In June of 2019, the New York Times reported that the United States was “stepping up digital incursions into Russia’s electric power grid in a warning to President Vladimir V. Putin.”¹ The reporters accused the United States of planting malware within Russian critical infrastructure under new authorities granted by the White House to the Department of Defense (DoD) for offensive cyber operations. According to the article, the acts were part of a new US strategy to use cyber operations to signal capabilities and therefore deter further Russian incursions into US critical infrastructure,² indicating that strategic cyber attacks—which create immediate physical violence to large segments of civilian population or attacks that affect a state’s ability to control its nuclear forces—were now credible arrows in the US foreign policy quiver against Russia.

The New York Times article highlighted a significant shift for US cyber strategy that occurred in 2018 when the DoD unveiled a new cyber strategy as well as a new vision for US Cyber Command, their joint cyber warfighting command.³ The strategy and vision promised to “defend forward” and “persistently engage” in cyberspace⁴—taking cyber operations into adversary networks even before the adversary could launch their own cyber attack—all without triggering escalation to armed conflict.

Proponents of defending forward assume that the United States can act in cyberspace without triggering escalatory responses from adversaries, because the
constant use of cyber operations inures states to cyber incidents and, therefore, decreases emotional or strategic incentives to respond to cyber operations with escalation—whether that be acts of war or other slightly less violent responses. However, the New York Times article and even statements within the US Nuclear Posture Review simultaneously suggest contrasting logic: the United States expects its cyberattacks to deter others from cyberattacks against the United States. Yet, it is logically unlikely that others will remain in a limited-retaliation cyber environment while simultaneously allowing the United States to threaten to escalate it.

I unpack this dissonance throughout the article by first discussing the evolution of US cyber strategy and the origin of its inherent contradiction, or the two-threshold problem. I then introduce the concept of no-first-use (NFU) and detail what cyber NFU would look like in practice. Next, I explore whether the arguments against a US nuclear NFU policy hold up in cyberspace. Finally, I discuss how the United States could pair this restraint with status quo cyber operations to solve the two-threshold problem that plagues US cyber strategy.

**US Cyber Strategy Evolution and the Origin of the Two-Threshold Problem**

The DoD released its first cyber strategy under the Obama administration in 2015. The strategy, which hedged against a presumed significant risk of escalation from unrestrained cyber operations, focused on norms and deterrence, calling on the DoD to “be prepared” in case of cyber attacks against the United States, but to use cyber attacks only under the authority of other uses of force, like conventional armed force campaigns.

The Obama administration saw the digitally dependent US economy, society, and military as uniquely and asymmetrically vulnerable to cyber attacks. It worried that an increase in US use of cyber operations would open a Pandora’s box of cyber retaliation against it. Therefore, the United States had to restrain its own cyber operations in order to credibly build norms of cyber activity and to deter adversaries from conducting cyber attacks against the United States. In practice, that deterrence was mainly focused on cyber attacks against critical infrastructure, though the strategy itself never defined exactly what types of cyber attacks the United States would seek to deter.

The Obama administration’s policy was best articulated by then-Secretary of State John Kerry in a 2015 speech: “no country should conduct or knowingly
support online activity that intentionally damages or impedes the use of another country’s critical infrastructure." The administration put this idea into practice in 2016 when Obama signed an executive order that authorized economic sanctions in response to any “significant malicious cyber-enabled activities.”

Despite the efforts of the Obama administration, cyber attacks and operations against critical infrastructure grew more sophisticated and normalized tools of state coercion. The 2016 Russian cyber-enabled operation to influence the US elections, Russian attacks on Ukrainian power grids later that year, and North Korean and Iranian attempts to extort money from the US financial sector dating back to 2014 all demonstrated the increasingly front-line role of critical infrastructure in state-led cyber attacks.

The more assertive and forward-leaning Trump cyber strategy adopted in 2018 was a response to what many viewed as overly fearful and ultimately risk-averse policies under the Obama administration. The Trump administration’s Department of Defense would now “defend forward,” launching attacks against adversary cyber capabilities even before large-scale cyber attacks could occur. Michael Fischerkeller and Richard Harknett, two scholars who worked closely with Cyber Command to craft its vision in this new cyber era, made two arguments in favor of this strategy: first, deterrence would not work in cyberspace—it demanded a strategy of persistence. And second, the only way to shape norms and behavior in cyberspace was not through restraint, but through persistent action, suggesting that, perhaps counterintuitively, “a doctrine of active mitigation may be less escalatory than one of restraint.”

