# America's Cyber-Reckoning: How to Fix a Failing Strategy

**Published in:** Foreign Affairs, 2022, Gale General OneFile

A decade ago, the conventional wisdom held that the world was on the cusp of a new era of cyberconflict in which catastrophic computer-based attacks would wreak havoc on the physical world. News media warned of doomsday scenarios; officials in Washington publicly fretted about a "cyber-Pearl Harbor" that would take lives and destroy critical infrastructure. The most dire predictions, however, did not come to pass. The United States has not been struck by devastating cyberattacks with physical effects; it seems that even if U.S. adversaries wanted to carry out such assaults, traditional forms of deterrence would prevent them from acting.

Behind those mistaken warnings lay an assumption that the only alternative to cyberpeace must be cyberwar. But in the years since, it has become clear that like all realms of conflict, the domain of cyberspace is shaped not by a binary between war and peace but by a spectrum between those two poles--and most cyberattacks fall somewhere in that murky space. The obvious upside of this outcome is that the worst fears of death and destruction have not been realized. There is a downside, however: the complex nature of cyberconflict has made it more difficult for the United States to craft an effective cyberstrategy. And even if lives have not been lost and infrastructure has mostly been spared, it is hardly the case that cyberattacks have been harmless. U.S. adversaries have honed their cyberskills to inflict damage on U.S. national security, the American economy, and, most worrisome of all, American democracy. Meanwhile, Washington has struggled to move past its initial perception of the problem, clinging to outmoded ideas that have limited its responses. The United States has also demonstrated an unwillingness to consistently confront its adversaries in the cyber-realm and has suffered from serious self-inflicted wounds that have left it in a poor position to advance its national interests in cyberspace.

To do better, the United States must focus on the most pernicious threats of all: cyberattacks aimed at weakening societal trust, the underpinnings of democracy, and the functioning of a globalized economy. The Biden administration seems to recognize the need for a new approach. But to make significant progress, it will need to reform the country's cyberstrategy, starting with its most fundamental aspect: the way Washington understands the problem.

## SHOTS FIRED

The first known cyberattack occurred in 1988, when Robert Morris, a graduate student in computer science, released a small piece of software--eventually dubbed "the Morris worm"--that created outages across the still nascent Internet. During the two decades that followed, cybersecurity remained the concern mostly of geeky hackers and shadowy intelligence operatives. That all changed in 2010 with the Stuxnet operation, a devastatingly effective cyberattack on centrifuges that Iran used to enrich uranium. U.S. leaders soon began sounding the alarm about their own country's vulnerability. As early as 2009, President Barack Obama had warned of cyberattacks that could plunge "entire cities into darkness." Three years later, while briefing the Senate Armed Services Committee, Keith Alexander, the director of the National Security Agency (NSA), said it was only a matter of time before cyberattacks destroyed critical infrastructure. Around the same time, Senator Jay Rockefeller, Democrat of West Virginia, claimed that "the prospect of mass casualties" made cyberattacks "as dangerous as terrorism."

These warnings seemed prescient when, in 2012, Iranian operatives targeted the oil company Saudi Aramco with malware, wiping out data on 30,000 computers. Two weeks later, Iran targeted the Qatari company RasGas, one of the largest natural gas producers in the world, in a similar strike. These cyberattacks were by far the most destructive in history and marked the first time a government had employed an offensive operation in cyberspace against a U.S. partner. The strikes rattled world energy markets. To signal support for the Saudis, Washington deployed a team of Pentagon cybersecurity experts to Riyadh.

Two months after the Iranian attacks, U.S. Secretary of Defense Leon Panetta gave a high-profile speech in which he warned of other countries or terrorists using cyberweapons to derail passenger trains or freight trains loaded with lethal chemicals, contaminate water supplies in major cities, shut down the power grid, or disable communication networks and military hardware. Americans, Panetta declared, needed to prepare for a kind of "cyber-Pearl Harbor: an attack that would cause physical destruction and the loss of life [and would] paralyze and shock the nation and create a new, profound sense of vulnerability." Panetta also attempted to outline the U.S. strategy for deterrence in cyberspace, arguing that "improved defenses alone" would prove insufficient. When the U.S. national security services detected an imminent cyberattack of significant consequences, he said, they would need "the option to take action." And so, he explained, the military had developed "the capability to

conduct effective [offensive cyber-]operations to counter threats to [U.S.] national interests in cyberspace."

