Check for updates

Research Article

# Warring from the virtual to the real: Assessing the public's threshold for war over cyber security

Research and Politics
April-June 2017: 1–8
© The Author(s) 2017
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/2053168017715930
journals.sagepub.com/home/rap

**Sarah Kreps and Debak Das**

**Abstract**

Accusations of Russian hacking in the 2016 US presidential election has raised the salience of cyber security among the American public. However, there are still a number of unanswered questions about the circumstances under which particular policy responses are warranted in response to a cyber-attack and the public's attitudes about the conditions that justify this range of responses. This research investigates the attributes of a cyber-attack that affect public support for retaliation. It finds that cyber-attacks that produce American casualties dramatically increase support for retaliatory airstrikes compared to attacks with economic consequences. Assessments of attribution that have bipartisan support increase support to a lesser extent but for a broader range of retaliatory measures. The findings have important implications for ongoing debates about cyber security policy.

**Keywords**

Cyber security, public opinion, partisanship

## Introduction

In August 2016, candidate Hillary Clinton told an audience that "As President, I will make it clear that the United States will treat cyber-attacks just like any other attack. We will be ready with serious political, economic, and military responses" (Williams, 2016). The assertion is consistent with a Pentagon task force report from 2013 indicating that a cyber-attack should be regarded "like any other attack," and that the use of armed military force should be considered an appropriate retaliatory action (Defense Science Board, 2013). Despite the apparent agreement, when confronted with Russian meddling in the 2016 United States election, decisions about whether and how to retaliate for any interference were mired in debate both within and across the political spectrum (Sanger, 2016a). While President Obama and prominent Republican Senators such as John McCain and Lindsey Graham called for aggressive measures against Russia, President-Elect, Donald Trump suggested that Russia's role in the attack was unclear and that retaliation was inappropriate (Volz and Schectman, 2016).

Embedded in these emerging debates about how to respond to cyber-attacks are three key considerations. The first is whether victims can ever be certain about the source of attack, which is necessary for retaliation – against whom do they retaliate? Second, what types of attacks justify military retaliation as a state's right of lawful self-defense? Third, under what conditions would the public support retaliation to a cyber-attack? This article engages those three sets of questions by investigating how the first two factors – attribution and the nature of attack – affect the third, public attitudes about retaliation.

It proceeds first by discussing how debates about the intersection between cyber security and the use of force have evolved in the prior decade. Next, it makes an argument for why the public is a relevant yet often overlooked actor in discussions about cyber security, and advances propositions about the circumstances in which the public is likely to favor the use of force in retaliation for a cyber-attack. It then briefly outlines the experimental design followed by a discussion of core findings: assessments of attribution that have bipartisan agreement consistently

Department of Government, Cornell University, Ithaca, NY, USA

**Corresponding author:**
Sarah Kreps, Department of Government, Cornell University, 317 White Hall, Ithaca, NY 14853, USA.
Email: sarah.kreps@cornell.edu

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

increase support for retaliation; whether a cyber-attack produces American casualties dramatically increases support for retaliatory airstrikes; and partisan differences about attitudes toward Russia in general do not carry over into support for particular retaliatory policy options. The article concludes with implications for ongoing debates about cyber security policy.

## Existing cyber security frameworks

The International Committee of the Red Cross defines cyber warfare as "means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict" (International Committee of the Red Cross, 2013). A Department of Defense (2011) memorandum similarly defines cyber warfare as "an armed conflict conducted in whole or part by cyber means…to deny an opposing force the effective use of cyberspace systems and weapons" (Vice Chairman of the Joint Chiefs of Staff, 2010). Cyber-attacks are not explicitly covered under existing laws of war, which took shape in a pre-cyber environment. Indeed, according to one perspective, only an *armed attack* can justify the use of military force, and cyber-attacks do not meet this threshold (O'Connell, 2012: 6).

A competing camp, reflected in US cyber policy, suggests that the law of armed conflict applies in full in this domain. The *Nuclear Weapons Advisory Opinion* by the International Court of Justice reinforces the inherent right of self-defense in response to "any use of force, regardless of the weapons employed" (Ohlin et al., 2015; Schmitt, 2013). The United States' 2011 International Strategy for Cyberspace affirms that the US has "the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with international law" in response to a cyberattack (Hughes, 2016; Obama, 2011). This applies irrespective of whether the perpetrator is a state or a "patriotic hacker" acting on behalf of a state but without its direction since states are implicated if "the person or group of persons is in fact acting on the instructions of, or under the control of, that State in carrying out the conduct" (Mačák, 2016: 3).

