Russia-gate’s Shaky Foundation

Special Report: The Russia-gate hysteria now routinely includes rhetoric about the U.S. being at “war” with nuclear-armed Russia, but the shaky factual foundation continues to show more cracks, as historian Daniel Herman describes.

By Daniel Herman

Anyone who watches the news knows that Russian hackers gave Democratic National Committee documents to WikiLeaks and hacked voter databases in 21 states. Prominent Democrats call these shenanigans “a political Pearl Harbor.”

On the blog Daily Kos, one contributor cries “we were robbed!” (arguing that somehow Russian meddling gave Trump a victory in North Carolina, where his margin was 180,000, and where no evidence whatsoever indicates a successful hack of voter databases).

In a new video propamentary, er, docuganda, or something like that, Morgan Freeman declares “we have been attacked. We are at war. This is no movie script.”

Before we hop on the Morgan Freeman train, we might want to consider some history. In 1898, the American press – taking the word of naval investigators – reported that a Spanish mine had destroyed the battleship, U.S.S. Maine. Leading newspapers promptly called for war, and the U.S. government obliged.

Finally, the U.S. became an imperial power with the acquisition of Cuba and the Philippines and a few other odds and ends, at the bargain cost of 2,500 American soldiers dead, plus another 4,000 lost in the Filipino rebellion that followed, not to mention the lives of tens of thousands of Filipino opposition fighters. Only later did it come to light that the Maine was destroyed by a boiler explosion.

In 1915, leading newspapers again whipped up the American public by announcing that a German submarine had sunk the unarmed passenger ship, Lusitania. Two years later – and in part due to lingering outrage over the Lusitania – the U.S. went to war, this time costing 116,000 American lives and over 200,000 wounded, not to mention creating a patriotic frenzy at home that led to beatings, lynchings, and attacks on civil liberties. Decades later, divers proved that the Lusitania was carrying arms to Britain – contrary to government assurances – thus violating international law. German naval intelligence had proved correct.

In 1950, Senator Joseph McCarthy claimed he had a list of men in the State Department who were communists. A credulous press played up his accusations,

despite the fact that the numbers on his supposed list kept shifting. McCarthy and his allies in Congress recklessly charged Americans in Hollywood and in government with being either communists or “fellow travelers,” often ruining their careers.

Congress meanwhile passed the McCarran Internal Security Act, which required suspected “subversives” to register with the government. It also permitted the government to round up and hold those same suspected “subversives” on the order of the President. McCarthy, of course, had no real list, and finally ruined his own reputation by accusing Army brass of communist sympathies. McCarthy’s many allies, however, paid no penalty for overreach.

Fake Intelligence

In 1964, President Lyndon Johnson announced that the North Vietnamese had attempted a second torpedo attack on an American destroyer in the Gulf of Tonkin, then used the incident to get Congress to give him the power to make war.

Thanks to the press endorsing the war effort and cheerleading on the nightly news (at least until the Tet Offensive four years later), the Vietnam War led to 58,000 American deaths and over a million war deaths altogether. Covert U.S. forces, meanwhile, kick-started a civil war in Cambodia that ended in genocide after the Khmer Rouge took power. Cambodia lost over half of its population of 7 million between 1970 and 1980.

It later became clear that there had been no second attack on the destroyer in the Gulf of Tonkin; its crew had misread radar signals.

In 2002, U.S. intelligence, via George W. Bush’s administration, told the American public that Iraq had a hand in planning the 9/11 attacks and, moreover, that Iraq secretly maintained an arsenal of weapons of mass destruction that might be shared with Al Qaeda. Both claims were utterly false, yet the American press – particularly the New York Times, the Washington Post, and CNN – led Americans to believe they were true. Far from questioning authority, the press became its servant. The result: 4,500 American war deaths; at least 110,000 Iraqi deaths (some estimates put the figure at over a million); and a destabilized Middle East, wherein both Iran and ISIS (who are bitter enemies) were empowered. In all likelihood, moreover, there would have been no Syrian war had there been no Iraq War.