Advocates of this mission also argued that constant confrontation within cyberspace would normalize cyber operations as status quo state competition, thereby minimizing the risk of violent escalation from US cyber sparring. As this line of logic concluded, constant confrontation by defending forward and persistently engaging would create a de facto agreed zone of competition and tacit bargaining space that would bind cyber interaction without resorting to armed conflict, while at the same time replacing or augmenting deterrence of strategic cyber attacks.

Critics of the new cyber strategy, however, pointed out a fundamental flaw in its logic. The new strategy assumed limited escalation risk from US cyber activity defending forward, but it was extremely vague about exactly what activities were included as a part of defending forward. Interviews and illustrations from DoD practitioners along with open source reporting detailed a huge potential range of activities under “defend forward,” from counter-deployment of cyber protection teams in allied nations, to cyber

**US strategy is extremely vague about what activities are included as part of defending forward.**
operations against adversary cyber networks, private sector intelligence sharing, and finally to the use of malware within adversary electrical grids. At the same time that the United States was struggling to explain what it meant by “defend forward,” its strategy threatened escalation across domains if adversaries conducted cyber operations against US critical infrastructure. The administration hypocritically assumed that its own cyber actions were non-escalatory (and could therefore occur at limited risk) while also threatening escalation if similar operations were conducted against the United States, a particularly precarious assumption given the lack of a clear definition for “defend forward.”

This dissonance places the success of the overall cyber strategy in jeopardy by threatening the viability of two cyber thresholds in US strategy, illustrated in Figure 1. US actions below the status quo competition cyber threshold, at the lower end of the escalation ladder, exist if retaliation against US cyber attacks is bounded to tit-for-tat engagement below violence or armed conflict. Meanwhile, at the high end of the escalation ladder, the United States seeks to maintain a strategic cyber attack threshold that uses the threat of punishment to deter cyber attacks with violent effects against US critical infrastructure as well as attacks against US nuclear control. In between these two thresholds are actions that, while more escalatory than status quo competition, are also not considered strategic. These include the use of cyber operations to create violent and non-violent effects within conventional (and irregular) military campaigns.

**Figure 1: The Two Cyber Thresholds in US Strategy**

- **High strategic actions**
  - Violent cyber attacks against US critical infrastructure
  - Cyber attacks against nuclear control

- **Strategic Cyber Attack Threshold**
  - Actions with limited violence or at a geographic distance
    - Cyber operations within conventional military campaigns

- **Status Quo Cyber Competition Threshold**
  - Actions with low to no violence
    - Counter-cyber operations with virtual effect
    - Cyber intelligence operations
If and when these actions in the middle of the escalation ladder were to occur, then US strategy would need a strong strategic cyber attack threshold to safeguard its domestic populations and nuclear inventory. The strategic threshold is more likely to hold if cyber actions in status quo competition (defend-forward counter cyber operations) degrade adversary cyber attack capabilities so that they are unable to make the attack in the first place. However, the status quo threshold comes under threat if the United States is unclear about what it considers off-limits cyber activity.

The cyber strategy’s ultimate success will be contingent on developing and strengthening both cyber thresholds: scoping actions under defend-forward while deterring strategic cyber attack. These aims may at first appear contradictory. Indeed, efforts to use cyber attacks on an adversary’s critical infrastructure (like those reported in the New York Times), which may have been envisaged to shore up the strategic threshold, are ultimately likely to degrade the status quo threshold. Because this lower threshold is contingent on adversary restraint, ambiguous threats of cyber punishment can inadvertently create incentives for adversary escalation and undermine efforts to bound cyber competition to the low end of the escalation ladder. Worse, emerging research suggests that the use of ambiguous threats of cyber attacks on adversary critical infrastructure is rarely effective at deterrence. Therefore, strategic cyber attacks not only threaten the efficacy of defending forward, but they may also not significantly increase deterrence success.