Even within the latter camp, questions of when the attack threshold is crossed and how to respond are unresolved. Amidst this ambiguity, the "notion of equivalence" – that an attack will warrant a commensurate response – has increasingly informed the thinking of United States on what constitutes an act of war in the cyber domain (Gallington, 2011; Gorman and Barnes, 2011). According to former legal adviser to the State Department, Harold Koh (2012), kinetic attacks, or "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."

Complicating debates about the appropriate legal framework to apply to cyber-attacks is the question of source attribution, which would be required for a retaliatory strike. Attribution is difficult in large part because online perpetrators can often remain anonymous and networks are complex (Rid and Buchanan, 2015: 7). A second problem is that, as Joseph Nye (2011: 22) suggests, "cyber intrusions that plant logic bombs in the infrastructure may go unnoticed for long periods before being used and, even then, can be difficult to trace." Third, states that have the capacity to carry out a large-scale attack also likely have organizational capacity, technical savvy, and therefore ability to hide their covert operations, including in the cyber domain (Lindsay and Gartzke, 2016).

## The public opinion context

Beyond the unanswered question of retaliation is the political context underlying states' responses to a cyber-attack. As Charles Dunlap (2011: 84) suggests, the threshold for what constitutes an "act of war" that would justify military retaliation is as much political as legal. There are several reasons to expect that the public would be an important consideration in these political discussions. First, public attitudes create political incentives for democratic leaders to make particular choices about the circumstances under which they carry out the use of force. Public opinion, as Leslie Gelb noted in his study of the Vietnam War, was the "essential domino" around which both sides (the US and Viet Cong) based their strategies (Klarevas, 2002: 418).

Second, the process of assessing the attack and identifying attribution would likely take time since "cyber incidents are reviewed on a case-by-case basis" (Murdock, 2016). As such, leaders would have ample opportunity at least to perceive the "public mood" – "the notion that a rather large number out in the country are thinking along certain common lines" – if not read poll numbers themselves (Kingdon, 1984: 153).

Third, the lack of policy agreement and protocol on cyber-attacks would likely open the door to public influence. Lack of consensus would enhance the effect of public opinion insofar "elites may arbitrate between competing views by determining what is most popular" with supporters, with mass attitudes acting to cue elites (Steenbergen et al., 2007: 20).

Fourth, observational data suggest that cyber security is a salient issue for the public. When asked whether individuals see cyber-attacks as a serious threat, 94% of the public indicated that the threat was either very serious (69%) or somewhat serious (25%). A Pew Research survey of a subset of the public – cyber researchers, policymakers, and engineers – found that 61% believed that a major attack that caused "widespread harm" would take place by 2025" (Lee et al., 2014).

While the observational data shed light about the public's attitudes regarding a cyber- attack, they also leave unanswered questions about how the public would react to the questions about attribution and magnitude that are

central to academic debates about cyber warfare and that would inevitably feature prominently in policy debates about whether to use force in retaliation for a cyber- attack.

### *Hypotheses on public attitudes*

Our primary expectation is that the "notion of equivalence" resonates with the public and drives its attitudes about policy responses. In practice, this would mean that individuals' attitudes about retaliation will correspond with the nature and magnitude of the initial cyber-attack. Attacks involving American fatalities (referred to as kinetic attacks) will be more likely to prompt support for aggressive action such as military force than non-kinetic attacks that fall short of having a physical effect. Moreover, within a particular type of attack (kinetic or non-kinetic), larger-scale attacks are more likely to engage US interests, and therefore support for retaliatory action, than smaller-scale attacks (Herrmann et al., 1999: 562).

Our first hypothesis is as follows:

> H1a (non-kinetic/kinetic): Kinetic attacks involving fatalities will generate higher support for retaliation than non-kinetic attacks.
>
> H1b: (scale): Large-scale attacks will generate higher support for retaliation than small-scale attacks.