From 2012 to 2014, the National Security Council staff held dozens of senior-level meetings to draft a complicated set of policies--known as Presidential Policy Directive 20--that established guidelines for when the United States could launch offensive cyber-operations to deter future attacks. At the Pentagon, the Joint Staff devoted several straight months to developing strict protocols for when the secretary of defense could approve an "emergency cyber action"--a targeted cyberattack to neutralize and counter an adversarial attack on the homeland.

That planning was put to the test in 2014, when North Korean operatives conducted the first-ever destructive cyberattack on U.S. soil, exfiltrating heaps of confidential information from servers belonging to Sony Pictures, which was planning to release a film that mocked the North Korean dictator Kim Jong Un. The hackers spread the information, including embarrassing emails, throughout the Internet; knocked out Sony's digital networks; and threatened to carry out further "terrorist attacks" in cyberspace. For weeks, the U.S. intelligence community feared that North Korean operatives had prepositioned cybermunitions inside American critical infrastructure and would soon detonate them.

That did not happen, and in many ways, the Obama administration's response to the attack was sophisticated and effective. The president directly called out the North Koreans for the hack, and the administration immediately levied economic sanctions, the first ever imposed in response to a cyberattack. The combination of public attribution and sanctions seemed to deter Pyongyang from conducting additional attacks. But the most important takeaway was that even after two years of planning and development, the U.S. military did not have the cyber-response capabilities Panetta had promised.

## LESSONS NOT LEARNED

Part of the problem was that the Obama administration took an old-school approach to cyberspace that was stuck, in some ways, in an archaic, Cold War-style paradigm according to which cyber-operations could quickly escalate into a full-blown war. This perspective carried over into the Pentagon's decisions when it came to building a force structure for the cyber-domain: in 2009, Secretary of Defense Robert Gates established U.S. Cyber Command, which is subordinate to the four-star commander of U.S. Strategic Command, the notoriously slo

moving organization that oversees the country's nuclear weapons. This structure suggested that the administration saw conflict in the cyber-domain as analogous to nuclear conflict or military activities in outer space, rather than as a dynamic sphere of operations more akin to counterterrorism or the world of special forces. Gates also determined that the new command would not carry out so-called information operations designed to influence the perceptions, thoughts, or beliefs of foreign actors in ways that would serve U.S. strategy.

These decisions delighted Washington's Russian adversaries. During a 2013 meeting between senior U.S. defense officials and their Russian counterparts, a high-ranking officer in the Russian military, General Nikolai Makarov, taunted the Americans. "One uses information to destroy nations, not networks," he said. "That's why we're happy that you Americans are so stupid as to build an entire Cyber Command that doesn't have a mission of information warfare!" At the time, defense leaders didn't consider that the United States might be one of the nations that Makarov had in mind. After Russian interference in the U.S. presidential election three years later, his remarks took on an even more sinister cast.

Cyber Command's structure and mission had serious consequences in the years that followed, especially in the U.S. campaign against the Islamic State (also known as ISIS). The Pentagon had structured the new organization and designed its capabilities based on existing war plans that focused on rival countries; as a result, Cyber Command had very few resources dedicated to counterterrorism. During the first two years of the conflict, poor leadership at the top, a lack of operational capability, and an unwillingness to risk intelligence sources and methods resulted in Cyber Command's failure to disrupt ISIS operations. In 2015, this debacle led a top military commander of the U.S. effort against ISIS to declare, "I only wish that Cyber Command could inflict as much pain on ISIS as DISA does on me!" (DISA, the Defense Information Systems Agency, provides tech support to the U.S. military.)

Beneath these flawed decisions on organization and mission lay a deeper failure to learn the lessons of the 2014 North Korean hack of Sony: cyberattacks require an immediate response, public attribution, and diplomatic confrontation. In the wake of that attack, China and Russia each carried out an increasingly bold and insidious wave of cyberattacks. In the spring of 2014, for example, a group of operatives linked to the Kremlin attempted to derail the Ukrainian presidential election with a potent combination of hacking, disinformation, and denial-of-service attacks. Ukrainian cybersecurity experts narrowly prevented the assault

from succeeding. But the White House was unwilling to confront Russia or provide Ukraine with any type of support in the cyber-domain.