**No-First-Use Policies and Declaratory Restraint**

Today’s cyber strategy is not the first time that states have struggled to set and maintain thresholds in order to mitigate instability and maintain deterrence. Throughout the Cold War, the United States struggled to signal credible nuclear capabilities to deter adversary nuclear strikes while limiting the risks of inadvertent escalation or accident. And while the resolution of the Cold War may have decreased the immediate danger of instability between the United States and the Soviet Union, many of these challenges continue today as states look to build nuclear postures that ensure strategic stability by balancing credible deterrence with restraint and non-proliferation. How states credibly signal nuclear restraint while also maintaining stability is therefore a potential model to solve the United States’ current two-threshold cyber problem.
One of the solutions for the stability, restraint, and deterrence problem within the nuclear world is the adoption of a declaratory policy of no first use of nuclear weapons. A nuclear NFU policy takes shape when a state declares that although it has nuclear weapons, and will continue to develop and rely on these weapons to deter nuclear strikes, it will not use nuclear weapons first. Instead, the NFU state will reserve the use of nuclear weapons as a second-strike capability to be used only after nuclear weapons have been used against it or its allies.

An NFU pledge is not a treaty. Instead, it is a public declaration of a state’s policy for restraint. Perhaps the most famous NFU policy is China’s nuclear pledge, first made in 1964, that it would “not be the first to use nuclear weapons at any time or under any circumstances.”\(^\text{15}\) And while outright NFU policies are rare, there are also gradations to NFU that offer more nuance than China’s pledge. For instance, at various times in its history, the United States has called its nuclear arsenal a “weapon of last resort,” signaling a desire to save nuclear weapons for only the most extraordinary circumstances, but falling short of declaring first-use restraint.

Finally, it is important to note that an NFU policy is not a weapons ban, an arms control agreement, or a taboo. To illustrate, the ban against chemical weapons is a treaty agreement between nations not to develop or to use chemical weapons. States that have signed onto the chemical weapons ban have no need to declare an NFU policy because they have already agreed never to use or even develop chemical weapons; declaring NFU would be redundant. Arms control agreements between the United States and Russia to limit nuclear weapons testing or nuclear weapons delivery platforms are also not NFU policies. Like NFU policies, they are developed to increase strategic stability, but unlike NFU policies, they are verifiable and often punishable treaty arrangements between states. Finally, a nuclear taboo, while a normative mechanism for restraint, is not necessarily an NFU policy (though it may lead to a policy of restraint).\(^\text{16}\)

No-first-use policies have existed primarily within the nuclear realm. However, the idea of an NFU policy is not restricted to the nuclear domain—in fact, it may provide a potential solution for the US cyber two-threshold escalation and deterrence problem because declaratory policies of restraint can increase states’ certainty about intentions, which is especially valuable for stability. And maintaining stability is especially important if a state wants to use other forms of power for coercion without unintentionally spiraling a relationship into war.

**Strategic Cyber No-First-Use Policies in Practice**

The cyber domain exhibits many of the same kinds of uncertainty that cause instability in the nuclear space. Cyber is often perceived as offense dominant
with a highly vulnerable landscape, a surfeit of bad actors, and a low cost of entry for attackers. It is difficult to discern intelligence exploits—or the development of cyber accesses and attack mechanisms—from precipitous attacks, making offense-defense differentiation a tall order for even the best cyber intelligence agencies. Further, ambiguous strategic vocabulary like “defending forward” or “persistent engagement” muddle offense and defense, complicating onlookers’ interpretation of US intentions in cyberspace. A declaratory policy of restraint like NFU could help solve these problems of inadvertent instability. However, the cyber domain is far more nuanced than nuclear with a panoply of different operations and effects. What would a cyber NFU policy for the United States look like?

**Distinguishing Strategic Cyber Attacks**

The first element of a cyber NFU policy must be the type of cyber operations that are included in the policy. Cyber operations span a spectrum of activities such as intelligence operations, information campaigns, defense operations, and cyber attacks. But even the highest end of the range of operations, cyber attacks, exists along a spectrum of potential effects that can include manipulation or deletion of data all the way up to physical damage. Further, cyber attacks can target many different types of networks and therefore may affect military, government, or civilian operations. An effective NFU policy must be clear about which of these operations are included in the restraint policy and which, like defending forward, are considered normal status quo cyber operations.

