Stanford | Cyber Policy Center
Freeman Spogli Institute

THE NEXT CYBER STRATEGY: PLAYING A BETTER GAME OF WHACK-A-MOLE

STANFORD UNIVERSITY

Jacquelyn Schneider, PhD
Hoover Fellow, Stanford University

THE NEXT CYBER STRATEGY: PLAYING A BETTER GAME OF WHACK-A-MOLE

Summary here.

In 2011, the Obama Administration penned their first cyber strategy. The International Cyber Strategy called for an internet that promoted "prosperity, security, and openness" by upholding principles of "free speech and association, privacy, and the freedom of information." The strategy leaned heavily on norms, diplomacy, and then dissuasion and deterrence in order to achieve these goals. It has been a decade since this initial strategy and the threats to these strategic principles have been perhaps more diverse and prolific than the strategy had imagined. Over this decade, and two administrations, the US has evolved and experimented its strategic efforts to respond to these threats. Now, as the US moves into a new administration, are we still focused on these same strategic principles? And what have we learned about what works and what doesn't in cyber strategy?

This article briefly introduces the trajectory of US cyber strategy over the last decade, identifying big changes (both in threat landscape and strategic effort) along the way. In looking back, it identifies a path for the future. Finally, it concludes with pragmatic suggestions for implementing and then evaluating the effectiveness of the cyber strategy.

A BRIEF TRIP THROUGH THE CYBER PAST

The Obama Administration made the first real forays into US cyber strategy, setting the foundation of US strategic interests and embarking on the first attempts to corral the US government to support those interests.

Throughout these eight years, the Obama Administration made openness and reliability a priority for cyberspace. This belied an assumption made by the administration that freedom of information was both good for the international community and the United States' economic and foreign policy interests. This stood in contrast to other countries like China or Russia that pushed back on openness, instead advocating for more balkanization and domestic sovereignty over cyberspace, ultimately restricting flows of information for domestic control. And while China and Russia represented the far end of this debate, at the same time Europe was experimenting with a hybrid model that focused more on digital sovereignty and regulation.

Perhaps the largest threat to the Obama Administration's strategic priority wasn't the international contest of openness versus balkanization, but instead the proliferation of threats to the capabilities and dependencies that came with the modern digital society. Over this time period, not only did non-state cyber-crime become more capable and ubiquitous, but states started to target cyber vulnerabilities for espionage, coercion, and conflict. From the North Korean-lead cyber-attack on Sony, Russian cyber-attacks within military conflicts in Georgia and Ukraine, Chinese mass exfiltration of data from the Office of Personnel Management and widespread intellectual property theft. Finally, on the tail end of the administration, foreign-led disinformation campaigns with hack and reveal strategies weaponized the free flow of information within US society, turning what had been a strategic strength of the US into a domestic vulnerability.

The Obama Administration's response to these cyber threats was to focus on norms and domestic information coordination and response while relying on the threat of sanctions and department of justice indictments to deter state-sponsored activity. US offensive cyber capabilities resident with the Department of Defense were closely held and restrained at the highest levels, used only sparingly within existing military campaigns (like the fight against ISIS). The Obama Administration spent much of their time creating the foundations of inter-agency coordination, determining the appropriate roles and responsibilities of federal agencies—a daunting task which was codified within an infamous PowerPoint bubble chart that put the Department of

Homeland Security and Federal Bureau of Investigation in charge of most of the existing cyber threats and leaned on the State Department to create and propagate norms that supported US strategic priorities. The Department of Defense was largely a supporting agency in this construct, building capabilities to deploy in conventional conflict and struggling to create credible deterrence options to dissuade states from conducting a wide array of cyber activities, from espionage to attacks against nuclear infrastructure.

This was a period of learning and building, in which the administration focused on creating a unified federal approach to cyberspace. Their work creating lanes of effort within the federal government created a strong foundation for the incoming administration. Further, the administration clearly articulated normative principles and worked hard to propagate these norms within the United Nations and in relationships with allies. Where it was most successful was when it could focus these normative discussions on concrete actions, for instance creating task forces that focused on Chinese intellectual property theft or packaging norms about attacks on civilian infrastructure with executive orders on sanctions.

Despite these successes, this was also a period of relative restraint in US responses to cyber threats, and, coming into the Trump administration, state sponsored cyber activity was in no way slowing down. There was a push from within both the private sector and the Department of Defense for a more active and forward leaning strategy to combat these proliferating cyber threats—a push which found a willing audience in the Trump Administration.

