EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election

The real story behind alleged foreign interference in our election isn't that it occurred—any impact on the outcome from Russian hacking and trolling was minimal—but that we set the standard for such activity and have no one but ourselves to blame.

It seems that the Russian election interference story has taken on a life of its own. According to a recent report in *The Intercept*,[1] Russian military intelligence launched a spear-phishing attack against at least one voting-machine software supplier and more than 100 local election officials in the US. *The Washington Post* alleges that President Vladimir Putin ordered such attacks to help elect Donald Trump.[2] Putin denies such involvement with pro forma political doublespeak: "We never engaged in that *on a state level*, and *have no intention* of doing so"[3] (italics added: note the qualifier in the first clause and the verb tense in the second). According to the *Intercept* article, a leaked NSA assessment "concluded with high confidence that the Kremlin ordered an extensive, multi-pronged propaganda effort 'to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.'" It's time to intelligently put this story to rest.

Did Russia engage in the spear-phishing attack and Democratic National Committee hack? I wouldn't put it past them. But all of the evidence has been classified by the US intelligence agencies, so we really don't know for sure. I've written before about the problem of establishing cyberattribution within a security vacuum.[4] With this story, the problem rears its ugly head again.

The NSA report states "it is unknown whether the ... spear-phishing deployment successfully compromised the intended victims, and what potential data could have been

accessed by the cyber actor" (assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf). One target was a developer who sells registration system software to voting-machine hardware vendors. Certainly, this would be an important hack of voting systems—removing people from voting registration records would deny them the opportunity to vote. (Indeed, as we'll see later, this is exactly what vote challengers have been doing domestically for years.) The backdrop of this story is that, based on earlier NSA reports, President Obama issued a series of warnings to President Putin to stop his cyberaggression against the US political infrastructure in September 2016—apparently without effect.[5] In July 2017, frustrated by President Trump's vacillating and inconsistent response to Russian meddling in the US election as well as in Syria and Ukraine, the Senate passed additional sanctions against Russia by a veto-proof vote of 92 to 2.[6]

However, the important parts of the story remain underreported, namely: (1) Russian interference in the 2016 US election was far from noteworthy, as the US has continuously interfered in other countries' elections for more than half a century; (2) such interference paled in comparison to long-standing domestic election-manipulation efforts in the US; and (3) the impact of any foreign interference in our election was exacerbated by the US's absurd commitment to outdated and insecure voting policies, procedures, and equipment. We take these up in turn.

The impact of any foreign interference in our election was exacerbated by the US's absurd commitment to outdated and insecure voting policies, procedures, and equipment.

THE GOLD STANDARD FOR FOREIGN ELECTION INTERFERENCE

Reports of Russian meddling in the 2016 US presidential election must be viewed from an objective, historical perspective. It is well documented that, since the end of World War II, the US has been the leader in global election interference,[7,8] with the USSR/Russia in a distant second place. Political scientist Dov H. Levin calculated that, between 1946 and 2000, one or both superpowers interfered in 117 of 937 competitive national elections (12 percent), and that the US conducted 81 of these interventions (69 percent).[9] Levin's analysis excludes covert and military operations to overthrow foreign governments, as detailed in William Blum's *Killing Hope*[7]—a book, it should be noted, that has been updated twice since 1995 to reflect the numerous recent US interventions. What's unique about the current situation isn't election interference; it's that one superpower might have interfered in the other's election.

The only intelligent conclusion that can be drawn is that, if the Russians did what they're accused of doing, we have only ourselves to blame: the shoes have changed feet. But at this point the allegations are just that. With the US intelligence services hiding all relevant evidence under the protective banner of classified sources and methods (even though for the most part they aren't[4]), the public might never know any more than the controlling elite want to reveal—or fabricate.

EVIDENCE-BASED ELECTION MANIPULATION

There's a certain irony to Donald Trump's campaign rhetoric. If, as he claimed, the 2016 presidential election was "rigged," it was likely rigged in his favor. Notwithstanding possible collusion between the Trump campaign and the Putin government, which is currently being investigated by special counsel Robert Mueller as well as various congressional committees, if Russia did interfere in the election, the consensus is that it was to Trump's benefit.