The first consideration when determining what to include in a cyber NFU is the relationship between NFU and credible deterrence. A policy of restraint is only possible when there are credible threats of punishment to ensure deterrence. In the nuclear world, this means that NFU is only credible if a state has a survivable second-strike capability. For the cyber realm, the concern is less about surviving a massive first-strike cyber attack (there is almost no evidence of these kinds of doomsday cyber scenarios happening) and more about whether or not the NFU state has the credibility to punish actors across domains if they cross a strategic cyber threshold.

This concern about credible cross-domain threats of punishment exists for two reasons. First, tit-for-tat cyber deterrence—or cyber attacks that deter cyber attacks—has shown little evidence of success. The characteristics that make cyber operations so effective at managing escalation risks (their virtual nature, difficulty in attribution, lack of emotional salience, etc.) are also those that make cyber
operations poor tools for signaling and deterrence.\textsuperscript{19} Second (and related), what have proven to be effective tools for deterrence by punishment are those means that exist across domains—for example, conventional military strikes.

What makes cross-domain threats of punishment for cyber actions challenging is that research has shown that cross-domain threats of punishment for cyber attacks are only credible when cyber attacks create violent and immediate effects and that they are more likely to trigger support for retaliation when the attacks affect civilian infrastructure or nuclear command and control.\textsuperscript{20} This means that the bar for effective cyber deterrence is high. In order to be successful, NFU policies will have to focus their efforts on the types of cyber attacks that create only the most violent and threatening effects.

What is this bar for a credible NFU? Can the United States delineate strategic cyber attacks from other attacks that fall below the strategic cyber threshold? For the purpose of an NFU policy, I define strategic cyber attack as one of two potential types of operations. The first is cyber attacks that create violent strategic effects on civilian populations (either intentionally or unintentionally). The focus on violence separates NFU strategic cyber attacks from those attacks that may have significant long-term effects, but in the short term only impact virtual data or create aggregate economic or societal costs. Based on this definition, the NFU policy would preclude attacks on financial systems, for example, which have significant long-term effects but do not necessarily create violence. These characteristics make NFU strategic cyber attacks discernable (based on their creation of violence) and differentiable from other more appropriate targets below the threshold of strategic cyber attack (for instance, conventional military forces).

The second category for the NFU policy is cyber attacks that threaten the control of nuclear forces. These are cyber attacks that directly impede a nation’s ability to launch—or call back—nuclear platforms. These are not cyber attacks that affect intelligence, surveillance, or warning, which may be dangerous to overall nuclear stability but are more difficult to differentiate from cyber attacks on conventional military systems (which are often entangled with these intelligence, surveillance, and reconnaissance, or ISR, capabilities).

The scoped focus of this cyber strategic attack NFU policy is designed to maximize deterrence success by focusing on a threshold that, if violated by an adversary, has the greatest possible deterrence by punishment credibility. But the specificity of the NFU’s focus also allows significant space for defend-forward counter-cyber operations to occur below the threshold of armed conflict. It also does not bind the United States to ceasing development of accesses or exploits that could be used as a retaliation to an adversary’s strategic cyber attack. Instead, it signals to adversaries that while the United States may actively probe for vulnerabilities and explore attack vectors, it will not exploit them unless another state takes a strategic cyber attack first.
Extended Cyber Deterrence
An effective cyber NFU policy would state that once another country has conducted a strategic cyber attack on US treaty allies, then the United States would consider it appropriate to conduct similar attacks. This caveat means that the cyber strategic attack NFU policy may remain even if there is significant escalation within other domains. For example, even if the Chinese were to pelt Taiwan with missile strikes, the United States would withhold cyber attacks against Chinese civilian infrastructure. However, if China were to launch cyber attacks with immediate violent effects against the Taiwanese citizenry (for example, a cyber attack on a dam that flooded a town), the United States could consider that a first use of strategic cyber attack that voids the cyber NFU policy. Also, like other examples of extended deterrence, it would always be the United States’ prerogative to determine attribution and strategic effects of cyber attacks. Allies would not have the ability to force the United States to renege its NFU cyber strategic attack policy.