Second, we expect that uncertainty regarding the source of the cyber-attack will affect how individuals think about retaliation.[1] Individuals tend to have "ambiguity aversion" and are likely to shy away from taking actions in the face of uncertain probabilities (Kahneman and Tversky, 1979). While the tools for judging attribution have improved (Rid and Buchanan, 2015), government officials almost always speak in qualified terms about the perpetrator of an attack. But according to Lindsay (2015: 57), "an unconvincing attribution case, even if nominally correct, can undermine the legitimacy of a retaliatory act in the eyes of skeptics, especially in a democratic constituency." Taken together, we expect the following:

> H2 (Attribution): Higher levels of certainty regarding attribution will increase support for retaliation.

Third, we expect the cyber security issue to be ripe for partisan influence. As Zaller (1992: 100) suggests, the combination of being politically salient and lacking clear precedent in terms of how to respond offer fertile ground for the effect of elite consensus on public attitudes. Indeed, high-profile episodes including accusations of election hacking make it topically relevant. However, it is a relatively new policy issue and even the government is trying to grapple with "a complex calculus" of policy options and their costs and benefits (Sanger, 2016b). Despite legislative leaders arguing that cyber security "cannot become a partisan issue," the polarization that defines the contemporary political landscape suggests that partisan divides are likely on the issue of cyber as well (Kim and Everett, 2016). Thus, to the extent that political elites *agree* on questions of attribution, public support for retaliation is likely to increase (Fandos, 2016; Gajanan, 2016; Hosenball, 2016). We therefore expect the following:

> H3 (Elite consensus): Elite consensus on attribution will increase support for retaliation.

## Research design

We designed a survey experiment to test these hypotheses. Two thousand subjects were recruited from Amazon's Mechanical Turk[2] online labor market and asked about their support for the use of force in response to varying types of cyber-attacks. We used a $2 \times 2 \times 2 \times 2$ factorial design that varied two main parameters, each with two subsets of factors.[3]

The first two varied aspects of the attack itself, which correspond with hypothesis one. The first consisted of the difference between attacks with physical consequences (kinetic) and those that were primarily economic (non-kinetic). In the non-kinetic scenario, the cyber-attack targeted "the computer systems of several of the nation's banks, causing an uncontrolled transfer of funds out of the system." In the kinetic scenario, the cyber-attack targeted "computer systems of several of the nation's nuclear power plants, causing core meltdowns and widespread radioactive contamination." The second consisted of the magnitude of attack. For example, in the smaller-scale non-kinetic attack, "hundreds of Americans had lost $3 billion in savings stolen out of their bank accounts" compared to thousands of Americans who had lost $30 billion. In the smaller-scale kinetic scenario, "hundreds of Americans had fallen ill with radiation sickness and hundreds more had died," compared to thousands who were ill and died for the larger-scale scenario. Although the nuclear scenario was qualitatively different from the banking scenario, these differences were nearly inevitable given that we were testing the effect of American fatalities.

The second two factors varied aspects of attribution, corresponding with the second and third hypotheses. First, we considered degrees of certainty regarding the perpetrator's involvement, suggesting either that the culprit was "probably" or "almost certainly" involved in the cyber-attack.[4] For purposes of external validity, we selected Russia because of its purported involvement in a range of cyber-related activities. Indeed, if we had used a hypothetical country, it is likely that respondents would have associated the action with Russia so we opted for explicitly designating the country as Russia despite the challenges to generalizability. To be sure, Russia's military power and