When the American press and American political leaders loudly accuse another country of “an act of war,” in short, the American public needs to be on the alert. Rather than marginalizing and belittling skeptics, the press and public

should give them a fair hearing. Far better to have a spirited debate now than to come to the realization in the future that groupthink created catastrophe.

Hack or Leak? It's Worth Asking

With all that history in mind, we should be grateful that William Binney, the National Security Agency's former technical director, is shouting with everything he can muster that the U.S. intelligence community has no solid evidence that Russians hacked the Democratic National Committee. The NSA, he says, would have a record of any overseas exfiltration and could release that data without danger to national security; yet the NSA hasn't. Though Binney left the NSA 16 years ago, he should know: he created the powerful cyber-vacuum that the NSA still uses.

Binney's organization, Veteran Intelligence Professionals for Sanity (VIPS), has produced a report in which they argue that forensic evidence from documents produced by Guccifer 2.0 (G2) suggests – strongly – that G2 was a hoaxer. Skip Folden, a VIPS associate and a former elite tech executive with IBM, has issued his own report that buttresses the VIPS report. Adam Carter (a pseudonymous investigator) and Forensicator (another pseudonymous investigator) have also buttressed the VIPS Report, as have cybersecurity expert Jeffrey Carr and former U.N. weapons inspector Scott Ritter (Ritter disagrees with VIPS in part but not on the basic charge of insufficient evidence).

To the extent they mention the skeptics, American journalists dismiss them as fringe. Yet the skeptics deserve a hearing. Among the important points they make is that U.S. intelligence has only identified the Advanced Persistent Threat (APT) groups (APT 28 and 29 to be precise) associated with the hacking, and not the hackers themselves. An APT is a set of common parameters – tools, modes of operation, target patterns – used by hackers. But how certain are our intelligence agencies that Russians stand behind APT 28/29?

It happens that Dimitri Alperovitch of CrowdStrike – the cybersecurity entity that analyzed DNC servers – was asked that question in June 2016. His answer: "medium-level of confidence that FancyBear is [Russian intelligence agency] GRU… low-level of confidence that CozyBear is [Russian intelligence agency] FSB."

Skip Folden suggests that Alperovitch's estimates equal a 37-38 percent probability that Russian intelligence stands behind APT 28/29. It's not clear how Folden came up with that figure. We should note here that Alperovitch subsequently raised his confidence levels to "high," but then had to reduce them again in March 2017 after realizing that his new assessment was based on phony data published by a Russian blogger. Meanwhile, in January, Director of National

of Intelligence James Clapper's hand-picked team had used Alperovitch's "high confidence" assessment of Russian hacking of the DNC, which every major network reported dutifully without so much as a blink.

It's hard to say what additional evidence the NSA/CIA team might have had – or whether there was any – though there are rumors that a Kremlin mole working for Latvia confirmed that Putin ordered his cyber-warriors into action. The NSA, however, didn't consider the source fully trustworthy (remember Curveball, the wonderful gift of German intelligence?), hence it committed itself to only "moderate confidence" even as the CIA stated "high confidence." At any rate, the January report lacked both solid technical evidence and more traditional evidence confirming Russian hacking.

Not Making Sense

Several other oddities stand out: first, why would G2 announce himself two days after the DNC reported being hacked, brag he was the hacker, and add that he had given his material to WikiLeaks? WikiLeaks exists for one reason: to give whistleblowers deniability. Normally, people don't give material to WikiLeaks and then brag about it publicly.

Least of all would Russian intelligence do such a thing, assuming – as some allege – that they routinely use WikiLeaks to disseminate hacked data. Why would Russia implicate its proxy? Why, indeed, would Russia not only cast aspersions on Julian Assange's honesty, but also cast doubt on the authenticity of the DNC data, given that intelligence services are known to doctor hacked documents? Why, moreover, would G2 give information to WikiLeaks in the first place, given that he had the ability to curate it and disseminate it on his own, as he showed by distributing "choice" (but actually innocuous) data to journalists?

Then there's the forensic evidence, which shows that (1) G2 put DNC documents into a Russian template; and (2) G2 made those changes on the computer in an East Coast U.S. time zone. Plus, linguistic evidence suggests that G2 showed none of the typical speech idiosyncrasies of a native Russian speaker.