Non-State Actors
While NFU is focused mainly on creating incentives for restraint between capable state actors in cyberspace, the same logic applies to non-state actors. US restraint against non-state actors may seem unappealing given that most cyber operations today come from non-state actors, but in reality, this restraint against non-state actors would cede very little US capability against them while increasing the credibility of restraint among much more capable state actors. Non-state actors have few strategic cyber targets (based on the definition presented above), meaning that the scoped conditions of US-declared restraint have little impact on US cyber campaigns against non-state actors. In other words, there is no two-threshold problem with non-state actors, so creating a rhetorical exception would confuse the matter more than it helps.

Furthermore, many campaigns against non-state actors are for hearts and minds and avoid collateral damage within civilian populations. Therefore, any cyber attack against non-state actors that creates violence against civilians would be potentially self-defeating for larger US strategic priorities. The reality is that most US actions against non-state actors in cyberspace look like counter-cyber operations a la defend-forward, and these actions are most likely to be successful when they occur without retaliation into other domains. Therefore, declaring to restrain strategic cyber attacks against both state and non-state actors can benefit US cyber strategy across a wide variety of actors without significantly impacting the toolset the United States is already using in cyberspace.

Attribution
The question of NFU’s applicability to state and non-state actors highlights the role of attribution in the successful implementation of this policy. Attribution
of strategic cyber attack is an important element of credible deterrence by punishment across domains, which is the primary mechanism for ensuring strategic cyber deterrence in an NFU strategic cyber attack policy.

Emerging research suggests that attribution may not be as unique or as challenging in cyberspace as previously assumed. Significant technical improvements have made attribution less of a unique concern for cyberspace, and the relatively quick attribution of North Korea for attacks against Sony or of Russia for attacks in Ukraine show a willingness for states to publicly attribute. Research also suggests that states and non-state actors can choose to use the uncertainty of attribution in cyberspace to refrain from public attribution and therefore decrease public pressure for retaliation. Similarly, wargames have shown that players use uncertainty about cyber attribution to restrain themselves and create cognitive hedges against retaliation to cyber attacks. Therefore, attribution does not impede the usefulness of an NFU cyber strategic attack policy—in fact, the uncertainty of attribution can provide incentives for restraint.

Inadvertent Strategic Attacks?

Another significant question for strategic cyber attack NFU is the role of uncertainty about intentionality in cyber effects. Modeling cyber effects prior to attack (and often tracing the effects of an attack post hoc) is certainly very difficult. Even surgical cyber attacks like Stuxnet—which used a targeted malware attack inside an Iranian nuclear control plant networks to damage centrifuges—have unintended effects beyond the initial target (in the Stuxnet case, the malware was found on control systems outside of Iran after the attack). What if a state meant to conduct a tailored counter-cyber operation, but instead accidentally impacted a cyber vulnerability that caused violent effects to civilian populations? And how important is intent for NFU?

First, the chance of an inadvertent attack that creates immediate and significant violent effects is extraordinarily rare, because the diffused nature of most digital networks often makes creating large-scale systemic effects difficult. It is also difficult to create large-scale first-order violence from cyber operations. Tales of cyber doom in which cyber hackers open dams or cut off the power to hospitals often discount the mitigating effects of back-up power, human fail-safes, or other resiliency mechanisms.

Second, these extremely dramatic cyber attacks often require unique accesses that come at significant cost and require dedicated attention. Therefore, because these types of attacks are so rare and hard to conduct, a cyber attack with immediate violent effects on civilians is more likely to show signs of intentionality than more common ransomware attacks on critical infrastructure or manipulation of data within financial systems (both serious attacks but not the kinds of attacks included in the NFU policy).
Third, the uncertainty about the potential effects of cyber operations can act as a restraint for actors, especially if an NFU policy is put in place in conjunction with a credible deterrence by punishment strategy. Concerns that a cyber attack may unintentionally cross the United States’ strategic cyber threshold (and be perceived as a cyber attack first use) because of collateral or unforeseen effects could restrain an adversary cyber attack, especially when the NFU is accompanied by credible deterrence by punishment threats.

Unilateral Action? Allied and Adversary Policy
The final question to address is whether the United States will require allied or adversary buy-in to the policy in order for it to be effective. Adversary perceptions about the credibility of NFU policies will always be up for debate. However, as the United States demonstrates strategic restraint over time, it will become more credible.

