

## **Putin's Attack on the U.S. Is Our Pearl Harbor**

*Make no mistake: Hacking the 2016 election was an act of war. It's time we responded accordingly.*

*By Mark Hertling and Molly K. Mckew*

*July 16, 2018*

On December 7, 1941, the Imperial Japanese Navy launched a surprise conventional attack against the U.S. Pacific Fleet moored at Pearl Harbor. The Japanese operation was part of a larger strategy: cripple the United States — in capability, naval manpower and mentality — so that we would be prevented from interfering as Japan continued military operations throughout Southeast Asia. Almost 3,500 Americans were killed or wounded; eight U.S. battleships were damaged and four were sunk; and more than 300 aircraft were damaged or destroyed. To this day, the wreckage of the USS Arizona is a monument to loss of life and totality of destruction. The attack happened without a declaration of war and without explicit warning, and President Franklin D. Roosevelt responded the next day.

On September 11, 2001, the Islamist terrorist group Al Qaeda conducted four coordinated unconventional attacks against our nation. Its leader, Osama bin Laden, chose targets linked to the U.S. government and American economic power as part of his larger strategy: bring “holy war” to the American homeland for what bin Laden alleged were aggressions against Muslims in the Middle East. Nearly 3,000 people were killed and more than 6,000 injured in attacks that caused at least \$10 billion in damages. The memorials in Manhattan, at the Pentagon, and in Shanksville, Pennsylvania, remind us of the loss and of the hollowness we felt watching the Twin Towers fall. The attack happened without a declaration of war and without explicit warning, and President George W. Bush responded the next day.

Story Continued Below

Many think of Pearl Harbor and September 11th in terms of the overwhelming devastation the attacks caused rather than the critical transformation they sparked. Yet both attacks were earth-shaking events that forced a forward leap in our strategic thinking about the defense of the American homeland and the projection of American power. As the smoke still rose over the wreckage of our fleet, and as the dust settled over Manhattan and the Pentagon, we went to war. We acted because Japan and Al Qaeda had underestimated us. We went to war knowing we must fight back, but uncertain how we would win. We acted because we had renewed political will, a newfound clarity toward an enemy and its objectives, and because we understood the cost of failing to rise to the challenge. We were tested in ways we never expected, and the cost was unthinkably high, but we acted because we had to.

In 2016, our country was targeted by an attack that had different operational objectives and a different overarching strategy, but its aim was every bit as much to devastate the American homeland as Pearl Harbor or 9/11. The destruction may not send pillars of smoke into the sky or come with an 11-digit price tag, and there's no body count or casualty statistics—but the damage

done has ravaged our institutions and shaken our belief in our immovability. But two years on, we still haven't put any boats or men in the proverbial water. We still have not yet acted—just today, President Donald Trump, a beneficiary of this attack, exonerated the man who ordered it: Russian strongman Vladimir Putin.

Piece by piece, name by name, one operational detail after the next, special counsel Robert Mueller's investigation has documented that the Russian attack on the American homeland and the American people was every inch as organized, expansive, penetrating and daring as that Japanese run on our fleet or bin Laden's plan to use civilian airliners as weapons. The Kremlin targeted no remote outpost or iconic landmark, but rather aimed at the very heart of what we are as a nation. The attacks target our processes of government, our democratic institutions and our trust in our values. The further this assault on our independence recedes into the past, the additional suggestions by anyone that it didn't happen, the more deeply entrenched the adversary becomes in our terrain.

\*\*\*

Russia's cyber warfare capabilities are just one element of an arsenal of hybrid, asymmetric means the Kremlin has focused on expanding since its cyberattacks against Estonia in 2007 and its invasion of Georgia in 2008. In 2013, the Russian chief of the general staff General Valery Gerasimov outlined this concept of warfare, emphasizing that “the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.” Putin polished what they had learned in earlier operations and put these on full display a year later, as Russia seized and then annexed Crimea, and then launched an invasion of eastern Ukraine fronted by local proxies backed by the Russian military.