Metadata can be fudged, so it's possible that (1) and (2) don't matter. If that is the case, however, one must explain why G2 would drop deliberate clues indicating that he's Russian – including leaving the name of the founder of the Soviet secret police in one document, along with Cyrillic error messages in another – while also dropping deliberate clues indicating he's an American leaker. Tricky indeed.

Then there's another important piece of forensic evidence: the transfer speed, which corresponds to the speed of a download to a local thumb drive rather than

to an overseas exfiltration. Critics – including a few VIPS dissenters – promptly insisted that the VIPS report was wrong to assume that such speeds could not be attained in an overseas exfiltration in 2016. Signers of the original VIPS report, however, subsequently conducted multiple experiments to prove or disprove that hypothesis; not once did they achieve a transfer speed anywhere close to that indicated in the DNC metadata.

Critics have also argued that the DNC documents transfer speed may refer to a download to a thumb drive *after* the initial hack, yet the download would nevertheless have had to have been done on the East Coast of the U.S., since transfer speed metadata correlate to time stamp data. Why would a hacker exfiltrate data to Romania or Russia, then return to the U.S. to download the material to a thumb drive?

Inconsistencies and Uncertainties

The above inconsistencies, I should add, apply to the DNC data, not the Podesta emails. No one, so far as I know, has cast doubt on the theory that the Podesta emails were phished via APT 28. Still, the same rules of caution apply. As Alperovitch himself testified in June 2016, APT 28 does not necessarily prove Russia involvement, and even if it did, no one has proven that Russians gave the Podesta emails to WikiLeaks. There are many other possibilities.

The Wall Street Journal, for instance, reported that Republican operatives were desperately reaching out to the hacking community to locate Hillary Clinton's 30,000 missing emails. They made contact with several hacking groups including some that claimed to have the emails and even sent samples. The Republicans told the hackers to turn over the emails to WikiLeaks, but – supposedly – offered no payment. It's not inconceivable, however, that the same Republican dirt-diggers – or others – indeed did pay hackers to turn over materials to WikiLeaks. Even if that occurred, however, the hackers might well have been non-state actors who occasionally work with Russian intelligence, but who otherwise work independently (more on that later), and who were not under orders from Putin. Or, they may have been hackers who have no connection to Russia whatsoever.

Regarding Roger Stone's infamous remark that "it will soon be Podesta's time in the barrel," which has been cited as proof that Stone had foreknowledge of WikiLeaks' publication of Podesta's emails, Stone explained on Tuesday that he was referring to his own research on Podesta's consulting work for foreign governments in the context of similar complaints being lodged against Stone's friend and Trump's erstwhile campaign manager Paul Manafort.

Questioning the Investigation

There are worrisome implications here. First, if we are "at war with Russia"; if the hacking was "the crime of the century"; if it's "bigger than Watergate"; why didn't the FBI examine the DNC server, given that James Comey admitted that was "best practice"? Why did he rely on CrowdStrike's analysis, especially given CrowdStrike's strong ties to the Atlantic Council (created solely to support NATO and heavily funded by foreign entities) and CrowdStrike's grossly mistaken charges of Russian hacking in other contexts?

Second, why has there been no comprehensive or coordinated Intelligence Community Assessment or a full-scale National Intelligence Estimate – weighing evidence of Russian culpability against contrary theories – by the U.S. intelligence community, given that it has known about alleged Russian election hacking of both the DNC and state voter databases for well over a year?

What we got in January was a hurried intelligence assessment put together by a "hand-picked" team from three agencies, not a consensus of "17 agencies," as the U.S. press wrongly blared for months. If Russia had committed an "act of war," then surely President Obama would have ordered the fullest assessment of intelligence that the U.S. is capable of producing; yet he didn't.

Third, why would Putin order an enormous campaign against Hillary Clinton, knowing that she would very likely win anyway (and did win the popular vote). Would Putin risk the likelihood of President Hillary Clinton finding out about his shenanigans? What implications would that have for the repeal of the Magnitsky Act, for additional sanctions, for Syria, for Ukraine, for NATO funding, for the possibility of renewed Cold War? Perhaps – as James Comey contends – Putin hated Clinton so much that he was willing to play "Russian roulette." Yet one wonders.