The United States may not need allies to adopt the same policy in order to be effective, but establishing (among both allies and adversaries) a definition of strategic attacks that would be unacceptable is useful to the proliferation of cyber norms about acceptable behavior in cyberspace. The end goal of an NFU policy is to encourage restraint across adversaries as well as allies. Therefore, the adoption of NFU by other countries is an end, but not a requirement, for successful policy.

Applying the Nuclear NFU Debate to Cyberspace
Despite the arguments for NFU, the United States has never implemented a clear declaratory NFU policy for nuclear weapons. Does that mean cyber NFU is dead in the water? In order to answer this question, it is important to first understand why the United States has never adopted a nuclear NFU policy and to see if the arguments hold up in the cyberspace domain.

Extended Deterrence
Perhaps the strongest argument against NFU policies for nuclear weapons is the impact of NFU on extended deterrence and the credibility of US commitment to allies in close proximity to adversaries. This concern was especially compelling when the USSR was considered conventionally more capable than the United States. As Paul Nitze, then-Director for Policy Planning at the Department of State, wrote in NSC-68, a declaration of nuclear NFU “would be interpreted by
the USSR as an admission of great weakness and by our allies as a clear indication that we intended to abandon them."\textsuperscript{23} Allies’ belief in US willingness to use nuclear weapons to head off an adversary invasion convinced these states they did not have to become nuclear powers themselves (serving a secondary purpose of shoring up the NPT).

This argument is less of a factor for cyberspace, where extended cyber deterrence has no empirical precedence and allies rely on conventional or nuclear weapons (not cyber attacks) to dissuade adversaries from launching invasions. As discussed previously, emerging work on cyber operations and deterrence suggests that cyber operations are, more often than not, poor tools for deterrence success.\textsuperscript{24} Therefore, restraining strategic cyber attacks’ first use does little to decrease immediate deterrence success and even less to impact extended deterrence.

Finally, the United States does not have the same concerns about allied proliferation in cyberspace as it does in the nuclear domain. Cyber capabilities are not restricted to a handful of states (as in the nuclear case), and arms control arrangements within cyberspace are non-existent to date. Absent these mechanisms, dissuading allies from using cyber attacks against enemy civilian or nuclear infrastructure is more likely to result through credible conventional military alternatives or significant changes to international norm about appropriate behavior.

\textbf{Credibility}

Second, there was the overarching concern that, even if the United States were committed to an NFU policy for nuclear weapons, when stakes were high, no adversary would believe the US NFU policy. NFU would therefore erode US strategic options without necessarily providing any benefits in assuring adversaries.

Could a US cyber NFU policy be credible? Here is where there may be significant similarities to the credibility problems of a nuclear NFU policy. It is difficult to look at what cyber accesses or weapons (exploits) are being developed within a country, and there is little intervening process between the development of a cyber exploit (to be used in retaliation to a first-use attack) and the actual use of that exploit. In cyberspace, warheads do not need to be mated; launchers don’t need to be mobilized. The movement between development and use in cyberspace is not much more than a few clicks of the keyboard. This ability to quickly conduct an attack without the intervening variables of major visible weapons
movements makes it difficult for the United States to signal to states that it has created a sincere internal mechanism for restraint.

However, there is something fundamentally different about cyberspace that also makes the potential for US cyber NFU credibility more likely than the nuclear case. Nuclear use has occurred only twice, and both times by the United States in the context of WWII. Therefore, nuclear intentions and predictions about whether a state will use nuclear weapons first are based solely on proxy variables, like what types of weapons a state develops, their doctrine, or notional beliefs about decision-making. These clues help signal whether a state is actually implementing its nuclear NFU policy, but it also leaves a lot up to interpretation.

By contrast, operations in cyberspace occur more often and between significantly more actors. This difference means that non-strategic attacks in cyberspace are occurring constantly from a wide array of state and non-state actors. The United States’ response to these attacks, including restraining the use of strategic cyber attacks with violent effects against civilians, builds an empirical precedent of restraint that makes a declaratory policy much more credible in cyberspace than it can ever be in the nuclear case.

Survivability
Third, the fear that the United States would not be able to survive a nuclear attack to conduct a second salvo has kept it from adopting a nuclear NFU policy. If the United States were unable to survive a first counterforce nuclear strike, then an NFU policy would make the US nuclear inventory essentially useless.