Then, in December 2015, Russian-backed operatives attacked Ukraine's electric grid, leaving parts of the country without power for days in the midst of winter weather. Once again, the Obama administration stood by without responding. This likely contributed to Russian President Vladimir Putin's calculus that he could conduct cyber- and information operations to interfere with the U.S. presidential election in 2016 without fear of reprisal. He was right: the Obama administration did little to push back against Russian meddling during the summer and fall of 2016--until it became a crisis and hit the front page of The New York Times.

The Obama White House proved similarly unwilling to confront China over its transgressions in cyberspace. This was of a piece with the administration's emphasis on building stable economic relations with Beijing, which also overrode concerns about Chinese human rights abuses and China's aggressive military moves in the South China Sea. Even before North Korea's Sony attack, China had taken advantage of this passivity to steal American intellectual property on a massive scale between 2008 and 2013, to the tune of between $200 billion and $600 billion of value per year. The strategic impact of this theft is difficult to prove empirically, but it almost certainly gave a huge lift to Beijing's Made in China 2025 initiative, which seeks to advance China's domestic production of artificial intelligence systems, telecommunications, clean energy technology, aerospace products, and biotechnology.

Later, in 2014 and 2015, Chinese intelligence operatives penetrated networks belonging to the U.S. Office of Personnel Management and exfiltrated the personnel files of around two million former or retired federal employees and more than two million current ones, including information on nearly all the background investigations of Americans who held security clearances at the top-secret level. Prodded by intense congressional pressure and media scrutiny, Obama confronted Chinese President Xi Jinping during a September 2015 meeting at the White House. Obama offered to not publicly attribute the OPM hack to China, and in exchange, Xi agreed to stop intelligence operations against U.S. firms and to establish a diplomatic working group to discuss issues related to cyberspace. Immediately following the summit, the volume of Chinese intellectual property theft plummeted, and Beijing and Washington held a round of talks about cybertheft. This positive outcome clearly

demonstrated the importance of challenging China--but it also served as a reminder that the administration had waited far too long to take action.

U.S. President Donald Trump took office in 2017 with a more assertive, combative tone than that of his predecessor. His administration's approach to U.S. rivals was inconsistent and unpredictable, but in 2018, the White House approved the elevation of Cyber Command to full combatant command status, which freed the organization from the constraints of working through U.S. Strategic Command. Later that year, National Security Adviser John Bolton announced that the administration would take a more aggressive approach to offensive cyber-operations by permitting the military, with the approval of the secretary of defense, to conduct operations below the legal threshold of an "armed attack." This policy, known as National Security Presidential Memorandum 13, set the foundation for cyber-operations, such as denial-of-service attacks and information operations, targeting the Internet Research Agency, a Russian "troll farm," and may have prevented the group from interfering in the 2018 congressional midterm elections. These moves demonstrated the effectiveness of low-level, proactive cyber-tactics and drove home the idea that when it comes to cyberspace, deterrence need not take place on the level of grand strategy: low-tech, low-risk, targeted operations can do the trick.

The Trump administration's approach to Russia's cyber-campaigns was by no means an unqualified success, however, owing to the behavior of the president himself. Trump's bizarre genuflection toward Putin undermined any coherent strategy against Russia, and Trump's unwillingness to stand up for U.S. interests vis-à-vis Russia posed a genuine threat to American democracy. From his public invitation to the Russians to hack his 2016 opponent, Hillary Clinton, to his endorsement of Putin's nonsensical proposal to create a joint U.S.-Russian "impenetrable cybersecurity unit," Trump repeatedly undermined the efforts of his own country's law enforcement agencies, intelligence organizations, and military to protect U.S. national security.

## OWN GOALS

But Trump is hardly the only American who has damaged U.S. cybersecurity in recent years. In 2013, an NSA contractor, Edward Snowden, perpetrated one of the most significant leaks in U.S. history when he provided journalists--and, according to some accounts, Chinese and Russian intelligence services--with thousands of highly classified documents revealing the

expansive reach of the NSA's global operations, including its eavesdropping on senior government officials of countries allied with the United States. It is difficult to overstate the negative impact these disclosures had on U.S. efforts to secure cyberspace. Washington essentially lost all credibility on the world stage when it came to issues regarding cyberspace. After learning that the NSA had spied on heads of state, including German Chancellor Angela Merkel, European governments were in no mood to work with Washington against Chinese or Russian cyber-operations. "Trust needs to be rebuilt," Merkel said at the time.