As yet, we have no conclusive answer to these questions. However, there's plenty of evidence of US election manipulation—but by domestic rather than foreign sources. Such manipulation goes back to the Jim Crow era that followed the end of Reconstruction in 1877, when Southern "redeemers" passed numerous voter-disenfranchisement laws.[10] Although these laws were nullified by the Voting Rights Act of 1965, more subtle and variegated forms of vote suppression emerged including voter purging and caging, reduced or eliminated opportunities for mail-in ballots and early voting, imbalanced resource allocation of voting equipment and facilities, required early registration, voter ID laws that effectively disenfranchise minorities and the disadvantaged, voter dilution through redistricting and at-large elections, and so forth.[11] To take just one example, voter suppression in Maricopa County (the seat of Phoenix), Arizona, goes back half a century.[12] None other than William Rehnquist—later Chief Justice of the Supreme Court—actively participated in the suppression of minority voters in that area in the 1960s as a part of a Republican Party program called Operation Eagle Eye. Indeed, the FBI created

<ALT>-FAQs>

Since my last Out of Band column ("Which Is More Dangerous—the Dark Web or the Deep State?," *Computer*, vol. 50, no. 7, 2017, pp. 86–91) three judges of the US 2nd Circuit Court of Appeals rejected Ross William Ulbricht's appeals of his conviction and sentencing relating to the Silk Road case (pdfserver.amlaw.com/nlj/ULBRICHT-ca2-20170531.pdf). The opinion, written by Judge Gerard E. Lynch on 31 May, reads like a proceduralist manifesto: the judges concluded that the district court that convicted Ulbricht properly followed judicial guidelines and thus the trial was fair, the court didn't err in overturning critical defense motions, and the life sentence was reasonable. In other words, the appellate court found that the district court did nothing illegal or unconstitutional—but it did not, and could not, convincingly affirm that the district court's decision made sense. The transcript is noteworthy for its summary of the case, which is highly relevant to the computing profession for many reasons.

For one thing, the circuit court reaffirmed use of the pen register to monitor computer networks. That is, no person may have a legitimate expectation of privacy regarding computing or networking information held by third parties as long as the information doesn't include message content. This means that any type of TCP data may be collected through surveillance without a warrant and used by the government. Presumably this includes all sundry forms of metadata, not just IP address fields in packets. The problem with this position, as privacy advocates have pointed out, is that the metadata itself can "profile" user behavior more than the message content. The circuit court rejected this position out of hand.

A second bothersome point is the district and circuit courts' liberal extension of the Fourth Amendment's "particularity" provision, which requires that a warrant identify the object of searches and seizures with some measure of specificity in order to avoid fishing expeditions. When applied to the digital domain, this presents a problem because a search of "computers and hard drives" is virtually unlimited in terms of the range and scope of data—that is, there's a "lack [of] meaningful parameters on an otherwise limitless search" of a defendant's electronic media. The district court denied Ulbricht's motions to throw out evidence gathered from his laptop on Fourth Amendment grounds, as well as to introduce expert testimony. In upholding this decision, the circuit court held that defendants must not "confuse a warrant's breadth with a lack of peculiarity"—read: as long as the cops meant well, whatever they find is fair game. Civil libertarians will no doubt greet this opinion with little enthusiasm.

Another aspect of the Ulbricht prosecution troubles me if not the circuit court: two of the federal Silk Road investigators connected with the US Attorney's Office for the District of Maryland, one an agent of the Secret Service and another of the Drug Enforcement Administration, were corrupt. Both were subsequently convicted of money laundering and obstruction of justice, and one was also convicted of extortion. The pair were sentenced to lengthy prison terms but not until they had inserted themselves into the Silk Road marketplace. The DEA agent actually operated in a double-undercover capacity: he provided information for the prosecutors as an undercover dealer, and also provided information to Silk Road about the progress of the government's investigation in exchange for $100,000 in bitcoins. He then attempted to blackmail Ulbricht (at this point known only as Dread Pirate Roberts) for another $250,000. Most of their illegal activity wasn't made available to the defense until just before trial—and some still remains unknown. In addition, the district court limited the defense's cross-examination of two other government witnesses. There's no way to know what damage, if any, that evidence about the corrupt agents might have done to the government's case against Ulbricht, but one thing is agreed to by all parties: these men were criminals, and if they were willing to engage in extortion, violating Ulbricht's rights was probably fair game. So much for the poisoned-fruit doctrine.