In 2018, the US rewrote all of its cyber strategies and moved from a diplomacy deterrence-first, "be prepared" stance under the Obama Administration to a forward-leaning, risk acceptant, and active strategy under Trump. In particular, the 2018 summary of the Department of Defense's Cyber Strategy introduced the concept of "defend forward," confronting adversaries before cyber-attacks even occur "to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." In general, the Trump Administration's approach was highly decentralized, giving much more autonomy and newfound responsibilities to the Department of Defense and Cyber Command (which was now a unified command).

This autonomy, combined with very operationally focused leaders like new commander, General Nakasone, led to large scale experimentation in Department of Defense cyber operations. Meanwhile, the Department of Homeland Security leaned forward under new leadership in its Cyber and Infrastructure Security Agency, ushering in a much more publicly responsive face to cybersecurity and new partnerships with both the private sector and the department of defense. Cyber Command and the Cyber and Infrastructure Security Agency began to release information about malware and threats broadly and created new operational structures centered around issue-specific task forces (for instance election security) that appeared to be relatively successful. Meanwhile, Cyber Command used its new authorities to develop new missions like "hunt forward," which sent US cyber troops into allied and partner networks to search for adversary activity and to grow the new Cyber Mission Force (in both mandate and personnel).

Despite these tactical and operational innovations, the Trump Administration struggled to translate innovation to strategic success. A revolving door of personnel within the National Security Council, White House strategies disconnected with agency or command visions, and conflicting foreign policy priorities within the White House itself stymied cyber progress. Further, unclear language within Department of Defense strategies and Cyber Command Vision, led onlookers to question what the defense cyber was really doing. While **public statements** and **DOD-sponsored articles** painted a picture of defend forward that included cyber defense teams in allied states or intelligence sharing with private sector, unofficial **reports by the New York Times** suggested US was placing malware exploits in Russian critical infrastructure. This led onlookers to question how far forward exactly the US was defending. Faced with this ambiguity, some critics worried the US' new strategic concept could inadvertently lead to retaliation, potentially violent. Further, even those who supported defend forward, voiced concern that these operations could become never ending task forces, expensive to sustain, and difficult to tell whether they were more or less effective.

BUILDING THE NEXT CYBER STRATEGY: GOALS

Moving into the new Biden Administration, where does that lead us? The recent SolarWinds hack suggests that the US is still playing whack-a-mole in cyberspace, but after heavy foundational lifting by the Obama Administration and four years of relative neglect but operational innovation from the Trump Administration, the US is playing a much better game. When the Biden Administration rewrites the next cyber strategy (optimally published before any new agency strategies), it should not return to Obama 2.0, nor should it continue on the disorientated path created by the Trump Administration.

> ***While the US may often compete with rising powers within cyberspace, the goal is not to just "win" at competition, but instead influence behaviors across the international community so that the US can create an international order that supports democracy, prosperity, and peace.***

Instead, it should draw on the strengths of both: looking to the strategic priorities articulated within Obama strategies while generating new lines of effort from the operational learning done under the Trump Administration.

Building a new cyberspace strategy begins with outlining strategic priorities. Here is where the Obama Administrations' original focus on an open, free, and secure internet is still incredibly valuable. These characteristics remain noble goals for the US and, if achieved, will support a larger Biden foreign policy strategy that returns to the democratic principles which make the US different from authoritarian states like Russia or China. While the US may often compete with rising powers within cyberspace, the goal is not to just "win" at competition, but instead influence behaviors across the international community so that the US can create an international order that supports democracy, prosperity, and peace.

The new cyberspace strategy, however, will have to have even loftier goals than the Obama Administration. That is because the US has learned about the danger not only in not having access to information, but also in accessing invalid information—whether that be campaigns of disinformation or the manipulation of data to degrade trust in our economic or governance systems. Therefore, the new US cyber strategy will have to seek not only an open, free, and secure internet but will also have to safeguard genuine or valid information. This is a key addition to strategic priorities because if the Biden Administration's strategic focus is on restoring economic prosperity and democracy at home, then having a cyberspace that can be relied on for valid or genuine information will be key. How can the US achieve these strategic goals, especially given the proliferation of threats to data and cyberspace?

BUILDING THE NEXT CYBER STRATEGY: LINES OF EFFORT

The primary line of effort for the Biden cyberspace strategy—around which all other lines of effort bolster—should be resilience, or as Dr. Erica Borghard explains, "the ability to anticipate and withstand a disruptive event, and to rapidly restore core functions and services in its wake, whether it be a pandemic, financial crisis, terrorist attack, or large-scale cyber incident." Resilience requires not only investing in federal networks and technologies that are more technically resilient, but also in building data users that are more resilient. For the largest US government data user, the Department of Defense, this involves building networks that gracefully degrade and campaigns that can be executed with limited access to data. At the core for any data user, whether it is a military officer, a federal civilian, or an American citizen is building human resilience—educating data users to question their data's biases, to look at data sources, and to have a back-up plan in place when they don't have access to digital resources.

