Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics

Sarah Kreps and Jacquelyn Schneider

1 Political Science Department, Cornell University, 313 White Hall, Ithaca, NY 14853, USA
2 Hoover Institution, Stanford University, 434 Galvez Mall, Stanford, CA 94305, USA
*Corresponding author: E-mail: jackie.g.schneider@gmail.com

Received 28 March 2019; revised 12 June 2019; accepted 21 June 2019

Abstract

Despite the growing literature on cyber security, most studies have sidestepped important questions of how conflict escalates in the cyber domain. To better understand this dynamic, we advance two main theoretical pathways of escalation, one in which actors respond with increasing intensity based on the effect of an attack, irrespective of how it is conducted (through cyber, conventional, or nuclear) and another in which the means of attack determines the actor’s willingness to escalate. We then test those effects- and means-based pathways with an original experiment that probes support for escalation, focusing on the American public, a key actor in debates about nuclear escalation and deterrence. Our study suggests that cyberattacks create a threshold that restrains the escalation of conflict. Americans are less likely to support retaliation with force when the scenario involves a cyberattack even when they perceive the magnitude of attacks across domains to be comparable. Our findings provide support for cyber strategies based on assumptions of cyber thresholds, while also casting doubt on the credibility of cyber deterrence by punishment. More broadly, our research suggests effects-based theories of escalation may not help understand the impact of emerging technologies on strategic stability.

Key words: Escalation; kinetic operations; deterrence; public opinion

In 1965, Assistant Secretary of Defense Alain Enthoven declared that there was “an important distinction, a ‘firebreak’ if you like, between nuclear and non-nuclear war, a recognizable qualitative distinction that combatants can recognize and agree upon.” Enthoven explained that, “As time goes by and the size and destructive power of nuclear arsenals increase, total war between nuclear powers will more and more mean total destruction” [1]. Enthoven, as many academics and foreign policy decision-makers after him, believed nuclear weapons were different from other means of warfare. They represented a higher rung in the conflict escalation ladder that, barring some unforeseen existential threat to the USA, should or would not be climbed.

The belief in nuclear restraint has received extensive attention in the academic literature [2–7]. There is, however, a puzzle within Enthoven’s statement on nuclear firebreaks that speaks more fundamentally to the logics of conflict escalation across domains of warfare, with particular implications for cyberspace operations. Enthoven’s belief in restraint hinged upon the idea that nuclear weapons were likely to create total destruction. It was not nuclear weapons on their own that were different from other means of warfare, but instead the effects nuclear weapons could create. Later debates, including those regarding the use of tactical nuclear weapons, questioned the effects-based logic undergirding Enthoven’s nuclear firebreak. Policy-makers and military planners doubted whether much smaller nuclear weapons could be used without leaping rungs in the escalation ladder, which produced a new set of debates about whether restraint was based on the effects of nuclear weapons, in which case tactical nuclear weapons might now seem permissible, or the means, in which case even tactical nuclear weapons would seem off limits [8, 9].

While this question of effects versus means in escalation is not new, the development of cyberspace operations—which may create
...effects as innocuous as website defacement to those as catastrophic as nuclear meltdown—pose a particularly interesting comparative case for testing Enthoven’s effects-based logic of nuclear firebreaks. Like nuclear weapons, cyber weapons are often categorized as strategic weapons, capable of coercing and deterring by threatening large civilian populations. In fact, the nuclear analogy has been used extensively within academic literature and policy to understand the dynamics of cyber escalation [10, 11]. Perhaps more importantly for comparing the logic of firebreaks across domains, a burgeoning body of research suggests that—like nuclear weapons—the saliency of cyberspace operations may uniquely define perceptions of escalation above and beyond the effects created by cyberspace weapons [12–14]. That cyber domains are qualitatively different would suggest that escalation can be defined just as much by the means used to create effects as the effects themselves. If so, then the logic is subtly different from Enthoven’s logic and suggests that means-based understandings of escalation dynamics embedded in normative and psychological accounts of conflict may be increasingly important to understanding the role of emerging technologies in modern warfare [4, 16, 17].

Further, the introduction of new US cyber strategies makes the issue of cyber firebreaks especially relevant. The 2018 Cyber Command Strategic Vision, e.g., argues for a new strategy of persistent engagement to combat adversaries that “operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantage” [18]. Meanwhile, the US Department of Defense Cyber Strategy introduced a new concept of defend forward, the goal of which was “to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict” [19]. Neither of these documents, which debuted preemptive and ongoing cyber operations as a key to strategic success, explicitly discussed the risk of escalation and instead hinged upon a firebreak assumption that cyber operations could and would operate under the thresholds of conventional armed conflict.

Building on the nuclear analogy, a common point of departure for many decision makers discussing the cyber domain, we advance two possible logics of cyber escalation. The first is a means-based logic, which would suggest that cyber domains are qualitatively different from conventional or nuclear, in which case escalation can be defined more by the means used to create effects than the effects themselves. Alternatively, we examine a logic of effects, in which cyberspace operations can exist under the threshold of armed conflict either because cyber does not produce impacts that would provoke escalation or does only if it produces kinetic effects commensurate with those within the conventional or nuclear domains, a logic that converges more closely with Enthoven’s effects-based firebreak.