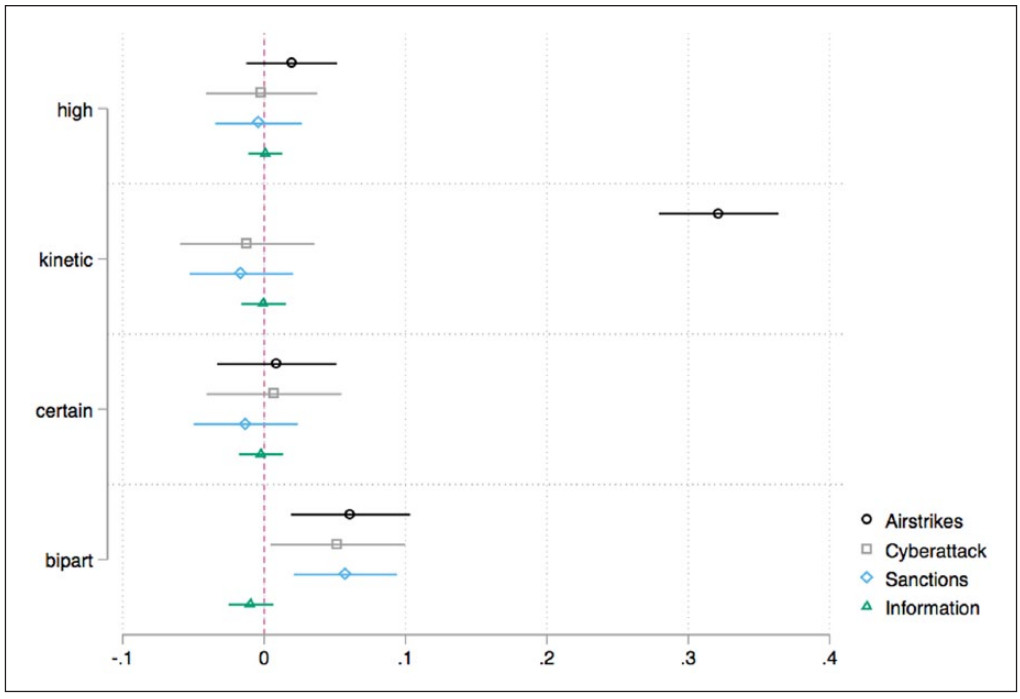


**Figure 1.** Estimated treatment effects for the four main attributes of cyber-attack, along with 95% confidence intervals from ordinary least squares regressions characterizing respondents' reactions to four different policy options.

nuclear status might be more likely to deter a US retaliation compared to a non-nuclear country and conversely a "least likely" case for individuals favoring aggressive retaliatory measures. If we find public support for such measures against Russia, then we might expect it for other less powerful countries as well.

Next, along different lines of attribution, we allowed for the prospect of political contestation regarding the diagnosis. In one condition, "US intelligence officials in the CIA and FBI have said" that Russia is involved, and in a condition implying elite consensus, respondents were told that this is an "assessment that has bipartisan support," whereas the elite dissensus treatment suggested that it "does not have bipartisan support."

To gauge support for different policy responses to the cyber-attack, we randomized four dependent variables. We queried whether individuals would support gathering more information before responding; economic sanctions; a similar cyber-attack against the perpetrator; and air strikes against Russia.

## Results

Figure 1 shows the way in which different attributes of the cyber-attack affected support for the use of force. Each category below compares the key factors that we speculated could affect how individuals think about responding to cyber-attacks, showing attitudes about whether the United States should gather more information, whether individuals would support a similar cyber-attack against the perpetrator, economic sanctions, or airstrikes. Each of the factors is compared with a "baseline," such that high impact is compared to a baseline of smaller-scale attack, kinetic (whether Americans were killed in the attack) versus non-kinetic, whether attribution was almost certain versus probable, and whether the intelligence estimate did or did not have bipartisan support.

As Figure 1 shows, the factor most strongly affecting attitudes about how to respond to the cyber-attack was whether the attack killed Americans or not. For scenarios involving American fatalities, support for airstrikes increased by about 32% compared to when a cyber-attack involves financial costs, although the kinetic scenario had no impact on support for sanctions or a reciprocal cyber-attack.

Whether the assessment had bipartisan support was a consistently important factor influencing support for retaliation, which increased by about 6% for sanctions, a reciprocal cyber- attack, or airstrikes. Whether the impact of the attack was high or low increased support for airstrikes by almost 4%, though this just missed significance at the 5% level. Individuals appeared unable to distinguish between attacks varying just by orders of magnitude.

Despite expecting that the degree of certainty about the attribution would affect individuals' support for particular policy responses, this factor had no appreciable impact, perhaps because respondents are unable to distinguish between "probably" and "almost certainly." Furthermore, it