Has the Press Fed Hysteria?

Why, moreover, has the U.S. press barely mentioned the fact that U.S. intelligence services – and the press itself – wrongly accused Russia of the Macron hack? France's head of cyber intelligence, after finding no evidence of Russian hacking, said this: "Why did [NSA Director Michael] Rogers say that, like that, at that time? It really surprised me. It really surprised my European allies. And to be totally frank, when I spoke about it to my NSA counterparts and asked why did he say that, they didn't really know how to reply either."

Think about those words for a moment; they were not meant to be diplomatic. They were unabashedly chastening.

Why, too, has the U.S. press barely mentioned the fact that German intelligence, after a months-long investigation, found no Russian meddling in its recent

election (and moreover, found that the supposed Russian hack of the Bundestag in 2015 was likely a leak after all), despite U.S. intelligence agencies' insistence that Germany was Russia's next target?

Why do we not hear that Britain found no evidence of Russian efforts to influence Brexit, despite allegations to that effect? Why has the U.S. press wrongly reported a Russian hack of a Vermont utility; a Russian hack of an Illinois water pump; a Russian hack of north Texas voter rolls; a Russian hack of Qatari news media? Add to those examples the latest round of debunkings: there was no Russian attempt to hack Wisconsin voter rolls, nor any Russian attempt to hack California's. Despite all the debunked stories, the U.S. press eagerly reports new Russia-done-it stories every time some anonymous source breathes a leak.

Here's a test you can do at home: Type "Germany Russia hacking" into your search engine and see what comes up. Then type "Brexit Russia hacking." Then try "France Russia hacking." You'll get an absolute barrage of stories – hundreds of links – that melodramatically attest to Russian hacking and/or meddling in all three situations, but you'll struggle mightily to find stories refuting those charges.

One can readily see why some curious soul sitting at home who takes it upon himself to do a little internet research would come away utterly convinced of Russian perfidy. Google here becomes an instrument not of truth-finding, but of algorithmic fake news.

Why, too, did former Assistant Secretary of Department of Homeland Security for Cybersecurity, Andy Ozment, insist in September 2016 that hacking attempts on voter rolls were not of Russian origin, but rather were criminal attempts to steal identification data for sale on the dark net? Why did DHS say as late as October that they lacked evidence to blame Russians? Were they simply protecting the nation against mass hysteria that could cast doubt on the presidential vote?

And yet the basic evidence pattern for attributing the attempted hacks to Russia (or anyone else) hasn't changed; it's not as if some new damning piece of evidence emerged after September. Even Reality Winner's leaked NSA document from June 2017 notes uncertainty about the identity of the hackers. If one looks at the leaked chart showing details of the flow of hacked information, one notes that the final arrow on the left pointing to Russian intelligence (GRU) is marked "probably." Click here and scroll down to see the blown-up chart.

Incidentally, if you think the case of Reality Winner is a bit suspect – i.e., a cleverish ruse to undermine *The Intercept* (publisher of the "Winner leak") and puff up the Russia hysteria – you might want to check out this story. I withhold

judgment, personally.

What I Am Arguing

Am I implicating Obama in a conspiracy? No way. Am I suggesting that G2 was a DNC actor seeking to blame Russia for a damaging insider leak to Assange? Not necessarily, but not "not necessarily," either. There is reason for suspicion at least.

Am I suggesting that U.S. intelligence agencies are lying in order to protect massive U.S. funding for NATO and to force Russia to loosen its ties to Iran and Syria, not to mention lay off Ukraine? *No, I am not suggesting any deliberate lie, though yes, wishes can father thoughts*. Certainly Trump's campaign talk of defunding NATO, friendship with Russia, and leaving Syria to Assad ruffled feathers in the intelligence community.

I am far from being a cyber-security expert, let alone knowledgeable about IT, so I write all this in modesty. And yet I find myself agreeing with experts who say that APT associations are not grounds for "high confidence" intelligence assessments, and that the American public deserves to see strong evidence not just of hacking – but of actual *Russian* hacking – given the magnitude of the issue.