In the wake of the revelations, a wide range of governments--from U.S. allies in Europe to China--labeled Washington as the greatest threat to cybersecurity in the world. The fallout from Snowden's leaks also dealt a devastating blow to the cooperation between the U.S. government and the private sector, an essential aspect of defending U.S. interests in cyberspace. Owing to a fear of bad publicity and the risk of losing business in China, U.S. technology companies that had previously collaborated on unclassified cybersecurity initiatives with the federal government decided to completely halt such cooperation.

Things got worse a few years later when the NSA lost control of some of its most sensitive hacking tools. In two separate incidents, employees of an NSA unit that was then known as the Office of Tailored Access Operations--an outfit that conducts the agency's most sensitive cybersurveillance operations--removed extremely powerful tools from top-secret NSA networks and, incredibly, took them home. Eventually, the Shadow Brokers--a mysterious hacking group with ties to Russian intelligence services--got their hands on some of the NSA tools and released them on the Internet. As one former TAO employee told The Washington Post, these were "the keys to the kingdom"--digital tools that would undermine the security of a lot of major government and corporate networks both here and abroad."

One such tool, known as "Eternal-Blue," got into the wrong hands and has been used to unleash a scourge of ransomware attacks--in which hackers paralyze computer systems until their demands are met--that will plague the world for years to come. Two of the most destructive cyberattacks in history made use of tools that were based on EternalBlue: the so-called WannaCry attack, launched by North Korea in 2017, which caused major disruptions at the British National Health Service for at least a week, and the NotPetya attack, carried out that same year by Russian-backed operatives, which resulted in more than $10 billion in damage to the global economy and caused weeks of delays at the world's largest shipping

company, Maersk. In the past few years, ransomware attacks have struck hospitals, schools, city governments, and pipelines, driving home the severe nature of the cyberthreat.

## HOW TO DO BETTER

Washington's decade spent in thrall to an outmoded conception of cyberconflict, the Obama administration's excessive passivity, the Trump administration's inconsistency, and the damage caused by leaks and sloppiness meant that when U.S. President Joe Biden took office earlier this year, he inherited a mess. Getting U.S. policy back on track will require his administration to substantially change the way that Washington conceives of and carries out cybersecurity. That will be particularly challenging given the current security environment, which is being shaped by China's rollout of the "digital yuan," the meteoric rise in the value and impact of cryptocurrencies, the flourishing of disinformation, and the sharp increase in ransomware attacks. Meanwhile, as nuclear negotiations with Iran intensify, the regime in Tehran will likely experiment with new cyber- and information operations to gain leverage at the negotiating table, and China and Russia will almost certainly test the relatively new administration with cyberattacks within the next year.

In this climate, the most important thing the Biden administration can do is embrace the notion that countries that can conduct destructive cyberattacks are not likely to be deterred by Washington's own cyber-capabilities but can still be deterred by the United States' conventional military power and economic might. When it comes to cyberspace, Washington shouldn't try to fight fire with fire--or at least not with fire alone. The United States, after all, has many more effective ways to contain and extinguish the flames.

With that in mind, the first practical step the administration should take is to prioritize the defense of data. Working with Congress, Biden must redouble efforts to pass a national data security law that will provide citizens with the right to take legal action against companies that fail to protect their data, similar to the European Union's General Data Protection Regulation. The United States is one of the only major democracies in the world that does not have such a law. As a result, an extraordinarily complex patchwork of state-level privacy and data security laws have sprung up, inhibiting the development of a secure information-based economy. The current effort on Capitol Hill to require companies that provide critical infrastructure--including those in the manufacturing, energy production, and financial

services sectors--to notify federal authorities of data breaches represents a promising development. But it is not nearly enough.

The administration should also make the rapid public attribution of cyberattacks a core component of its strategy, even in politically complex situations. The conventional wisdom used to hold that it was difficult to attribute cyberattacks with a high level of confidence. But over the past five years, advanced digital forensics have allowed intelligence agencies and private-sector cybersecurity firms to conclude with reasonable certainty who is behind most cyberattacks. That evolution is important: attribution alone has proved to be an effective, if short-lived, way to deter U.S. rivals from carrying out attacks.

Better U.S. policy will also require some organizational shifts. For starters, the Cybersecurity and Infrastructure Security Agency, established in 2018 within the Department of Homeland Security, must become the true center of gravity for domestic cybersecurity operations; the final authority over such operations should not be granted to intelligence organizations, law enforcement agencies, or the military. In the past three years, CISA has developed important capabilities to combat election interference and disinformation campaigns. Now, it must improve its defense of federal government networks, speed the sharing of threat indicators with the private sector, and offer expertise and operational support to the providers of critical infrastructure that face threats from ransomware. To do all that, CISA will need more funding: the organization's current annual budget of $3 billion should be tripled over the next four years, and it should eventually equal that of the NSA.