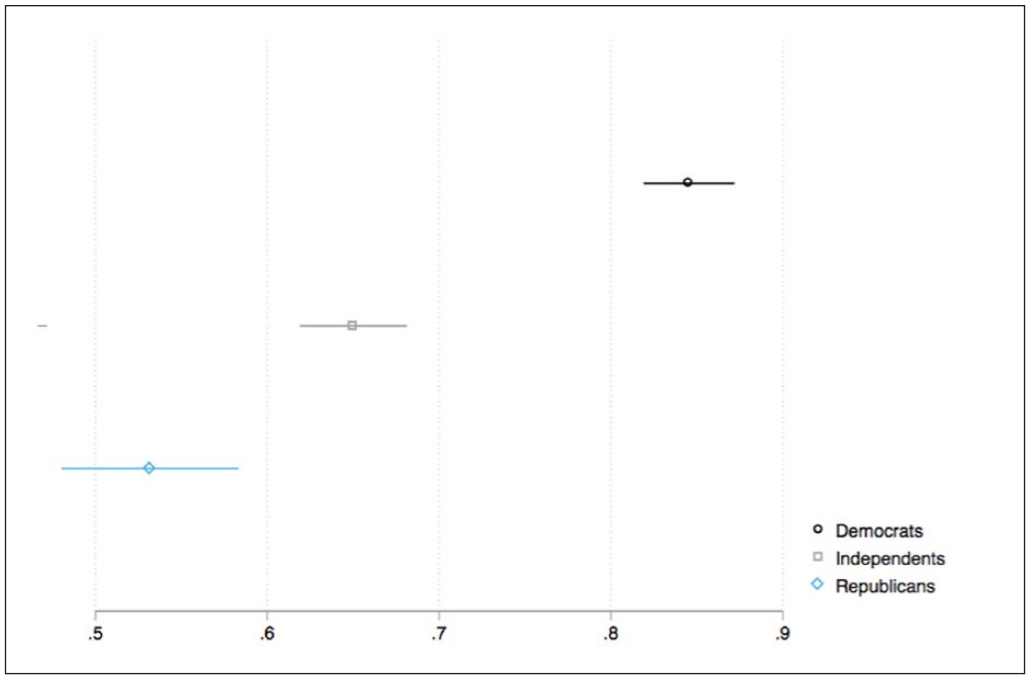


**Figure 2.** Fraction of respondents who view Russia as an enemy or unfriendly (by party identification).

may be that individuals actually assigned lower probability to "almost certainly," as some scholars (Mosteller and Youtz, 1990: 6) have found, or that the partisan cues diluted the effect of the certainty of attribution.[5]

While Amazon Turk is suitable for treatment effects, the question of representativeness often arises. We therefore disaggregated the data based on one of the most politically relevant considerations, which is partisanship. We found that individuals had clear partisan differences in terms of their attitudes toward Russia, as shown in Figure 2, consistent with recent survey data showing that Democrats are more hostile than Independents or Republicans.

These differences, while stark, did not carry over to how the respondents thought that the US should respond to cyber-attacks from Russia. As Figure 3 shows, about 36% of Republicans supported airstrikes in retaliation to a cyber-attack on the US compared to 31% of Independents and 33% Democrats, but these differences are not statistically significant.

All the policy preferences of the respondents followed this pattern – in which partisan differences on Russia did not carry over into attitudes about particular retaliatory options toward Russia – except for on economic sanctions. There the Democrats did appear to be more supportive than either Independents or Republicans (90% of Democrats versus 76% of Independents and 81% of Republicans). Even here though, there was remarkable convergence of bipartisan support for sanctions.

Based on qualitative responses expressing concern about escalation with a nuclear weapon country such as Russia, we suspect that factors about power, escalation, and nuclear weapons acted as a structural deterrent to more aggressive responses in ways that minimized partisan differences, though we think this warrants additional study.

## Conclusion

Accusations of Russian hacking in the 2016 US presidential election raised the salience of cyber security. However, there are still a number of unanswered questions about the circumstances under which particular policy responses are warranted and the public's attitudes about the conditions that justify this range of responses. In this research, we focused on how the certainty of attribution and the nature of attack affected public opinion.

We found that individuals support the notion of equivalence in that the nature and magnitude of the initial cyber-attack influence support for aggressive forms of retaliation. When a cyber- attack's effects cross over into actual fatalities, for example, the public is considerably more likely to support airstrikes in return. Partisan effects had the most consistent effect on support, with bipartisan consensus about attribution increasing public support for a range of retaliatory measures. Scholars have long viewed partisan consensus as an important determinant of public attitudes, but it may be even more relevant in an era of political polarization. With consensus even more difficult to reach, the public may view this outcome as requiring a higher evidentiary standard and thereby an even more important signal of the assessment's objective merits.