I also find myself agreeing with cyber-security experts who tell us that U.S. intelligence agencies – as well as private cyber-security firms like CrowdStrike – tend to build the evidence around hypotheses, rather than letting the evidence lead to its own conclusions.

I don't think there's a conspiracy; I think there's bias, groupthink, and boss-pleasing – in both the press and the intelligence agencies – just as there was in the Iraq WMD fiasco.

As Folden points out, there are numerous international crime organizations (an $800 billion industry last year) that might well stand behind APT 28/29. Given the sloppiness of the DNC and Podesta hacks (assuming they were hacks), what's probable is that Russia isn't doing the work directly, but might be paying a third party that sells its wares to bidders. Or, perhaps Russia isn't involved.

As Folden notes, numerous states and international crime organizations have strong economic and/or strategic interests in both internal U.S. campaign information and in U.S. elections outcomes. The same observation goes for allegations of hacked voter databases. Any number of entities have both the wherewithal to employ APT 28/29 and an economic interest in harvesting voter identification data.

We should pause to note here that almost all the state database attacks were just that – attacks – not breaches. Unsuccessful attacks cannot be traced to APT groups, only to IP addresses, which are highly unreliable evidence. What few confirmed breaches there were (e.g., Illinois), moreover, did not change election results, and – as with the alleged DNC hack – can only be traced to APTs, not to actual hackers.

Here's an aside just for fun: why would Russian hackers imagine for a second they could turn Illinois into a Trump state? Clinton won that state by a million votes. Sure, one can understand why Russians might want to meddle with voter roles in a swing state, but Illinois? More likely the hackers were criminals seeking voter identification info, which is precisely why they downloaded 90,000 registration records. The FBI absurdly claimed that Russians needed all those records to figure out precisely how Illinois voter registration works, thus to improve their dirty work. Really? They needed 90,000 records for that?

Pressuring Facebook

Of course, if the voter database attacks turn out to be no-big-deal, the press still will find some new way to exploit the Russia hysteria. The Washington Post and the New York Times – along with the House and Senate Intelligence Committees – are now investigating Russian attempts to use Facebook ads and posts to help Trump win the election. Facebook – thanks to subpoenas from Special Prosecutor Robert Mueller and pressure from congressional Democrats – has turned up $100,000 of suspicious ad buys from phony accounts.

Think of that for a moment: Russians (supposedly) mustered fully $100,000 for ads in a presidential campaign that cost $2.4 billion. Talk about bang for your buck! The current allegation is that over the past three years, a few hundred Russian trolls armed with $100,000 and 470 Facebook accounts (compared to Facebook's $27 billion in annual revenue and 2 billion monthly users) deployed issues ads (not primarily attack ads against specific candidates) to out-brigade millions of ordinary Americans who posted campaign pieces on Facebook every day, not to mention Clinton's public relations army.

Poor David Brock paid a million dollars for his own pro-Clinton troll brigade, but they were children compared to these nefarious Russians. It's a feat right up there with Xenophon's *Anabasis* … a tiny force of foreigners, slashing their way through the Persian hordes! Someone get an epic poet!

Of course Sen. Mark Warner, a hawkish vice-chair of the Senate Intelligence Committee, informs us that the $100,000 is just the "tip of the iceberg." Who knows, maybe the Russians spent $200,000.

Even if these propaganda charges turn out to be 100 percent true – and even if the Russians were clever enough to target voters in the Upper Midwest – it is highly unlikely that they had more influence on the election than a host of other factors, ranging from Clinton's bad campaign decisions to emailgate to anti-establishment fervor to Trump's 4-Chan volunteers (did he really need several hundred Russians? Surely he had plenty of home-grown trolls).

Silencing Dissent

So, maybe the Russians did play some small role on Facebook – though I suspect this suspicion, too, will be challenged – but should we therefore conclude that we're at war, as Morgan Freeman declares? Should we demand that Facebook and Google continue to rework algorithms to shut down posts or ads deemed pro-Russian? Doesn't that remind anyone of the anti-German hysteria – and censorship – during World War I?