I have no background in law, but do try to practice common sense whenever I can get away with it. I'm not impressed with the circuit court's ruling or convinced that any criminal trial could be fair under these circumstances. Given the law-and-order makeup of the current Supreme Court, it seems unlikely that Ulbricht will fare much better there than with the 2nd Circuit Court unless, perhaps, the defense adopts a new strategy, such as looking for evidence of parallel construction as mentioned in my July column. In any event, this case has practical consequences for computer professionals, and the transcript deserves perusal.

an extensive file on his activities, some of which was released after his death in 2005.[13,14] Questionable voting practices in Maricopa County continue today.[15, 16] This is how close elections are won and lost in the US. Foreign influence has thus far had a minimal documented effect, although given the propensity in this country to rely on inexpensive electronic election equipment, it's likely just a matter of time until some US election is provably "hacked."

RUSSIAN TROLLING AND THE FAKE NEWS PHENOMENON

There's one area where the Russians and other ideological aggressors might have made a difference in the 2016 election: misinformation campaigns.

Technologists have been particularly insensitive to network trolling, and very few are seriously involved in its detection and debunking.[17] I've discussed the problems that fake news causes with elections before,[18,19] but suffice it to repeat here that without new computing tools, there isn't much that can be done against pervasive and persistent misinformation campaigns—foreign or domestic.

What I call the Fake News Phenomenon holds that the effect of disclosing fake news will be directly related to the knowledge and open-mindedness of the recipient and will be wasted on the uninformed and tribalists. Like other forms of psychological reactance—for example, the Streisand effect, in which people become more interested in information after an attempt to conceal it—is among the most deep-seated because (a) it is motivated by partisan passions and (b) it has been weaponized by ideologues. This accounts for irrational adherence to a belief despite contrary evidence. In recent years, the phenomenon has been compounded by the politicization of fake news to the point that in some circles it has lost its original meaning of news that is false and instead connotes news that conflicts with a particular system of beliefs.

The Russian government's involvement in Internet trolling is well known.[20–22] BuzzFeed offers a "how to" manual with examples,[23] and the US Department of State has a webpage devoted to the practice (share.america.gov/trolls-everything-you-wanted-to-know). That said, modern governments have used propaganda to control global and domestic public opinion for more than a century—in fact, it's the rule rather than the exception. From China's 50 Cent Party to Russia's Olgino factory to the CIA-initiated Radio Free Europe/Radio Liberty, Radio and TV Martí, and Donald Trump's tweets, it's all primarily partisan, content-free misinformation sourced to control public opinion. Fake news, Internet trolling, alternative facts, and a healthy dose of BS are the weapons of choice for modern political picadors. The reason that Russian trolling has drawn so much media attention recently is that it has been effective. However, let's remain clear about the proximate cause of these misinformation campaigns—we perfected the technique. This is just one of the nasty effects of American exceptionalism that has come back to haunt us.

The solution to foreign interference in our elections isn't to condemn other sovereign nations for doing what we do, but to raise the issue for discussion in public forums. In the meantime, the best short-term hope we have for mitigation is technological: mobile apps, browser add-ons, and the like—and certainly not a "cybersecurity alliance" between the principal offenders.[24]