To test the two logics of means and effects, we conduct an original experiment that probes public support for escalation. The experimental design varies the means of attack (cyber versus conventional versus nuclear), and three sets of effects, and consequences: treasure (economic costs); blood (loss of life); and nuclear (radiation). By holding effects constant, we seek to isolate how the effect versus the means of attack impacts public support for retaliation and explore the logics behind escalation firebreaks across domains of warfare. We focus on the American public, given its prominence in debates about nuclear escalation and foreign policy more generally [20–23], and the theoretical expectation that bottom-up influences are likely to be even more salient in the cyber domain, which lacks clear rules of engagement or elite consensus on what constitutes an “act of war” [24].

We find that individuals are far more reluctant to escalate in the cyber domain than for the corresponding conventional or nuclear attack. Indeed, the public exhibits far more caution when it comes to responding aggressively to cyber conflict than either conventional or nuclear. The finding provides strong support for the means-based argument; cyber is perceived as qualitatively different in ways that create a clear firebreak between cyberspace and either conventional or nuclear domains. That the public exhibits an unwillingness to escalate in cyber even for consequential attacks supports the persistent engagement strategy but also erodes the foundations of cyber deterrence, which would rely on the threat and execution of inflicting damaging costs in retaliation to a cyberattack [25–28].

...
As Joseph Nye asserts, “escalation ladders and thresholds are integrated processes of reasoning and experience in which existing concepts of non-use such as deterrence or the nuclear taboo are developed theoretically and upheld as beliefs that rule action in practice” [48].

Cyberspace escalation: a firebreak analogy?

The perseverance of the firebreak has come to define nuclear strategy, especially for the United States. It is also increasingly central to debates around US cyber strategy. Therefore, as critics of the persistent engagement strategy argue, understanding the logics of cyber escalation is vitally important to the strategy’s success [49–51]. Despite the importance of escalation for current US cyber strategy success, there is very little scholarly consensus about cyber escalation. As Joseph Nye asserts, “escalation ladders and thresholds are poorly understood” in the cyber realm [66].

A number of scholars and policymakers argue that cyber operations do not change the fundamental nature of escalation. For these scholars, it is the effects created by weapons that matter for escalation and not necessarily the means or the domain in which the effects are created. Cyberspace operations may have unique qualities, but the fundamental logics of escalation are tied to weapons’ effects and rather than how these effects are delivered. As long as cyberspace operations can create similar effects as operations in other domains, they create the same escalation ladders. The debate within this literature is about the technical ability of cyberspace operations to create the same effects as the other domains [56, 59, 60, 62, 67, 68]. Kostyk et al., e.g., equate permanent damage to civilian infrastructure as the cyber equivalent of a nuclear war and existential attack, all of which should warrant a comparable escalatory response. They caveat that “at present, we do not believe a single mode of cyber attack alone would pose an existential threat to the US, however, this may change in the near future” [69].

Scholars within this line of reasoning devote significant attention to understanding the difficulty cyberspace operations have achieving access, the resources required for creating complex effects, and the highly-reversible nature of most cyberspace operations. Glaser and Farrell provide an effects-based typology and point to five characteristics of effects that may decrease escalation of cyberattacks: physical versus nonphysical damage (first- or second-order physical effects), no visible damage, military versus civilian, attacks that kill versus those that do not, and attacks in war versus peace [13]. According to this understanding of cyberspace and escalation, responses to a cyberattack should not be qualitatively different from any other attack as long as cyberattacks can advance to the level of nuclear or large-scale conventional capabilities [57, 59]. Until cyber-space attacks can provide the decisive edge toward taking territory or create the lethal effects comparable to large-scale or nuclear war, they will not be treated the same as attacks in other domains. The perspective is largely consistent with Valeriano and Maness’s quantitative analysis of cyberspace operations, who find cyber operations to be largely low intensity and find no evidence of higher intensity retaliation to cyber attacks [69].

In contrast to those who believe that cyberspace escalation is effects-based, a second set of arguments focuses on the qualitative importance of the means of cyberattacks, arguing that the way in which cyberspace operations deliver effects (often covert, virtually, and usually with second or third-order effects) makes the means find a willingness to use these weapons if they are seen as more effective mechanism of counterterrorism or counterproliferation, for example.

1 Brodie’s assertion that the firebreak theory has become stronger over time has not gone unchallenged, including policy debates about the use of tactical nuclear weapons within the Trump Administration’s Nuclear Posture Review as well as recent research by Press et al. and Sagan and Valentino that questions the public’s taboo against nuclear weapons and
of attack less likely to trigger escalation than attacks conducted from the conventional or nuclear domains. Glaser and Farrell allude to this possibility for escalation and cyberspace attacks, concluding that “It could result from the belief that cyber attacks and kinetic attacks are fundamentally different in kind, such that one is considered fundamentally acceptable, and the other is considered non-acceptable. If this were generally accepted, then the effects-based doctrine that we outlined initially would be more or less useless, since it would be undermined by an understanding that there is a crucial qualitative difference between cyber and kinetic weapons” [70].