Should we demand, moreover, that the tiny Russian-owned media outlet RT register as a foreign agent – as the Atlantic Council has insisted, and as the Justice Department is now demanding – but not require the same of the BBC and CBC, which are financed by the British and Canadian governments respectively?

What about the Atlantic Council itself, which, receives much of its funding from foreign nations that seek to strengthen NATO? Should the Atlantic Council be required to register as a foreign agent? Does anyone seriously think the Atlantic Council doesn't propagandize for NATO and for hawkish policies more generally? Or what about the hawkish Brookings Institution, or a host of other think tanks that welcome money from foreign powers?

The unspoken assumption here is that only Russia propagandizes; no other nation is so shifty. Surely Saudi Arabia wouldn't do such a thing, nor Israel, nor Ukraine, nor countless other nations that seek to influence American policy. After all, they have their paid lobbyists and press buddies working for them every day; they don't need several hundred trolls.

Let's be honest, we live in a world in which foreign powers seek to influence American public opinion, just as we seek to influence public opinion in other nations. Which brings to mind a bill that President Obama signed in December, at the outset of the Russia hysteria: "The Countering Disinformation and Propaganda Act," which created the State Department's "Global Engagement Center," which seeks to "recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United Sates national security interests."

The act also offers grants to organizations (think news agencies and research

groups) that promise to “counter efforts by foreign entities to use disinformation, misinformation, and propaganda to influence the policies and social and political stability” of the U.S. and allied nations. (Shout out to Rob Reiner; did you apply for one of those grants? Might be a good opportunity for you.)

Does no one see a problem with this? What exactly is foreign propaganda? Is it RT’s occasional charges that the U.S. press treats Trump unfairly? Is it RT’s penchant for left-wing, anti-establishment commentary, e.g., Chris Hedges, Thom Hartmann, and Lee Camp? Our intelligence elites certainly think so, judging from the seven pages they dedicated to RT’s supposed rascally programming in the January intelligence assessment.

And what exactly will it mean to “counter … foreign … disinformation, misinformation, and propaganda”? Will it mean countering any news or commentary deemed anti-NATO or pro-Russian? Any news or commentary deemed pro-Iranian? How exactly will our government define “foreign propaganda”? How, moreover, will it define “national security”? What lengths will it take to deny the American public — not to mention foreigners — access to legitimate opinions?

Alien and Sedition Acts

Perhaps the real analogue here isn’t World War I after all, but the Alien and Sedition Acts of 1798. Of course it wasn’t Russians that President John Adams worried about; it was hot-blooded Irish radicals and French émigrés with their revolutionary idealism, which was ostensibly corrupting the nation. Ordinary Americans were suddenly refusing to vote for their Federalist political betters, and those betters determined to make them pay. Far better to jail Jeffersonian editors and drive out foreigners than to let them endanger America’s “national security.”

We are forsooth reliving the age of Hamilton, I fear, when political elites dance to Wall Street theatricals about anti-democrats while feeling virtuous about opposing “deplorables.” Just don’t expect them to care about free speech. Thanks to our government’s push against so-called fake news, both Google and Facebook have already altered algorithms to such an extent that they have pushed down readership for one old and revered progressive venue, AlterNet, by fully 40 percent (other progressive venues have seen similar declines), thus starving them for ad revenue. Meanwhile neoconservative researchers are trumpeting inch-deep investigations into supposed Russian propagandizing that — thanks to vast funding — may get churned out for years to come.

Let’s not kid ourselves; this project isn’t about shutting down “fake news.” From the moment the Washington Post ran its infamous PropOrNot story in November

2016, the message has been clear: the real threat isn't Russians, it's any media outlet that fuels anti-establishment politics.

The Universality of Hacking

All that said, it is still very possible that CrowdStrike and the intelligence community are correct to attribute at least some DNC exfiltration of data to Russians or to loose-leashed teams working as subcontractors, or, alternatively, criminal organizations that sometimes answer to Russia. The one thing that the skeptics (of whom I am obviously one) have not answered is why the CrowdStrike investigation found uniquely modified X-TUNNEL source code in DNC servers, which would seem to have been created for this particular hack.