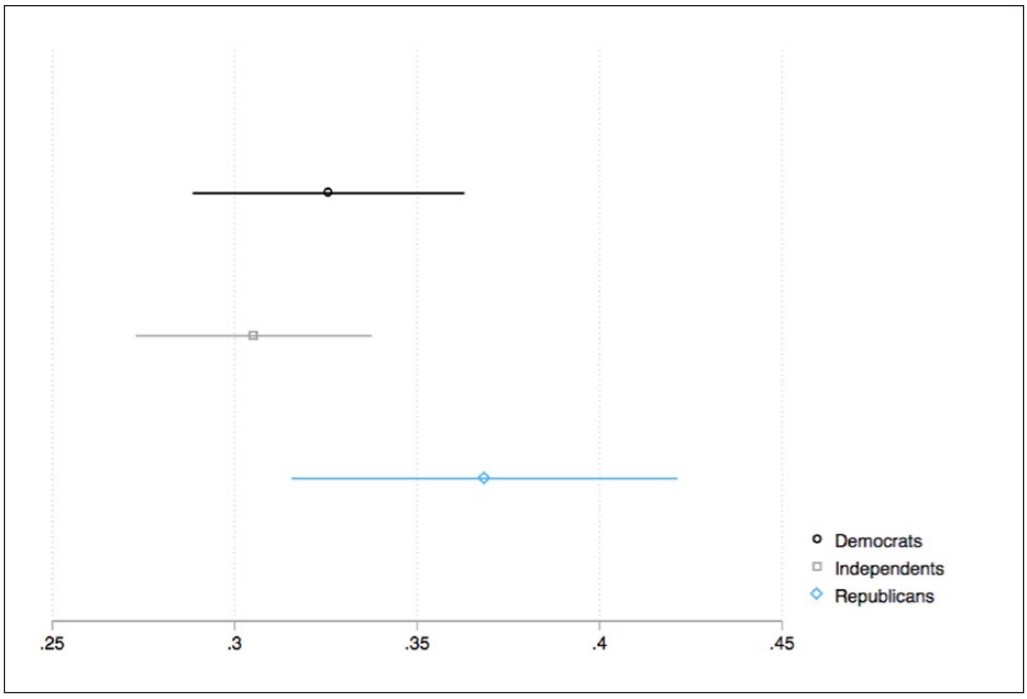


**Figure 3.** Fraction of individuals who support retaliatory airstrikes (by party identification).

This study represents the first known investigation of public attitudes toward cyber security, but it should not be the last. Other scholars should consider varying attributes that were bracketed for this analysis. For example, how does the nuclear status of the perpetrator affect respondents' willingness to retaliate? Does Russia's nuclear status deter respondents from supporting the use of force – which could lead to escalation – in more acute ways than would be the case than if the culprit were non-nuclear (e.g., Iran)? How would the public respond to considerably lower levels of kinetic cyber-attacks on infrastructure with few or no deaths? Would disagreement within the intelligence community or from the private cyber sector affect respondents' attitudes about retaliation? Recent political debates suggest that the issue of cyber security is here to stay. It behooves scholars to carry out additional systematic social scientific inquiry about the relationship between cyber-attacks, attribution, and domestic policy preferences.

## Acknowledgements

The authors would like to thank Mariel Barnes, Sarah Maxey, Jeff Friedman, Jon Lindsay, and Rebecca Slayton for helpful feedback on earlier versions of the manuscript.

## Declaration of Conflicting Interest

The authors declare that there is no conflict of interest.

## Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## Supplementary Material

The replication files are available at: https://dataverse.harvard.edu/dataverse/researchandpolitics

## Notes

1. See Edwards et al. (2017) for a complementary game theoretic overview of when states decide to attribute cyberattacks and when they choose to tolerate them in silence.
2. According to Berinsky et al. (2012), online convenience samples are useful for showing treatment effects, even if they are not representative of the public at large. Since we are more interested in treatment effects, we present those results although aggregate support levels in the Online Appendix.
3. Full instrument available in the Online Appendix.
4. These percentages correspond to 55–80% and 95–99% likelihood in assessments used by the intelligence community.
5. The latter could explain why our study finds little effect of attributional certainty while that of Friedman et al. (2016) finds that individuals *do* care about changes in probability estimates. Our study varies two aspects of attribution, and it may be that the partisan modifier is diluting the effect of the probability estimates themselves, meaning that the two sets of results are not necessarily incompatible.

## Carnegie Corporation of New York Grant

This publication was made possible (in part) by a grant from Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the author.