Evidence suggests that Glaser and Farrell’s concern about an effects-based logics is warranted. In a study of crisis war games, Schneider finds that across six years of games US decision-makers chose not to retaliate to cyberattacks. Discussion about decisions during the game suggests that players did not view the cyberattacks within the same psychological frame as conventional or nuclear attacks. In one of the games, Schneider recounts an interaction between the cyber player and the team lead:

Cyber briefs that adversary has conducted ‘very escalatory’ destruction of the blue homeland C2 nodes. BLUE LEAD says “we need to have discussion about how we treat cyber attacks versus kinetic attacks.” CYBER feels this is nearly kinetic...like bombing our C2 tower. BLUE LEAD says it is different psychologically [71].

If cyber represents a firebreak analogous to the difference between nuclear and conventional, then we would expect that actors would hesitate before escalating from the cyber domain to anything kinetic, whether conventional or nuclear irrespective of the nature of the hostile act.

**Escalation ladders: the role of the public**

There are many ways in which escalation occurs, both inadvertently and deliberately. We bracket inadvertent escalation—since it implies a stochastic element of miscalculation rather than actor intentionality—and focus on deliberate escalation, which “occurs when the actions of a state (or other actor) cross an escalatory threshold in a conflict or a confrontation more or less intentionally. The results may not be precisely as expected, but, at least in broad terms, the decision includes recognizing that the action under consideration could or will be escalatory and deciding that, in spite of—or because of—this, it is worth doing” [72]. Central to understanding deliberate escalation dynamics, and particularly the role that cyber operations could play in escalation, is identifying the cyber-space actions states believe are significant enough to require responses across domains, with greater violent intensity, or across geographic locations. For our purposes, we are interested in understanding the point at which populations support retaliation to cyber operations with kinetic conflict [74].

Public opinion has always featured prominently in debates about the deliberate escalation of conflict. Democratic governance relies on support from the polity. For decades, scholars believed that the public was either too capricious or irrelevant to constrain leaders’ decisions about the use of force. Especially since Vietnam, which made manifest the electoral perils of acting contrary to public opinion—most salient of these being President Johnson’s decision not to seek re-election—the conventional wisdom has taken as a given the importance of public support and shifted to a discussion of which features the public weights most heavily [75–77]. With blood and treasure at stake, the public has both an interest in the decision to go to war and the intensification of war, and leaders, whose electoral and policy fortunes are intertwined with public attitudes, have incentives to heed those preferences [23].

Despite the importance of public opinion in foreign policy in general, and the reasons to take it seriously in cyber in particular, the literature on public opinion and foreign policy not yet engaged the new domain of cyber conflict [78]. Instead, the cyber literature has tended to focus on questions of international law [79], attribution [80], and deterrence [81], while disregarding the intersection of these two fields to investigate the public opinion context in which decisions about retaliation would take place. One exception is a study that evaluated individuals’ support for airstrikes when a cyberattack had kinetic versus nonkinetic impacts, but it did not compare across domains, making it impossible to understand whether individuals think differently about escalation in cyber compared to if the same effects were perpetrated by a conventional or nuclear weapon [14].

Finally, understanding the American public’s support for retaliation is an under-theorized part of the current strategies. These strategies hinge on not only the USA ability to keep adversaries from escalating beyond the cyberspace domain, but assumes that adversary cyber operations largely exist under the threshold of what the US population is willing to respond to. Is this true? How high is the US population’s threshold to withstand these cyberattacks?

**Research design**

To evaluate whether the public’s attitudes about escalation are predicated on an effects-based or means-based escalation ladder, we carried out an experiment that tested whether individuals responded fundamentally differently to a cyberattack compared a conventional or nuclear attack. Our baseline scenario involved a foreign attack “a power plant that supplies a major American city.” The experimental design varied the means through which an attack was carried out—through cyber, conventional, and nuclear—and the effects of those attacks—treasure (economic cost), blood (casualties), and nuclear (radiation). In terms of the cyber vehicle, we noted that “the country’s government hacked into the computer networks that control the power plant’s critical system and caused a key safety control mechanism to fail.” The conventional means also involved attacking the power plant but through aircraft that intentionally crashed into the facility “to cause damage to the plant.” The nuclear attack scenario entailed using a nuclear device to cause damage.

The second set of parameters varied the consequences of those attacks. In the treasure scenario, we noted that “the attack produced massive economic damage because of disruptions to the power grid, including power outages to residences and businesses, the need to rebuild the plant’s data systems, and losses in the stock market.” In terms of blood effects, we indicated that the attack had caused “significant casualties because of disruptions to the power grid,

---

3 Inadvertent escalation operates by a different mechanism, one in which an actor unintentionally crosses a threshold by miscalculating the other side’s willingness to retaliate [73].
4 The experiment was conducted through the Amazon Turk (Mturk) labor market between 4 and 8 August 2017 (See Online Appendix for additional detail on the experimental design, including theoretical trade-offs.) A number of scholars have found that treatment effects are similar for Mturk as for many other subject pools, including the in-person convenience samples that are typical for political science papers. On the use of mechanical turk, see [82].
including power outages in hospitals, residences, and nursing homes.” We then suggested that the attack had “produced a significant nuclear hazard because of a meltdown at the reactor, radiation in the air surrounding the facility, and contamination of local water.”

