COMMENTARY ON THE ROLE OF LAW
COMMENTAIRE SUR LE RÔLE DU DROIT

"Our Democracy Itself is in the Cross Hairs":* Why Election Security Matters in the United States

William C. Banks[**]

Candidate Donald Trump stated during the campaign that he reserved the right not to accept the election result, as if only vote-rigging or corruption could explain his possible defeat. While certainly cynical, candidate Trump acted consistently in his campaign to tap into the populist theme of mistrust in government. Although Trump's warnings about legions of illegal voters never materialized, despite his continuing claims to the contrary, the lingering mistrust has been sustained by the vulnerabilities in our electoral process that can be exploited through cyber means and by influence operations.

Americans now know that in November 2016, voters narrowly elected Donald Trump as President, aided by Russian cyber hacking and influence operations designed to harm the chances of opponent Hilary Clinton and support Trump. Before and after the election U.S. intelligence officials officially concluded that Russia had attempted to infiltrate and influence the outcome of the presidential election in favor of candidate Trump even while candidate and then President-elect Trump repeatedly dismissed the report of the Intelligence Community as "all a big hoax." Trump claimed that "it could be other people" and not the Russians and that, in any case, he won the presidency on the merits of his candidacy.

Now, nearly two years into his presidency, Donald Trump continues to dismiss the Russian electoral threat entirely or say that it is not serious, or worse yet, say at a Helsinki press conference that he believes Vladimir Putin's denial of Russian involvement in our elections. Meanwhile, special counsel

---

* Department of Homeland Security Secretary Kirstjen Nielsen, quoted in Michael D. Shear and Michael Wines, Russian Threat 'Is Real," Trump Officials Say, Vowing to Protect U.S. Elections, NY Times, Aug. 2, 2018.

** Board of Advisers Distinguished Professor, Professor of Law and Professor of Public and International Affairs emeritus, Syracuse University; Editor Journal of National Security Law and Policy.

Robert Mueller continues an investigation of Russian meddling in the 2016 election, including possible collusion between the Trump campaign and Russian operatives. The President has repeatedly disparaged the investigation as a "witch hunt," threatened to fire Mueller and/or his overseer in the Department of Justice, and obstructed the inquiry itself by firing FBI Director James Comey and asserting that Attorney General Jeff Sessions should put a stop to the investigation.

Although both houses of Congress have opened their own investigations of 2016 election interference, partisan grandstanding has stood in the way of significant substantive legislative outcomes. Bills to protect the integrity of the special counsel have languished in committee, and proposals to greatly expand investment in election security for 2018 and beyond have failed to advance.

After the President back-tracked from his denials of Russian interference in Helsinki, in early August 2018 senior Trump administration intelligence officials reiterated that the Russian threat in 2018 and 2020 is "real," and is a "24-7 365-days-a-year" effort by Russia to sow divisions as Americans head to the polls this fall. At the same time, federal officials recognized a fundamental fact about election security in the United States – that their role is secondary. In our federal system, "the times, places and manner of holding elections . . . shall be prescribed in each State by the legislature thereof. . . ."[1] Indeed, the threats are manifested directly in our states, counties, and cities, where elections systems are developed, implemented, monitored, and governed. Although federal grants have allowed some states to upgrade computer systems and voting machines since the 2016 elections, those systems and the infrastructure of individual political campaigns remain vulnerable to hackers and influence operations. No one is sure what to expect from Russian hackers or influence operations in the weeks and months ahead.

As extraordinary as these events may be, foreign governments have interfered in U.S. elections before, with some success. In 1796, after President George Washington concluded a treaty with Great Britain, France decided that it was time for a change in leadership in the United States. France began openly supporting Republicans and favored candidate Thomas Jefferson, who eventually lost to Federalist John Adams in succeeding Washington. The French released notes critical of the treaty and Washington for publication in a Philadelphia newspaper and otherwise lobbied Jefferson, with little apparent success. Washington warned in his farewell address "against the insidious wiles of foreign influence . . . one of the most baneful foes of Republican Government."

In 1940 and 1941, Great Britain used its intelligence services to help President Franklin Roosevelt push for U.S. intervention in World War II. Their spies spread negative rumors about aviator Charles Lindbergh, leader of an isolationist America First movement. They wiretapped foreign embassies in Washington and passed information along to Roosevelt and gave money to

---

[1] U.S. Constitution, Art. I, sec. 4, cl. 1.

interventionist groups in the U.S., all with the approval of Prime Minister Winston Churchill.