REFERENCES

1. M. Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election," *The Intercept*, 5 June 2017; theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election.
2. G. Miller and Adam Entous, "Declassified Report Says Putin 'Ordered' Effort to Undermine Faith in U.S. Election and Help Trump," *The Washington Post*, 6 Jan. 2017; www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html.
3. Associated Press, "Putin: Russian State Has Never Been Involved in Hacking," *Politico*, 1 June 2017; www.politico.com/story/2017/06/01/putin-russian-state-has-never-been-involved-in-hacking-239014.
4. H. Berghel, "On the Problem of (Cyber) Attribution," *Computer*, vol. 50, no. 3, 2017, pp. 84–89.
5. G. Miller, E. Nakashima, and A. Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *The Washington Post*, 23 June 2017; www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking.
6. K. Demirjian, "Senate Overwhelmingly Passes New Russia and Iran Sanctions," *The Washington Post*, 15 June 2017; www.washingtonpost.com/powerpost/senate-overwhelmingly-passes-new-russia-and-iran-sanctions/2017/06/15/df9afc2a-51d8-11e7-91eb-9611861a988f_story.html.
7. W. Blum, *Killing Hope: U.S. Military and C.I.A Interventions Since World War II*, rev. ed., Zed Books, 2014.
8. T. Weiner, *Legacy of Ashes: The History of the CIA*, reprint ed., Anchor, 2008.
9. D.H. Levin, "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset," *Conflict Management and Peace Science*, 19 Sept. 2016; journals.sagepub.com/doi/pdf/10.1177/0738894216661190.
10. T. Campbell, *Deliver the Vote: A History of Election Fraud, an American Political Tradition—1742–2004*, Carroll & Graf, 2005.
11. T.A. Wang, *The Politics of Voter Suppression: Defending and Expanding Americans' Right to Vote*, Cornell Univ. Press, 2012.
12. J.T. Tucker et al., "Voting Rights in Arizona: 1982–2006," *Southern California Rev. of Law and Social Justice*, vol. 17, no. 2, 2008, pp. 283–365.
13. S. Taylor Jr., "4 Rebut Testimony of Rehnquist on Challenging of Voters in 60's," *The New York Times*, 2 Aug. 1986; www.nytimes.com/1986/08/02/us/4-rebut-testimony-of-rehnquist-on-challenging-of-voters-in-60-s.html.
14. "FBI Documents Reveal Nixon, Reagan Intimidated Rehnquist Witnesses, and Detail the Late Chief Justice's Addiction to Painkillers," Democracy Now!, 5 Jan. 2007; www.democracynow.org/2007/1/5/fbi_documents_reveal_nixon_reagan_intimidated.

15. M.J. Pitzl, "Maricopa County Sending Replacement Ballots to 618 Voters after Error," *The Arizona Republic*, 20 Oct. 2014; www.azcentral.com/story/news/arizona/politics/2014/10/21/maricopa-county-ballot-mailing-error/17649675.
16. F. Santos, "Angry Arizona Voters Demand: Why Such Long Lines at Polling Sites?," *The New York Times* , 24 Mar. 2016; www.nytimes.com/2016/03/25/us/angry-arizona-voters-demand-why-such-long-lines-at-polling-sites.html.
17. A. Chen, "The Troll Hunters," *MIT Technology Rev.*, 18 Dec. 2014; www.technologyreview.com/s/533426/the-troll-hunters.
18. H. Berghel, "Which Is More Dangerous—the Dark Web or the Deep State?," *Computer*, vol. 50, no. 7, 2017, pp. 86–91.
19. H. Berghel, "Lies, Damn Lies, and Fake News," *Computer*, vol. 50, no. 2, 2017, pp. 80–85.
20. S. Walker, "Salutin' Putin: Inside a Russian Troll House," *The Guardian*, 2 Apr. 2015; www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.
21. M. Seddon, "Documents Show How Russia's Troll Army Hit America," BuzzFeed News, 2 June 2014; www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america.
22. J. Acosta, "White House Furious after Being Trolled with Russia Oval Office Photos," CNNPolitics, 12 May 2017; www.cnn.com/2017/05/11/politics/oval-office-photos-donald-trump-russians/index.html.
23. S. Armitage, "Russia Just Delivered a Master Class in Trolling," BuzzFeed News, 10 May 2017; www.buzzfeed.com/susiearmitage/russia-just-delivered-a-master-class-in-trolling.
24. C. Bennett, "Trump's Cyber Tweets Cause Dismay, Confusion," *Politico*, 9 July 2017; www.politicocom/story/2017/07/09/trump-russia-cyber-experts-240340.

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.