We attempted to keep as much of each scenario the same as possible, but acknowledge that readers may attribute more significant effects for the nuclear vehicle than conventional or cyber. In other words, it might be improbable for respondents to think that the effects of a nuclear attack would be limited to treasure, e.g., or even blood, without causing fallout. To deal with this problem, we provide respondents with information about the main effects of the attack. Moreover, in the scenarios that involved nuclear devices but did not have primarily nuclear effects (i.e. the blood and treasure scenarios), we specified that “no immediate nuclear fallout was caused by the attack.” This statement acknowledges that the nuclear vehicle may be seen as fundamentally different from the others, and actually creates a bigger challenge for retaliation support due to a nuclear effect since it prompts respondents to exclude nuclear as the primary effect for treasure and blood.

Following the scenario, we asked a number of questions. Our main dependent variable involved support for a range of retaliatory measures. We randomized responses including diplomatic threats, economic sanctions, cyberattacks, airstrike with drone, airstrike with manned aircraft, cruise missile strike, nuclear attack, and ground invasion. We also asked individuals to assess the magnitude of the particular strike both to assess whether individuals did attribute greater gravity to the effects, even within the same type of effect, and to see whether the perceived magnitude or the type of strike (cyber, conventional, or nuclear) was more consequential for individuals’ support for increasingly aggressive retaliatory responses. To gauge whether the perceived magnitude of a strike affects support for the use of force, we ask individuals to rank on a scale of 1–10 the degree of threat to the nation’s security. Finally, while we used a hypothetical attacker for the purposes of greater generalizability, it is possible that individuals make assumptions about the identity of the country in ways that would affect responses about retaliation. We therefore asked individuals whether they associated the scenario with a particular country and then assess the effect on support for retaliatory measures.

**Results**

Our analysis points to a firebreak between cyber and both conventional and nuclear domains. It reveals that controlling for the effect, individuals respond systematically different for attacks in the cyber domain compared to either of these other two domains. In other words, they do not treat cyber “like any other attack” and are considerably more restrained when it comes to aggressive retaliatory actions involving the use of force.

Figure 1 illustrates support for one of the most likely forms of aggressive retaliation, the use of airstrikes. Grouping the responses by the category of effect caused by the attack—impacts to treasure (financial), blood (casualties), and radiation (nuclear)—reveals the stark differences between the cyber domain and either conventional or nuclear. For no type of effect did the cyber scenario reach a majority of support (over 50%). According to Gilens [83], the relationship between public opinion and policy impact is S-shaped, with a key inflection point for public influence is around 50%, such that small changes in public opinion around that level have a comparatively large policy impact compared to either much higher or lower levels of support. Page and Shapiro similarly find that support around this level increases the likelihood that official policy will become more congruent with public sentiment [84]. Interestingly, support for airstrikes in the conventional and nuclear domains was over a majority irrespective of the nature of consequences.

Figure 2 shows the increase in support across all retaliatory measures, using the cyber conditions as a baseline; thus, it compares conventional with cyber and nuclear with cyber. As the figure illustrates, the perpetration by either a conventional or nuclear weapon—controlling for the same average effects—makes individuals less inclined toward the more modest retaliatory measures such as diplomatic or cyber response. It makes them far more willing to use aggressive measures such as airstrikes, drone strikes, special operations forces, invasion, and cruise missile strikes. Only in the nuclear domain did a nuclear response achieve statistically higher support (conventional relative to cyber did not). Otherwise stated, cyber significantly dampened bellicosity relative to either conventional or nuclear, holding the effects constant.

Although our instrument did not explicitly test the mechanism for why individuals were more reluctant to retaliate in the cyber domain than either conventional or nuclear, we did ask open-ended responses that shed light on the distinctions. A number of individuals who supported retaliation for cyber did cite the need to respond aggressively to deter future attacks. For example, one individual responded that “if the country is attacked then we must retaliate to deter further attacks,” while another respondent simply stated “deterrence” as the basis for retaliating, dovetailing on a related comment that “to be compliant would just encourage more of the same cyber behavior,” or that “if you do nothing then the attack can happen again.” This line of response that “a cyberattack in this manner is very similar to a

![Figure 1. Support for airstrikes across effect and domain.](https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971)
traditional military strike” and demands a commensurate response is consistent with official US cyber policy. It was also the minority view among respondents who received the cyber treatments.

More common was a “desire not to escalate” and the fear that an aggressive response would create higher costs and “worsen the conflict.” Many of the respondents who received the cyber treatments emphasized the need for diplomacy or sanctions, and that they did not condone violence that could start “a global war.” For some respondents, the basis for inaction was explicitly because cyber is qualitatively different domain that requires a more muted response. According to one respondent, “a cyber attack should have a non violent response.” Another pointed to the uncertainty underlying attribution, suggesting that “just barely knowing the cyber attack origin is not enough merit to take any action other than more investigation.” Although these assertions are anecdotal, they do offer suggestive evidence of cyberspace attacks’ qualitative difference in the minds of our survey respondents.