Tied intimately to resilience are three activities: defense, intelligence, and information sharing. Cyber defense includes adopting commercial cybersecurity best practices for the federal government and defense information network but will also require new focus on cybersecurity when acquiring these capabilities. These defense efforts are aided by investments in technical intelligence talent and information sharing across the private sector and federal agencies. All three of these activities benefit from investments in commercial cybersecurity technology, as well as federal investment in research and development in cybersecurity. Further, the Biden administration should continue to build out the interagency and public-private information sharing that matured over the Trump Administration. In particular, creating ways to quickly share threat information across economic sectors and within the existing agency partnerships will reap large rewards.

> ***The US needs to resolve a current contradiction in the strategy between a nation that nominally propagates norms to not attack civilian critical infrastructure and yet does not define the limits of its own cyber actions taken under the Department of Defense's defend forward strategy.***

During the Obama Administration, norms and deterrence played a central role in cyberspace strategy. However, they were largely punted during the Trump Administration in favor of new concepts like "defend forward" and "persistent engagement." But these concepts are not replacements for each other and can and should co-exist. The difficulty is two-fold. First, the US needs to define what it cares about so that it can have credible cross-domain threats of punishment to deter the worst type of cyber-attacks: those that create violence to US citizens or threaten the US nuclear arsenal. Secondly, the US needs to resolve a current contradiction in the strategy between a nation that nominally propagates norms to not attack civilian critical infrastructure and yet does not define the limits of its own cyber actions taken under the Department of Defense's defend forward strategy.

How can the Biden Administration shore up strategic deterrence and maintain stability while being more actively engaged in countering cyber operations? The good news is that key parts of the Department of Defense's 2018 strategy, and in particular the assumptions behind defend forward, are supported by scholarly research. The increase in cyber-attacks pre and post-COVID, as well as **scholarly analysis of cyber deterrence**, suggest that ambiguous threats of deterrence are not enough to significantly curtail most cyber-attacks. In addition, **wargames with private sector representatives** provide evidence of strong support within American businesses for a more forward leaning cyber strategy to counter adversary cyber-attack. Finally, **experimental research** largely supports the strategy's assumption that cyber operations rarely lead to violent retaliation.

That's the good news for the 2018 Department of Defense cyber strategy. The US can use "defend forward" to counter adversary's cyber-attack capabilities and decrease cyber-attacks. The bad news is that if the US defend forward strategy is going to successfully degrade bad guy cyber capability and preserve strategic stability, it still has to rectify the hypocrisy problem lurking in the US' overly ambiguous strategy.

Here the Biden Administration has a real opportunity—not only to ensure the success of its own strategy, but also to build norms of appropriate behavior in cyberspace. To do this a new strategy first needs to announce to adversaries and allies what is off limits, and subsequently deter these strategic cyber-attacks by threatening credible retaliation options. We've come close to this before. The Obama Administration crafted an **Executive Order on sanctions** in response to cyber-attacks on critical infrastructure and Trump's State Department has called out cyber-attacks on health infrastructure as inappropriate behavior in cyberspace. However, the US has always stopped short of binding its own hands or credibly threatening anything beyond sanctions or tit for tat cyber punishment for these cyber-attacks.

This is partially because the US has been too expansive in what it has deemed as “off limit” cyber targets for adversaries. The Obama Administration’s definition of critical infrastructure spanned 14-16 sectors and both Administrations have struggled to define what kinds of cyber operations against these infrastructures they seek to deter. If everything is important, then nothing is important. Absent an understanding of what the US cares about in cyberspace, ambiguous cyber deterrence by punishment policies have been unable to stem the increasingly prolific and sophisticated wave of cyber operations against US civilian enterprises.

The first step, therefore, in solving the US cyber strategy problem is to decrease strategic ambiguity about what cyber-attacks are serious enough to warrant a violent response from the US. To date, the US has not resorted to violence in response to cyber-attacks, even though the US has threatened up to nuclear response to cyber-attacks. Instead of these ambiguous threats, the US needs to focus strategic deterrence on the cyber-attacks which are the most likely to have credible deterrence options. This is a high bar. Most cyber-attacks will not be able to be credibly deterred, but the US may be able to credibly threaten cross-domain punishment for truly strategic cyber-attacks: those that create violent effects against civilian populations or threaten a state’s nuclear control. At this high strategic level, which is only reserved for the most dangerous cyber operations, the US can credibly threaten its vast and lethal military force and therefore shore up deterrence.