While it has become quite popular to debate whether or not what is referred to as “[the Gerasimov Doctrine](#)” was intended to be military or security doctrine or not, the way of war Gerasimov discussed is, in fact, how the Russians now fight. Testifying before the House Armed Services Committee in March 2018, General Mike Scaparrotti, head of U.S. European Command, was asked about Gerasimov, and [he responded](#) succinctly and with candor: “Russia has a doctrine that ... sees these activities below the level of conflict as part of the full spectrum, with the intent that if they can undermine a target country using these means ... never having to use military force, that's their objective.”

Story Continued Below

Gerasimov has since [updated](#) his thinking on the uses of hybrid warfare to erode the will of the enemy, saying that “spiritual resources—the nation's cohesion and desire to confront the aggressor at all cost,” were one of the most important determiners of victory or defeat in these new shadow wars. Confusing the enemy has always been a doctrinal tenet of Russian war-fighting, so this new approach just replaces the old “Maskirovka” (deception) as a primary objective. The more you read about how Russia has tested and adapted these tactics in its near-abroad, the harder it is to deny that the Kremlin's attack on America is no outlier but rather one

more entry in an ongoing, evolving playbook that is yielding more success than anyone wants to admit.

So where are the air-raid sirens and the calls to arms from those who vow to protect and defend our Constitution against all enemies, foreign and domestic? Last week, as Deputy Attorney General Rod Rosenstein released Mueller's latest indictment of the 12 Russian intelligence officers, Director of National Intelligence Dan Coats was [also testifying](#) on Capitol Hill. "The warning lights are blinking red," he said. The risk of a "crippling cyberattack on our critical infrastructure" by a foreign adversary was increasing, he added. Coats named Russia as the most aggressive threat, saying: "The digital infrastructure that serves this country is literally under attack."

Not in 2016. Now. It's happening all over again.

\*\*\*

The Mueller indictments have pulled back the curtain on enough of the details that we should see how much we still don't know—but need to. They show the extent to which Russia has learned to "hack" our systems using these hybrid/asymmetric means with an emerging and polished cyber capability at its core. They are, in short, working us. Using our social media and free press to manipulate opinion; using willing collaborators to act on their behalf; using a degraded trust in government institutions and the free press to sow further confusion and distrust. They are winning using covert, deceptive means, and it's all completely out in the open, while remaining totally invisible.

The earlier indictment of the Internet Research Agency (IRA) explained the extent to which these government proxies had gone to set up false identities—using forged and stolen IDs, fraudulent bank accounts, and other fake identify documents—in order to create networks of interlinked accounts pretending to be Americans. These accounts were meant to embed within and learn to emulate the discourse of target communities, expand their following and influence, and then amplify certain tendencies. This included setting up completely fictitious local news portals, group pages and other content purveyors. They chose identities as veterans and their wives, wholesome grannies, devout evangelicals and, above all, patriots. All of this was a process begun years in advance of the 2016 elections, based on the exact same tactics of psychological control the Kremlin had tested and refined against its own population.

The IRA was a close proxy for these Kremlin activities—more than anything, a way to recruit civilians to act as hostile agents. But the actions described in the new indictment, for the Democratic National Committee hacks, were conducted by real units from within the Russian military architecture. They aren't civilians, and they aren't deniable proxies—though Putin did try just that in his news conference with Trump, calling them "alleged" intelligence officers. Even identifying them by name and rank demonstrates our potential for fighting back.

Story Continued Below

A dozen seasoned Russian military intelligence officers conducted hacking and infiltration operations against U.S. political parties and state elections infrastructure, including voter rolls and registration systems. They established false identities, covered their trail and used cryptocurrency to hide the origin of their operations. These units created false personas that successfully masqueraded as journalists, other hackers, and other influencers, and they built out the infrastructure of a fictitious “hacktivist” group to release materials stolen from the DNC. The indictment also explains that these GRU cells were generating their own revenue to conduct these operations, both by mining bitcoin and by diverting donations from the Democratic Party via a spoofed webpage. That is true evil genius.