Next, we consider how the nature of the attack’s consequences affects support for the array of retaliatory measures. As Fig. 3 shows, an attack that produces nuclear fallout increases support for retaliating with drone strikes, cruise missile strikes, special operations forces, and ground invasion as the dependent variable, the conventional and nuclear scenarios are statistically more likely to produce support than the comparable cyber scenario.

Beyond the main independent variables, we also control for other factors that could affect individuals’ support for retaliatory measures (see Table 1). Whether an individual is hawkish (“to what extent do you agree that the use of military force usually makes problems worse”) is a strong predictor of support for aggressive retaliatory measures such as airstrikes or a nuclear strike, as might be expected. People who are older and male were more likely to support a range of retaliatory responses for both the effects- and means-based scenarios. Education had a strong effect in terms of support for diplomatic measures in response to strikes that had economic effects (for both effect and means). The perceived magnitude of the attack affected only the kinetic retaliatory responses, suggesting that the perceived gravity of the attack had a strong effect on individuals’ willingness to respond aggressively to an attack. Separately, we interacted the perceived magnitude of attacks with the treatments and found that it had no statistically significant effect on the propensity for supporting aggressive retaliatory measures.

While we opted to anonymize the country name so that the findings would be more generalizable beyond a specific country, we entertained the possibility that individuals might nonetheless be inclined to associate the scenario with a particular country. In a follow-up question, we asked whether individuals thought about a specific country as the hypothetical attacker, and if so, which country? The plurality of respondents (43%) did not think of a specific country, whereas 38% responded North Korea, compared to 5% for Iran, 3% for Russia, and 10% for China. In the table above, we distinguished between advanced nuclear weapon countries (ANWC) that have the capability to strike the USA, which includes Russia and China, and those that do not.”

Figure 2. Effect of conventional and nuclear relative to a cyber baseline, and with respect to the full range of retaliatory responses (95% confidence intervals shown).
effect and domain. As the table shows, any assumptions about whether the perpetrator was an advanced nuclear power did not affect support for any of the retaliatory measures, and did not condition willingness to respond across the two sets of factors (effects and means). That the presumed identity had no effect on respondents’ attitudes about retaliation validates the decision to use a hypothetical country although further research might investigate specifically whether nonnuclear perpetrators are associated with a higher willingness to retaliate, since its capacity to deter would be lower.

Having uncovered evidence that responses to cyber operate differently from other domains, we investigate the possibility that the relative unwillingness to take aggressive retaliatory actions in the cyber domain compared to either conventional or nuclear, holding effects constant, was driven by features of the instrumental design. In other words, while we were attentive to the internal validity of our instrument—working to ensure that the treatments varied only the nature of the consequence (i.e., treasure versus blood versus nuclear fallout)—it is possible that individuals made assumptions about the treatments that went beyond those that were intended. For example, they may have assumed that the treasure scenario for a nuclear device also resulted in casualties, which would have an impact our ability to draw clean inferences about how the effect and
domain affect retaliatory responses. We therefore evaluated, again using cyber as the baseline, whether those in the conventional or nuclear scenarios had, on average, higher assessments of the magnitude of the strike. While respondents who received the nuclear scenario did associate the strike as having a higher magnitude, perceptions of the conventional versus cyber are statistically indistinguishable on average, suggesting that differences in attitudes about retaliation are not informed by perceptions of whether the attack was greater in magnitude, but because of attitudes about the domain itself.

Figure 4 illustrates this dynamic in the context of one particularly salient retaliatory measure, the use of airstrikes. It shows that the perceived magnitude of conventional strikes had no statistically significant difference compared to cyber strikes, yet the support for airstrikes was almost 23% higher compared to the base levels of support for cyber, a difference in support between 34% for cyber and almost 57% for the equivalent attack perpetrated by a conventional weapon. The differences between nuclear and cyber vary, as might be suspected, more uniformly across magnitude and support for airstrikes, with the nuclear strike increasing the perceived magnitude by about 49% compared to cyber, and support for airstrikes increasing by about 25% compared to the baseline of cyber.

We also consider that the means through which an attack takes place causes individuals to assume that the corresponding response will be proportional. If they were assuming, e.g., that a nuclear-based attack would produce more aggressive retaliatory responses, individuals might be registering attitudes less about the means of attack than concern about taking aggressive action. To ensure that individuals were not influenced by their assumptions about the magnitude of likely responses, we compared responses across domains to the question about how aggressive an action they viewed each retaliatory measure. We examined whether the responses to that question—the degree of aggressiveness they associate with a particular retaliatory action—depended on the means. The table above includes a sample of retaliatory responses, with differences between cyber and either conventional or nuclear as the basis of comparison for ranking the perceived aggressiveness of the retaliatory responses. In no case did individuals perceive the aggressiveness of a response as statistically different depending on the means, which suggests that they are unlikely to be conditioning their support for a response on its proportionality to the means (rather than the means itself, as we have argued).