The same logic does not work for cyberspace. Cyber attacks do not have the same physical consequences as nuclear attacks, and no state has demonstrated an ability to launch a counter-force cyber attack that cuts off all long-term ability for a state to conduct a cyber attack. The United States would almost certainly retain capability to conduct punishment against a strategic cyber attack in the conventional or nuclear domains. Even the most dangerous scenario—a cyber attack that degraded US ability to control its nuclear forces—would risk a nuclear retaliation from a pre-delegated second-strike force. In all but the worst nuclear scenarios, the United States would survive a first-strike strategic cyber attack; adversaries would have to be ready for a potentially dangerous cross-domain retaliation from the United States.

Asymmetric Weakness
Concerns about asymmetric weakness during the Cold War were about counter-force—would Soviet nuclear attacks defeat US nuclear forces before they could be launched? For cyberspace, the main concern is about counter-value. The United States asymmetrically benefits from a digitally enabled economy and
society with a free and open internet, making it asymmetrically vulnerable to strategic cyber attacks against its civilian population.

By contrast, states like Russia and China benefit from a closed-off and divided internet. They build technical and societal walls to control and protect their information. The United States has made a strategic choice to privilege digital capabilities over cyber protectionism, and therefore it will always lose in a cyber counter-value fight. Therefore, cyber NFU may be a strategic choice to try and incentivize others to exercise restraint at the strategic level so the United States can negate its own inherent disadvantage and its adversaries’ superior strategic cyber power.

**Leading in Cyber Space: Being a Norm Entrepreneur**

A strategic cyber NFU policy on violent strategic cyber attacks against civilians, as well as attacks that keep a country from controlling its nuclear arsenal, can be an effective solution for the United States to maintain its two cyber thresholds. The key to this policy’s ultimate success is in its ability to solve the US hypocrisy problem—to credibly convince other states that the United States will restrain itself in cyberspace while it simultaneously conducts counter-cyber operations on a day-to-day basis. The implementation of a declaratory cyber strategic NFU attack policy is a first step to solving this two-threshold problem, but the policy will be even more successful if the United States pairs the statement with a series of actions and engagements to incentivize policy adoption.

The literature on norm entrepreneurship suggests that norms—like strategic cyber restraint—are most likely to be adopted when states are able to incentivize, persuade, and socialize across the organizations that lead the culture (in this case, the cyber culture) of adversary and allied states. These organizations include not only heads of states or official diplomatic representatives, but also military cyber organizations, intelligence communities, and non-state entities.

For the United States, therefore, a strategic cyber NFU policy needs to be incentivized through positive means—like information sharing, foreign aid, or transfers of cyber/military capabilities to other participating NFU nations—and deterred through credible cross-domain punishment. The United States cannot just incentivize others, especially since strategic NFU advantages the US internet and system of digital governance. It must also persuade, presenting a unified and coherent narrative about strategic
restraint and the normalization of counter-cyber operations through track-series negotiations, inter-agency cyber meetings between the United States and its top adversaries and allies, and outreach with both international citizens and top technological companies. The United States needs to socialize its two-threshold strategy through continued discussions through the UN Group of Governmental Experts (UN-GGE)—the most established international diplomatic exchange on cybersecurity, as well as through other traditional security alliances and institutions.

Finally, the United States will have to recognize that the success (or failure) of this scoped strategic cyber NFU policy is not based on an overall decrease in cyber attacks or operations. It is also not in assessing the economic cost of cyber attacks on the United States or in the ability of the United States to conduct conventional military operations. Instead, dealing with these threats is the job of cyber defense, resiliency, defend-forward, and cyber campaigns against militaries within conventional armed campaigns.

Strategic cyber NFU is about encouraging restraint of cyber attacks against civilians or nuclear forces so that the United States can contest adversary cyber capabilities without concerns about violent retaliation for defend-forward operations. It is about shoring up strategic deterrence and creating norms of restraint at the highest level of cyber attacks to decrease the incentives for the most dangerous and destabilizing attacks. Therefore, its success will be measured both by the lack of strategic cyber attacks against US civilians or nuclear forces and by the ability of the United States to conduct counter-cyber defend-forward operations without leading to escalation outside of the cyberspace domain.

Notes


