairs: Cyber Interference, Dark Money, and Foreign Influence." Most of the conference was conducted under Chatham rules, which means that this report will not include reference to individual people for various statements or understandings.

There is good news and bad news. The good news is that sources in the U.S. intelligence community do not see any activity that suggests that the Russians may be attempting to hack the election on Tuesday – at least in the sense of actually trying to get access to voting machines or registrations to affect the result directly. The United States has not yet taken the steps that it should to defend itself, however, and the Russians (and maybe other foreign powers) may simply be waiting for the Presidential election in 2020 to interfere directly. We know that many states' voter registration systems were accessed by the Russians in 2016 – though there is no evidence that the Russians made changes in registrations, perhaps owing to a very strong warning of a counterstrike by President Obama if they did. Approximately $350 million was allocated by the Congress and Obama Administration to shore up election security. Disturbingly, some states refused to accept any funding. So the bad news is that the U.S. electoral infrastructure remains relatively weak in many states. Improving the security of the election system in the United States should meet with broad political approval. But it's clear that at least some Republicans who support Trump do not wish to pay much attention to this issue – for obvious reasons.

As one participant observed, a significant problem with building a consensus on security for our national elections is that one side will often benefit from a foreign intervention. Flip the narrative at the moment (where President Trump has been the beneficiary of Russian intervention), and imagine that the Chinese decided to intervene in the 2020 election after being on the receiving end of punishing Trump tariffs. If Democrats won in a landslide, in part with the help of the Chinese, then Democrats might (like Republicans now) be more likely to defer examining election security as a priority.

This thought experiment should show why it's important – and even essential – for election security to become a high priority for American citizens and politicians regardless of party and ideology. If we can agree that American citizens should retain the right to self-determination – as one paper at the conference emphasized – then we all should agree to make our elections more secure against foreign intervention. And there at a number of reforms that should be prioritized.

1. **Harden the targets of our election machinery against the threat of outside cyberattacks.** The fact that the Russians have been able to gain access to the voting systems of seventeen states in 2016 should put us on notice that there is a serious problem. Individual states should invest in reforms of their election systems – coordinating with U.S. Cyber Command and the Department of Homeland Security. Moving toward voting-by-mail or paper ballot systems would be helpful – providing a forensic check on any attempt to actually change votes after they have been recorded electronically. Sufficient training of those overseeing polls should also be increased – and perhaps more civil servants added for this purpose as well. One issue for the future is whether the federal government should have the authority to require states to make changes. My own view is that the answer to this question is "yes." The right to vote is guaranteed under the various voting amendments to as well as in the basic structure of our Constitution. Congress should enact legislation – and provide funding – to protect our election infrastructure as a high priority of national security.

2. **Increase transparency of identities in cyberspace.** One of the most disturbing and most effective methods of Russian interference in the 2016 election was their adoption of fake American personas by which to spread disinformation and otherwise manipulate public opinion. The effectiveness of the Russian active measures (which also included hacking of both the Democratic National Committee and the Republican National Committee) led to the evolution of the Russian intelligence objective – from merely sowing dissension to actually attempting to change the result of the election. The Russians used the information that it stole from the DNC to devastating effect via well-timed disclosures to Wikileaks. According to a study by Penn colleague Kathleen Hall Jamieson, the Russian intervention in fact made the difference in a very close election. According to her careful and detailed analysis in *Cyberware: How Russian Hackers and Trolls Helped Elect a President* (2018), Jamieson concludes that given the very close election (caused by many factors, including the relative success of the Trump versus Clinton campaigns), "the Russian intervention swung the election to Trump" (p. 213). The Russian covert influence campaign in the 2016 election will therefore go down as one of the biggest espionage victories in history.

However, winning one election – or one battle – is not winning the war. I would draw an analogy to the Japanese attack on Pearl Harbor. It was a great victory, and the Japanese caught us by surprise. But just as the American dragon awoke to fight and defeat the authoritarian regimes of Japan and Germany in World War II, I believe that the Russians have awoken the American dragon of democracy.

In addition to the need for political parties to harden their own targets against outside hacking, more general reforms are needed to prevent similar fake personas. No consensus emerged about how far to go in terms of requiring disclosure of "real identities" on Facebook, Twitter, and the internet in general. Facebook has been cracking down on fake identities, though the problem seems to be rather large (at least judging from many fake friend requests that I get and hear about). Regulation may be needed – and education measures would also help. Once fooled, people will often not be fooled again – at least not once they are informed and understand how they got fooled in the first place.

3. **Follow the money: increase the transparency of legal entities.** Another problem that aided the Russians was the relative ease by which investments can be made in the United States anonymously. Another Penn colleague, Kevin Werbach, has shown that worries about bitcoin and cyber-currency have been overblown. It appears Special Counsel Robert Mueller's investigation was able to identify Russian fingerprints on our election interference in part through tracing bitcoin through intermediaries. A larger problem involves the anonymity that American legal entities allow. Many state corporate laws do not require the identification of the actual owners of corporations. And the situation is even worse for limited liability companies (LLCs). Money can be funneled through these entities without revealing the true owners. Although some arguments in favor of economic efficiency may have supported allowing this anonymity (such as for a real estate developer putting together a large block of properties without revealing the true owner to all sellers), the threat of anonymous electoral interventions by foreign powers – combined with the threats of financing terrorism and criminal syndicates – should tip the balance toward reform. Congress should enact legislation requiring states to close these loopholes. One good approach would be to require full disclosure of ownership for any legal entity that wishes to open a U.S.-based bank account.

Many other topics were discussed at the conference. Suffice it to say that the Russian attack on the American election of 2016 have revealed huge vulnerabilities that a free society faces in the world of cyberspace. This new technology is extremely powerful – and has been used and will continue to be

used for good. The internet speeds the process of globalization and reduces transaction costs for the movement of people, money, goods, and materials in international commerce. At the same time, the openness and freedom of the internet – as well as the anonymity that it often provides – raise difficult problems for the preservation of democratic government.

My own view – which may have been a somewhat hawkish minority view at the conference – is that Russia's attack on our election in 2016 – was the equivalent of an act of war. The Russians attacked our country at its very core: our political system of constitutional democracy. There are indications that President Trump or his operatives may have colluded with Russian intelligence. (We will soon see the result, I expect, of Robert Mueller's investigations.) Whether or not there was collusion, it now appears likely that the Russian espionage campaign of "active measures" in fact had the result of electing Trump rather than Clinton. The question then remains how the United States should respond in the future to cyberattacks of a similar kind. Clint Watts at the public forum called for immediate counterstrikes in cyberspace to "melt their keyboards") – and probably the United States should become more forceful without escalating the conflict to dangerous levels, namely, nuclear war. Long-term consequences must also be considered.

In conclusion, the free world – as General McMaster argues – is now in a renewed fight with Russia's authoritarian regime. Most likely, this fight for freedom and democracy will extend to China as well, which even as it benefits economically from joining the global liberal order is now, like Russia, also failing to keep its promises to reform and follow "the rule of law" and recognize basic human rights. One of the principle fronts of what I would even go as far as to call the New Cold War will be the world of cyberspace. And if there is one thing that everyone at this conference agreed: there is a lot of work to be done on many levels on this very different and complex battlefront.

* Eric W. Orts is the Guardsmark Professor of Legal Studies and Business Ethics at the Wharton School of the University of Pennsylvania. He is author of *Business Persons: A Legal Theory of the Firm* (Oxford University Press, rev. ed. 2015) and will be teaching a new course on "Business, Law, and Democracy" next semester.