### Conclusion

Is there a cyber firebreak, and is it related to means or effects? Our study suggests that Americans’ propensity for escalatory responses to cyberattacks cannot be explained solely by the effects created by attacks. Just as other scholars have argued that a nuclear firebreak exists, it appears that a cyber firebreak exists at the bottom of the escalation ladder. According to our experimental findings, cyberattacks create a threshold that restrains the escalation of conflict. For the American public, cyberattacks are qualitatively different than those of similar magnitude from other domains. They are statistically less

### Table 1. Logistic regression analysis with for retaliatory measures as the dependent variable

|                | Model 1 (economic) | Model 2 (airstrikes) | Model 3 (nuclear) | Model 4 (economic) | Model 5 (airstrikes) | Model 6 (nuclear) |
|----------------|--------------------|----------------------|-------------------|--------------------|----------------------|-------------------|
| Cyber          | −0.19 (0.17)       | −1.00 (0.19)***      | −1.37 (0.29)***   | −0.36 (0.19)*      | −0.33 (0.27)         |
| Conventional   | −0.05 (0.18)       | −0.05 (0.19)***      | −1.28 (0.29)***   | −0.14 (0.18)       | −0.27 (0.27)         |
| Nuclear        | Treasure           | 0.26 (0.18)          | −0.36 (0.19)*     | −0.33 (0.27)       |
|                | Blood              | 0.26 (0.17)          | 0.14 (0.18)       | −0.27 (0.27)       |
|                | Radiatiation       | 0.15 (0.45)          | −0.01 (0.45)      | −0.15 (0.45)       |
|                | ANWC (Offense)     | −0.12 (0.62)         | −0.59 (0.63)      | −0.12 (0.62)       |
|                | ANWC X Cyber       | 0.45 (0.53)          | −0.68 (0.55)      | 0.45 (0.53)        |
|                | ANWC X Nuclear     | −0.12 (0.62)         | −0.59 (0.63)      | −0.12 (0.62)       |
|                | ANWC X Treasure    | −0.46 (0.46)         | 0.05 (0.48)       | −0.22 (0.76)       |
|                | ANWC X Blood       | −0.37 (0.56)         | −0.75 (0.56)      | −0.98 (1.16)       |
|                | ANWC X Radiation   | 0.49 (0.14)***       | 0.91 (0.15)***    | 0.39 (0.23)*       |
|                | Male               | 0.00 (0.03)***       | 0.11 (0.06)***    | −0.27 (0.09)**     |
|                | Age                | 0.20 (0.06)***       | 0.10 (0.06)***    | −0.07 (0.09)       |
|                | Education          | 0.06 (0.09)          | 0.89 (0.10)***    | 0.63 (0.15)***     |
|                | Party ID           | −0.02 (0.04)         | 0.07 (0.04)**     | 0.17 (0.06)**      |
|                | Income             | 0.00 (0.03)          | 0.08 (0.03)**     | 0.07 (0.06)        |
|                | Magnitude          | 0.06 (0.03)*         | 0.21 (0.04)***    | 0.27 (0.06)***     |
| Observations   | 1052               | 1061                 | 1061              | 1061               | 1061                 |

**P < 0.001, *P < 0.05, *P < 0.1.

### Table 2. Logistic regression analysis with perceived rank of retaliatory aggressiveness as the dependent variable

|                | Model 1 (economic) | Model 2 (drone) | Model 3 (SOF) | Model 4 (cruise) | Model 5 (nuclear) | Model 6 (invasion) |
|----------------|--------------------|-----------------|---------------|-----------------|-------------------|--------------------|
| Cyber versus Conventional | 0.03 (0.21) | 0.21 (0.17) | −0.26 (0.18) | −0.19 (0.18) | −0.16 (0.22) | −0.22 (0.20) |
| Cyber versus Nuclear | −0.15 (0.21) | 0.21 (0.18) | −0.18 (0.17) | −0.07 (0.18) | −0.17 (0.22) | −0.01 (0.19) |
| Observations    | 1052               | 1057            | 1054          | 1046            | 1061              | 1040               |

**P < 0.001, *P < 0.05, *P < 0.1.
likely to support retaliation with force—escalation into a kinetic response—when our scenario took place in the cyber domain. Those differences in support for retaliation are significant even when the perceived magnitudes of the effects of the attack are the same.

Our findings suggest an answer to our initial puzzle about the importance of means versus effects in modern escalation but also introduce new puzzles about the determinants of the cyber reverse-firebreak. What might explain the reluctance of individuals and the American population to respond in cyberspace? What is the mechanism through which the resistance to retaliation for cyberattacks operates? Several factors might come into play. First, although attribution has improved, individuals may have assumed that corroborating a perpetrator would be more difficult, thereby also dampening their willingness to engage in aggressive retaliatory responses. Second, individuals may find the types of kinetic consequences described in the cyber scenario implausible. Cyber is, by definition, virtual. Since it does not create large-scale first-order effects in the same way as an explosive, it creates a cognitive dissonance for individuals considering responses to threats emanating from cyberspace. Individuals cannot fear cyberattacks that lack a physical quality that they have evolutionarily associated with death or existential threat. If cyber creates this cognitive distance, then the cyber firebreak may be as much a product of our constructed understandings of threat as the nuclear taboo.