Law enforcement still has an important role to play, particularly when it comes to domestic defensive cyber-operations to thwart ransomware attacks. The FBI recently undertook an effective and creative effort to remove malicious tools implanted by Chinese intelligence services in hundreds of servers across the United States. In a novel and precedent-setting step, the bureau obtained warrants to unilaterally identify and delete the Chinese malware without the consent of the equipment's owners. The legal authority for that operation was established by an update to the Federal Rules of Criminal Procedure; the administration should seek additional innovative updates to laws that will allow the FBI to take more proactive measures.

The U.S. military must also continue to adapt to the cyber-era. Biden should shape Cyber Command into something more akin to today's nimble, flexible Joint Special Operations

Command and less like the lumbering Strategic Air Command of the 1950s. Cyber Command has relied too much on the NSA to create unique, non-attributable cybertools, which can take years to develop; to increase its agility, Cyber Command should turn to less complex, "burnable" tools, that is, ones that are expendable because they are already publicly available, which means there is no need to conceal their origin. The Trump administration, to its credit, upped Washington's game by increasing the frequency of low-tech, publicly attributable offensive cyber-operations. This had the effect of bolstering U.S. credibility in the cyber-realm--even in the face of Trump's erratic personal conduct. For example, after Iran's elite Islamic Revolutionary Guard Corps shot down a U.S. surveillance drone in 2019, Cyber Command conducted a retaliatory attack on a database crucial to the group. The strike demonstrated Washington's ability to achieve strategic goals while avoiding escalatory tactics. New legislation and new approaches would go a long way toward fixing Washington's flawed cyberstrategy. But the government cannot improve U.S. cybersecurity on its own: it must meaningfully engage with the private sector to build cyberdefenses and cyberdeterrence. Companies are in the cross hairs of hackers of many stripes, and corporate leaders have become de facto national security decision-makers. To create shared norms and encourage the independent enforcement of cyberprotection standards, at least by publicly traded companies, Congress should consider creating a cybersecurity analog to the Securities and Exchange Commission, which protects the integrity of markets, and a version for cyberspace of the Generally Accepted Accounting Principles, which shape the public disclosures that companies must make.

Even if Washington does everything right, it will still need global cooperation. Luckily, the geopolitical environment today is conducive to strong U.S. diplomatic leadership on issues regarding cyberspace. Washington has mostly recovered from the fallout of the Snowden and the NSA leaks, and the world has finally recognized that the Chinese and Russian models of Internet autocracy are antithetical to a liberal order and a globalized economy. Washington needs to take advantage of this state of affairs through intensive cooperation with like-minded countries, such as France, Germany, Japan, South Korea, and the United Kingdom.

The UN is not the place to do so, however: in that forum, China and Russia can advance their interests by entangling Washington and its partners in abstract debates about norms even as they wantonly violate those norms in the real world. Many strategists have suggested that NATO could serve as the center of gravity for cooperation in cyberspace between the Unit

States and its allies and partners, but the organization was built for the Cold War and is too clunky to foster creative strategies. Instead, Washington should pursue a series of bilateral agreements to prevent the spread of black-market ransomware tools. One model might be the Proliferation Security Initiative, a multilateral effort inaugurated by the George W. Bush administration to improve the interdiction of weapons of mass destruction.

If American policymakers have learned anything in the past decade, it is that cyberconflict is a murky business, one that resists black-and-white notions about war and peace. That lack of clarity in the battle space makes it all the more important for Washington to be clear about its goals and strategies. The cyber-realm will always be messy. But U.S. cyber-policy does not have to be.

~~~~~~~~

By Sue Gordon and Eric Rosenbach

SUE GORDON is a Senior Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs. She served as Principal Deputy Director of National Intelligence from 2017 to 2019, after nearly three decades at the CIA.

ERIC ROSENBACH is Co-Director of the Harvard Kennedy School's Belfer Center for Science and International Affairs. He served as the Pentagon's Chief of Staff from 2015 to 2017 and as U.S. Assistant Secretary of Defense for Homeland Defense and Global Security from 2014 to 2015.

---
~~~~~~~~