Proxy or official, the Russian operatives were able to create “American” personas that interacted freely with American voters, journalists, activists—and campaign officials. They also seemed to have considerable knowledge of how to target and parse American audiences. All of this was subversive and deceptive—but done right out in the open. It was targeting American society and individuals in a way that bypassed the existing system of protections, including those inherent in our own decision-making.

Why fight this way, using intelligence operations, proxies, information operations, compatriots? This asymmetric way of war exposes Russia’s comparable weakness. Their preferred use of proxies has the unique benefit of lowering the accountability for their actions while raising the appetite for risk-taking. There’s a lot of testing, and a lot of failure—but no one cares as long as the testing continues to generate new lines of attack. Their tactics are asymmetric and guerrilla in nature—which through history has always been how a less powerful adversary fights a more powerful force. This way of war is flexible, adaptive, cheap, decentralized, and—most important—deniable.

But we must stop denying how the Kremlin acts and what it says. As Coats testified, the U.S. intelligence community continues to see “aggressive attempts [by Russia] ... intended to exacerbate social political divisions” in the U.S., including by the establishment of new accounts “masquerading as Americans.”

\*\*\*

Mueller’s indictments have given incredible visibility into an ongoing Russian intelligence operation against the United States—the full scale of which, when exposed fully, will likely make it the most successful, and perhaps the most important, in history.

But it’s been years—years!—and despite all this detail held by our intelligence community and known by many in our military and national security apparatus who study these things, nothing has changed. Members of the House and Senate have been briefed, but remain deadlocked in partisan bickering. Some in the House have spent more time investigating the investigators than they have in trying to hold Russia accountable. Trump’s suggestion to accept Russian investigators into this process adds a new layer to the sideshow. When right of the boom feels like left of the boom, it’s easy to miss the fact that what the Kremlin did—is doing—was, and is, an act of war.

## Story Continued Below

Why would Putin take such a dangerous risk? Because it is his only potential means of survival. Everyday this invisible, seemingly impossible attack becomes a little more known and a little more visible—but this exposure absent any sense of clarity, leadership, public communication, or plan to counter it instills fear and panic as much as it elicits outrage. And it destroys trust in the institutions of government, a critical element of any democracy.

What Clausewitz called the center of gravity is no longer the physical environment of the opponent's capital city, but it could be the elements of the nation's institutions. And we won't be able to count our daily dead or counter the enemy's advances by "fielding" new battlefield equipment. But in the information age, the intelligence and leadership of our fighters—those in uniform and those in civilian clothes—becomes paramount. The old formula of resistance to an enemy is accomplished by either affecting his will to fight or his means of fighting. So far, we have neither deterred Russian behavior nor its means of attack. Today, we may even have given them additional license to believe they can continue.

As Gerasimov himself noted: Fighting hybrid attacks requires an informed, prepared, mobilized population with the will to fight and to understand. Our friends [closer to the Russian border](#) understand this, as well. Gaining clarity is required. Facts, not narratives, are essential. We're now so deep in the churn, all of this will be quite challenging—for military and civilians alike. The president of the United States stood next to the foreign adversary responsible for ordering an attack on the American homeland and American people, and he dismissed the whole thing and said nothing happened. This is disarming the American public in what should be the most important fight in our history.

When Japan attacked, and when Al Qaeda attacked, they wanted to be known as the enemy of America, and they wanted it to be known that they had brought the fight to us. Revanchist Russia has a new formula: giving their domestic audience a clear enemy, but denying one to us by muddling our thinking, our judgment and our leadership.

So far, this attack has been met by relative silence at the top, by at least two consecutive presidents who have failed to find the right formula for dealing with a calculating foe like Putin. This silence propagates fear, division, unrest and diminishing trust—and it is every bit as crippling as Putin could have hoped.

Trump may think of the European Union as America's primary foe, but the Kremlin identifies the United States as its primary adversary. It is using asymmetric means to attack our society and our alliances, and to attack the citizens of the West. More details of this are being exposed daily, and our intelligence, military and national security communities are getting louder and louder in signaling their alarm. For now, our civilian leadership is shrugging this off, even acquiescing, which leaves every individual to defend themselves against the assault of information levied by a foreign attacker. This should not be the way we defend our people and our homeland.