The findings also raise the question of whether the responses we observed are idiosyncratic to the American public or might they generalize to other countries? On the one hand, the USA is more digitally dependent than most nations, a vulnerability that might have made its public more protective in response to cyberattacks, which might mean other countries’ publics are even less prone to retaliation. On the other hand, the USA retains conventional military superiority and a geographic advantage against any military invasion, which means Americans are willing to absorb some level of cyberattacks both because it always has other capabilities to fall back on and out of a fear that retaliation could escalate into a Pandora’s box of large-scale cyberattacks on US digital capabilities. In any case, further research is warranted to understand whether the US results generalize and which cultural, structural, or institutional factors might condition the public’s propensity for retaliation.

Evidence that the American public is most reluctant to escalate for cyber-based strikes has important implications for theories of escalation in the cyber domain. Since retaliation with force for a cyberattack is unlikely to be popular, it undermines political prospects for escalation from a cyberattack and undermines the effectiveness of cyber deterrence [87]. Relatedly, the findings validate the policy shift toward persistent engagement in cyber, which implies anticipating and deflecting a cyberattack [51]. Deterrence hinges on public resolve for overwhelming uses of force and a willingness to escalate, which appears lacking in the cyber domain, whereas persistent engagement can operate at a lower intensity of confrontation—albeit one that is relatively continuous—that gains legitimacy by virtue of the public support we found in our analysis.

Finally, this exploration focused on the differences and similarities between one emerging technology—cyberspace operations—and nuclear and conventional air strikes. While these findings suggest cyberspace has unique implications for escalation, our study more generally highlights the limits of effects-based escalation theories for modern warfare. As emerging technologies increase the role of machines, remove the human from the battlefield, or increase precision and diversity of effects, their impact on escalation cannot be explained by the physical effects they create. This study therefore highlights the need for greater focus on understanding which qualities of emerging technology may create new rungs on the escalation ladder and incentivize or de-incentivize states to transition crises toward large-scale armed or nuclear conflict.

Supplementary data
Supplementary data is available at Journal of Cybersecurity online.

References
1. Enthoven A. American deterrent policy. In: Kissinger Henry (ed.), Problems of National Strategy: A Book of Readings, New York: Prager, 1965; 123–24.
2. Schelling T. The role of nuclear weapons. In: Ederington L. Benjamin and Mazarr Michael J. (eds.), Turning Point: The Gulf War and U.S. Military Strategy. Boulder: Westview, 1994; 105–15.
3. Gaddis J. The Long Peace: Inquiries into the History of the Cold War. Oxford: Oxford University Press, 1987.
4. Tannenwald N. The nuclear taboo: the United States and the normative basis of nuclear non-use. Int Organ 1999; 53:433–68.
5. Hymans J. The psychology of nuclear restraint. Bull Atomic Scientists 2015. https://thebulletin.org/2015/10/the-psychology-of-nuclear-restraint/.
6. Solingen E. The political economy of nuclear restraint. Int Sec 1994; 19: 126–69.
7. Potter W. The NPT and the sources of nuclear restraint. Daedalus, Winter 2010.
8. McNamara R. The military role of nuclear weapons: perceptions and misperceptions. Foreign Affairs 1983; 62:59–80.
9. Kenny S, Panotsky W. Mad versus nuts. Foreign Affairs 1982; 60:287–304.
10. Nye Jr. Nuclear Lessons for Cyber Security. Montgomery: Air University Press, 2011.
11. Goldman E, Arquilla J. Cyber Analogies. Monterey: Naval Postgraduate School, 2014.
12. Schneider J. The information revolution and international stability: a multi-article exploration of computing, cyber, and incentives for conflict. Ph.D. Diss., The George Washington University, 2017.
13. Farrell H, Glaser C. The role of effects, saliencies and norms in US cyber-war doctrine. J Cybersecurity 2017; 3:7–17.
14. Kreps S, Das D. Warring from the virtual to the real: assessing the public’s threshold for war over cyber security. Res Politics 2017; 4:https://doi.org/10.1177/2053168017715930.
15. Tannenwald N. The nuclear taboo: the United States and the normative basis of nuclear non-use. Int Organ 1999; 53:433–68.
16. Finnmere M. The Purpose of Intervention: Changing Beliefs about the Use of Force. Cornell: Cornell University Press, 2004.
17. Hymans J. The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy. Cambridge: Cambridge University Press, 2006.
18. U.S. Cyber Command. Command Vision for U.S. Cyber Command. April 2018: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010-1.
19. U.S. Department of Defense. Department of Defense Cyber Strategy Summary. September 2018: https://media.defense.gov/2018/Sep/18/2002041658/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
20. Graham T. American Public Opinion on NATO Extended Deterrence and Use of Nuclear Weapons. Cambridge: CSIA Occasional Paper, 1989.
21. Sagan S. Why do states build nuclear weapons? Three models in search of a bomb. Int Security 1996; 21:54–86.
22. Press D, Sagan S, Valentiio B. Atomic aversion: experimental evidence on taboos, traditions, and the non-use of nuclear weapons. Am Polit Sci Rev 2013; 107:188–206.
23. Tomz M, Weeks J. Public opinion and the democratic peace. Am Polit Sci Rev 2013; 107:489–65.