But defining and deterring what the US cares about at the strategic level is only the first necessary step to solving the US cyber strategy problem. The US must not just assert these targets off limits for US adversaries, but also declare them off limits for the US. The adoption of a **no-first-use cyber strategic attack policy**, especially one buttressed by credible threats of retaliation across military options, can help signal credible US restraint and scope appropriate “status quo” cyber activity, thus shoring up both a strategic threshold of restraint and a lower threshold of status quo cyber activity that occurs without violent retaliation. Both of these thresholds are essential for the current US cyber strategy to succeed. And while a no first use policy was never adopted in the nuclear world, there are important differences in cyberspace that make no first use more credible and more advantageous than in the nuclear domain.

While the adoption of a no first use strategic cyber-attack policy will help shore up strategic restraint, the US will have to go beyond no first use in order to ensure strategic success. It must also pair a strategic no first use policy with clearer statements about what types of activities fall under defend forward—thus making both ends of the cyber spectrum less ambiguous and more defined. Ideally, defend forward is a concept scoped to include only counter-cyber operations against cyber adversaries and not to target adversary civilian infrastructure. While defend forward may include up to offensive cyber activity, a clearer articulation of the focus of defend forward activities should help assure adversaries (and allies) that the US will restrain these attacks and not target civilian infrastructure preemptively. This may help to solve the US strategy's hypocrisy problem and correct the logical inconsistencies of an otherwise ambiguous defend forward.

All of these actions support norms that the strategy should propagate about what are responsible actions in cyberspace—what is off limits (for us and our adversaries) and where does the US need to invest in resiliency, defense, and punishment to make cyber exploits less likely to succeed. Diplomacy should focus on what might be largely popular across both allies and adversary nations, for example agreements (binding or non-binding) to restrain state-sponsored attacks against critical infrastructure. Meanwhile, the State Department could pursue bilateral or hub and spoke agreements that graft off of existing arrangements—for example negotiating agreements to restrain cyber network exploitation or attacks against nuclear arsenals by grafting off existing nuclear arms control agreements. While norms are not a line of effort in the strategy, they are the result all the other lines of effort seek to achieve. They are most likely to succeed when all lines of effort converge and so future diplomatic efforts should include military to military discussions as well as coordinated signaling strategies.

Finally, the Biden Administration will have to carve out of an already tight budget investments in crisis response, cyber support to conventional campaigns, and law enforcement. All of these lines of effort require more cybersecurity talent as well as federal funding for technology and coordination between local governments and federal agencies. The Biden Administration should not be afraid of creative approaches to talent in the federal workforce, including a better use of the military reserves, the development of a civilian reserve corps, and more government fellowships for both academic and industry leaders to contribute to the federal workforce, even for a short time.

These efforts also require a closer look at whether our current planning and organizational structures are optimized for the threat. For example, the development of task forces within Cyber Command and other federal agencies was an important innovation that replaced a rigid military campaign planning structure that never worked for cyber. But how does the US organize task forces for non-time-delineated tasks like dealing with China? Further, these never-ending task forces are expensive and manpower intensive. How do we know how these task forces should be manned and what is working (or not working)?

FINAL THOUGHTS

Over the last few decades, the US has doubled down on digital technologies, using these digital resources to forge a dominant military, an advanced digital economy, and a highly connected society. But these technologies have also come under threat and the operational cyber innovations made over the last four years at places like the Department of Homeland Security's Cyber and Infrastructure Support Agency or the Department of Defense's U.S. Cyber Command will not be enough to forge strategic success. The incoming Biden Administration should return to the principles and strategic focus of the Obama Administration, but also build on the tactical and operational successes the Trump Administration may have unwittingly created by largely ignoring the cyber efforts at defense or homeland security.

An open and free internet is still important to democracy and a vibrant economy, but the incoming administration will have to do more to safeguard valid information in order to salvage the role of the internet in our society.

Finally, it is important to highlight that the greatest instability created by data has not been in warfare but instead in the ways in which our digital dependencies can be manipulated to further schism already existing divides within our societies. The Biden Administration will have to take on the very difficult task of regulating information without suppressing freedom of speech. An open and free internet is still important to democracy and a vibrant economy, but the incoming administration will have to do more to safeguard valid information in order to salvage the role of the internet in our society. As with all things cyber, the answer is not in the technology, but instead in humans and building resiliency and trust in the data that undergirds our democracy, our society, and our economy. It will be a tall order, but the US is better postured for that challenge today than it has been in the previous decade.

ABOUT THE AUTHORS

Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution. Her research focuses on the intersection of technology, national security, and political psychology with a special interest in cybersecurity, unmanned technologies, and Northeast Asia. She is a non-resident fellow at the Naval War College's Cyber and Innovation Policy Institute and a senior policy advisor to the Cyberspace Solarium Commission.