In 1968, Richard Nixon's campaign colluded with the South Vietnam government to delay peace in the Vietnam War. During the period when President Lyndon Johnson offered to call a halt to bombing in Vietnam in return for progress in ongoing peace talks, Republican activists reached out to Saigon with a promise of better peace terms from a Nixon presidency. The Vietnamese then delayed negotiations and prolonged the war, assisting Nixon's victory.

There are other, more recent incidents: the Soviet Union attempts throughout the Cold War, spreading false theories about the Kennedy assassination and that FBI director J. Edgar Hoover was gay, discrediting Martin Luther King, Jr., spreading false rumors that the AIDS virus was manufactured by the U.S. government, and Israel attempting to leverage partisan disagreement on Iran's nuclear program in order to ensure tougher sanctions on Iran, all without informing the Obama White House.

These tactics are really tactics of war, chronicled by Sun Tzu: When confronted by a stronger enemy, sow confusion and dissension in its ranks. Director of National Intelligence Dan Coats has said that, 30 years after the fall of the Soviet Union, Russia remains our adversary and the signals of continuing Russian interference are similar to the warnings the U.S. had before 9/11. As Coats said, "The warning lights are blinking red again." Unsurprisingly, the Russian tactics have been spelled out in recent years by Russian military thinkers who have predicted that upcoming conflicts will be dominated by information and psychological warfare, melting away conventional lines between states of peace and war. Eastern Ukraine and Georgia are stark reminders.

The recent indictment by special counsel Mueller of 12 Russian intelligence officers for meddling in the 2016 election made clear that the Russians are using a 21st century version of Sun Tzu's ancient playbook. The indictment richly details how hackers within the Russian military intelligence service GRU conducted cyberattacks against specific targets in the U.S. Human error and software vulnerabilities were exploited to gain access to IT systems belonging to political campaigns and software companies. The attackers worked to use our political and social divisions against us, and they stole or created identities of conservative and progressive activists to sow misinformation and elevate mistrust. They also targeted election systems themselves in at least 21states. The Russians gained access to the records of at least 500,000 voters, although there is no evidence that vote tallies were changed. The mass-production of fake news occurred in so-called "troll factories," primarily distributed through social and alternative media channels. The goal was to embarrass, confuse, or tie up resources, and also to reinforce conflicts, reduce confidence in politicians and traditional news media, and to foster polemical debate.

It bears emphasizing that only with trust in an election's outcome does the opposition accept defeat and legitimacy is conferred on the winner. Sowing

doubts about the credibility of election results, or the impartial process of campaigning that precedes the election, undermines the foundation of democracy.

Indeed, states and their political subdivisions are the new battleground for these assaults on our national security. A successful attack in just one state could sow seeds of distrust in the coming midterm or 2020 presidential election. We know about weaknesses in the IT infrastructure inside and outside government. Voting infrastructure sorely needs help in threat detection and prevention. Ironically, not much of it can come directly from the federal government. After outgoing Secretary of Homeland Security Jeh Johnson declared voting to be a critical infrastructure and thus "eligible to receive prioritized cybersecurity assistance" from DHS, the National Association of Secretaries of State opposed such a designation on the grounds that it may constitute encroachment and thus challenge the supremacy of state and local governments in administering and running elections. A recent study by the Center for American Progress found that, while all 50 states have taken some steps to provide security in their election administration, most states received mediocre or failing grades on the security and reliability of their systems.

Responsibility for managing election system vulnerabilities is spread among about 5,000 local, mostly county-level, offices. On the one hand, decentralization is a security advantage because adversaries normally prefer big targets and high return on investment. On the other hand, successful hacking or influence operations in even a single congressional district could greatly impact a national election and/or sow mistrust among citizens in the integrity of voting in other districts. Particularly in the United States, with a two-party system (effectively) and its winner-takes-all principles (including in choosing delegates to the Electoral College) narrow, majority-changing interventions can have tremendous effect. The "swing states" can be the battleground for the hackers and outside influencers, just as they are for the two parties and their candidates.

There is no doubt that the Kremlin meddled in the 2016 election and expects to do so again in 2018 and beyond. Regardless of whether Russia conspired with the Trump campaign, and it looks increasingly certain that they did, Russia benefited from the 2016 election outcome. Sanctions and criminal indictments will not deter Russia now or in the future. Those actions have little impact, and Russia gains from its relatively modest investment in cyber hacking and influence operations. Expect more of the same, in ever more sophisticated forms.