5 In their study, Michael Tomz and Jessica Weeks similarly find public reluctance to retaliate aggressively even in circumstances when the cyberattack has provoked public ire. See [86].
24. Dunlap C. Perspectives for cyber strategists on law for cyberwar. *Strat Stud Q* 2011; 8:1–99.
25. Fischkoffler M, Harknett R. Persistent engagement and tacit bargaining: a path toward constructing norms in cyberspace. *Lawfare*, 9 November 2018. https://www.lawfareblog.com/persistent-engagement-and-tacit-bar-gaining-path-toward-constructing-norms-cyberspace.
26. Healey J. Taking down Russian trolls is my kind of cyber attack. *The Cipher Brief*, 28 February 2019. https://www.thecipherbrief.com/column_article/taking-down-russian-trolls-is-my-kind-of-cyber-attack.
27. Schneider J. Persistent engagement: foundation, evolution, and evaluation of a strategy. *Lawfare*, 10 May 2019. https://www.lawfareblog.com/persistent-engagement-evolution-and-evaluation-strategy.
28. Schneider J, Kollars N. Defending forward: The 2019 cyber strategy is here. *War on the Rocks*, 20 September 2019. https://warontherocks.com/2019/09/defending-forward-the-2018-cyber-strategy-is-here/
29. Morgan F, Mueller K, Medeiros E et al. Dangerous thresholds: managing escalation in the 21st century. Santa Monica: Rand Corporation, 2008, 8.
30. Kahn H. Thinking about the Unthinkable in the 1980s. New York: Simon & Schuster, 1984, 29.
31. Brodie B. Escalation and the Nuclear Option. Santa Monica: The RAND Corporation, RM-4544, June 1965, 104.
32. Tannenwald N. The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. New York: Cambridge University Press, 2007, 2.
33. Glaser C. The security dilemma revisited. *World Politics* 1997; 50: 171–201.
34. Glaser C, Kaufmann C. What is the offense-defense balance and how can we measure it? *Int Security* 1998; 24:44–82.
35. Jervis R. Cooperation under the security dilemma. *World Politics* 1978; 30:167–214.
36. Jervis R. Cooperation under the security dilemma. *World Politics* 1978; 30:172.
37. Brodie B. Escalation and the Nuclear Option. Santa Monica: The RAND Corporation, RM-4544, June 1965; 64.
38. Jervis R. Perception and Misperception in International Politics. Princeton: Princeton University Press, 1976.
39. Jervis R. Deterrence and perception. *Int Security* 1982; 7:3–30.
40. Stein JG. Building politics into psychology: the misperception of threat. *Polit Psychol* 1988; 9:245–71.
41. Levy J. Prospect theory and international relations: theoretical applications and analytical problems. *Polit Psychol* 1992; 13:283–310.
42. Farnham B. Avoiding Losses/Taking Risks: Prospect Theory and International Conflict. Ann Arbor: University of Michigan Press, 1994.
43. McDermott R, Fowler J, Somin O. On the evolutionary origin of prospect theory preferences. *J Politics* 2008; 70:335–50.
44. Tetlock P, Boettger R. Accountability; a social magnifier of the dilution effect. *J Personal Social Psychol* 1989; 57:388.
45. Mercer J. Human nature and the first image: emotion in international politics. *J Int Relations Rev* 2006; 9:288–303.
46. Samuel A, Lumsdaine A, Lumsdaine MH et al. The American soldier: combat and its aftermath. *Stud Social Psychol World War II* 1949; 2:234.
47. Samuel A, Lumsdaine A, Lumsdaine MH et al. The American soldier: combat and its aftermath. *Stud Social Psychol World War II* 1949; 2:237.
48. Sauer F. Atomic Anxiety: Deterrence, Taboo and the Non-Use of US Nuclear Weapons. New York: Springer, 2011; 176.
49. Valeriano B, Jensen B. The myth of the cyber offense: the case for restraint. *CATO Institute Policy Analysis*, no. 862, 13 January 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint?utm_source=RC%20Defense%20Morning%20Recon&utm_campaign=c28bd1616c-EMAIL_CAMPAIGN_2019_01_15_08_47c&utm_medium=email&utm_term=0_69475a8d-c28bd1616c-81835773.
50. Miller J, Pollard N. Persistent engagement, agreed competition, and deterrence in cyberspace. *Lawfare*, 30 April 2019, https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.
51. Smeets M. There are too many red lines in cyberspace. *Lawfare*, 20 March 2019, https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace.
82. Berinsky A, Huber G, Lenz G. Evaluating online labor markets for experimental research: Amazon.com’s mechanical turk. *Political Analysis* 2012; 20:351–68.

83. Gilens M. Inequality and democratic responsiveness. *Public Opinion Quart* 2003; 69:778–96.

84. Page B, Shapiro R. Effects of public opinion on policy. *Am Polit Sci Rev* 1983; 77:175–90.

85. Cirincione J, Wolfsthal JB, Rajkumar M. *Deadly Arsenals: Nuclear, Biological, and Chemical Threats*. Washington, DC: Carnegie Endowment for International Peace, 2005, 121, 166.

86. Tomz M, Weeks JL. Public opinion and foreign electoral intervention. *Changes* 2016; 2019:1.

87. Alexander DUS. Reserves right to meet cyber attack with force. *Reuters*, 15 November 2018.