Since I don't have years to become a cyber-security expert, I'll leave the technical experts to further argue that question. However, I am left to wonder whether X-TUNNEL indeed betrays a Russian hack of at least some DNC emails, but that another party altogether – a leaker – was nevertheless responsible for handing the full complement of DNC documents to Wikileaks.

None of the skeptics are claiming that the Russians for certain didn't hack the DNC (which wouldn't be that surprising, really; we probably hack their political entities, too). The skeptics are only claiming that G2 was an insider who downloaded documents onto a thumb drive. Both claims can be true.

I'll add – just to be clear – that I am quite certain that the U.S. intelligence community is correct that the Russian government is engaged in broad hacking attempts aimed at targets all over the world, many of them associated with APT 28/29. But that doesn't mean they carried out the particular hacks at issue here (or, at least, it doesn't mean that Russian state actors were behind the WikiLeaks releases, or the attacks on state databases).

And it certainly doesn't mean – contrary to what over-wrought bloggers claim – that Russians changed 2016 vote tallies. The answer isn't to shout "war" and create hysteria; the answer is to secure U.S. infrastructure.

I'll also add that even "high confidence" that Russia hacked the DNC, Podesta, and/or state databases is insufficient grounds for aggressive policy – e.g., harsh sanctions and diplomatic ejections, not to mention military action – let alone grounds for announcing "we are at war." Suppose for the sake of argument that "high confidence" is 75 percent probability. Would we convict an accused murderer on 75 percent probability?

If we did that – and if the accused were then put to death – we would be knowingly killing 25 innocents out of every 100 we adjudge. The same logic should apply to foreign policy. We should not be taking punitive measures unless

we can assess culpability with greater certitude, else we risk harming millions of people who had no role in the original crime.

Where We Stand

It seems to me that we are in uncharted waters. Not everyone can be a cyber-security expert; we must trust those who are. And yet in doing so, we put enormous powers into the hands of unelected technocrats with their own biases and agendas. As others have noted, moreover, the cyber-war community is at odds with the cyber-security community.

On the one hand, intelligence operatives are constantly developing new tools to exploit cyber vulnerabilities of other nations and criminal actors. On the other hand, cyber-security people (e.g., DHS) seek to patch those same vulnerabilities to protect U.S. infrastructure. The problem is that the people who know how to exploit the vulnerabilities don't want to report those vulnerabilities because it means years of work down the drain. Why make your tools obsolete?

We need to resolve these contradictions in favor of security, not cyberwar.

I cannot say this loudly enough. This whole episode isn't just about Hillary Clinton losing the election, or Russian hacking of the DNC, or Deep State bias and boss-pleasing. The upshot is that we are entering a cyber-arms race that is going to become ever more byzantine, hidden, and dangerous to democracy, not just because elections can be stolen, but because in guarding against that, we are handing over power to unelected technocrats and shutting down dissenting speech. We are entering a new era; this won't be the last time that hacking enters political discourse.

We might already be in the midst of a cyber Cold War, though the American public has no idea — flat zero — what sort of offensive gamesmanship our own cyber-warriors are engaging in. (One interesting theory: The Russians deliberately implicated themselves in the DNC hack in order to send a warning to U.S. cyber-warriors: we can play dirty, too).

Presumably not even our cyber-security experts at the DHS and FBI know what the CIA and NSA's cyber-warriors are up to. Thus Russian hacking becomes "Pearl Harbor" rather than an unsurprising reciprocal response. Both the State Department and the CIA, after all, have been in the foreign propaganda business for decades; the American public, however, has not the vaguest idea of what they do.

We might also be on the brink of something else nightmarish: an international cyber-war with multiple parties participating — attacking one another while no-one-knows-who-did-what.

The intelligence community’s whispered “trust us, we’re the experts” simply isn’t good enough. If we don’t demand hard evidence, then we’re following the same path we took in 1898, 1915, 1950, 1964, and 2003. Let’s not go there.

Daniel Herman is Professor of History at Central Washington University. He specializes in American cultural history and the American West.