## References


Berinsky A, Huber G and Lenz G (2012) Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis* 20(3): 351–368.

Defense Science Board (2013) Resilient Military Systems and the Advanced Cyber Threat. Available at: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf (accessed 27 January 2017).

Department of Defense (2011) Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934. Available at: https://fas.org/irp/eprint/dod-cyber.pdf (accessed 27 January 2017).

Dunlap C (2011) Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly* 5(1): 81–99.

Edwards B, Furnas A, Forrest S, et al. (2017) Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America* 114(11): 2825–2830.

Fandos N (2016) Bipartisan Letter Seeks Single Inquiry into Russian Hacking Claims. *New York Times*. 17 December 2016. Available at: https://www.nytimes.com/2016/12/18/us/politics/donald-trump-transition.html?_r=0 (accessed 27 January 2017).

Friedman J, Lerner J and Zeckhauser R (2016) Behavioral Consequences of Probabilistic Precision: Experimental Evidence from National Security Professionals. Available at: http://scholar.harvard.edu/files/jenniferlerner/files/friedman_lerner_zeckhauser_-_behavioral_consequences_of_probabilistic_precision_-_august.31.2016.pdf (accessed 28 January 2017).

Gajanan M (2016) More than Half of Americans are Concerned about Russian Election Interference. *Fortune*. 18 December 2016. Available at: http://fortune.com/2016/12/18/russian-election-interferance-poll/ (accessed 27 January 2017).

Gallington D (2011) The Pentagon 'Equivalence Doctrine' Relating to Cyber War. *C-Span*. 1 June 2011. Available at: https://www.c-span.org/person/?danielgallington (accessed 27 January 2017).

Gorman S and Barnes J (2011) Cyber Combat: Act of War. *Wall Street Journal*. 31 May 2011. Available at: https://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (accessed 27 January 2017).

Herrmann R, Tetlock P and Visser P (1999) Mass public decisions to go to war: A cognitive–interactionist framework. *American Political Science Review* 93(3): 553–573.

Hosenball M (2016) US Intelligence Agencies Feud with Republicans over Russian Hacking. *Reuters*. 16 December 2016. Available at: http://www.reuters.com/article/us-usa-cyber-congress-idUSKBN1452E1 (accessed 27 January 2017).

Hughes A (2016) Statement of Mr. Aaron Hughes, Deputy Assistant Secretary of Defense for Cyber Policy Office of the Secretary of Defense Before the Committee on Oversight and Government Reform Informational Technology and National Security Subcommittees. 13 July 2016. Available at: https://oversight.house.gov/wp-content/uploads/2016/07/Hughes-Statement-Digital-Acts-of-War-7–13.pdf (accessed 27 January 2017).

International Committee of the Red Cross (2013) What limits does the law of war impose on cyber- attacks? Available at: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (accessed 27 January 2017).

Kahneman D and Tversky A (1979) Prospect theory: An analysis of decision under risk. *Econometrica* 47(2): 263–292.

Kim S and Everett B (2016) Trump vs. Congress on Russian Hacking. *Politico*. 11 December 2016. Available at: http://www.politico.com/story/2016/12/democratic-gop-senators-russian-hacking-cannot-become-a-partisan-issue-232475 (accessed 27 January 2017).

Kingdon J (1984) *Agendas, Alternatives, and Public Policies*. Boston, MA: Little, Brown.

Klarevas L (2002) The 'essential domino' of military operations: American public opinion and the use of force. *International Studies Perspectives* 3(4): 417–437.

Koh H (2012) International Law in Cyberspace. *Harvard International Law Journal* 54: 1–12. Available at: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers (accessed 27 January 2017).

Lee R, Anderson J and Connolly J (2014) Cyber Attacks Likely to Increase. *Pew Research Center*. Available at: http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/ (accessed 16 May 2017).

Lindsay J (2015) Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity* 1(1): 53–67.

Lindsay J and Gartzke E (2016) Coercion through cyberspace: The stability–instability paradox revisited. In: Greenhill KM and Krause JP (eds) *The Power to Hurt: Coercion in Theory and in Practice*. Available at: http://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf (accessed 27 January 2017).

Mačák K (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors. *Journal of Conflict and Security Law* 21(3): 405–428.

Mosteller F and Youtz C (1990) Quantifying probabilistic expressions. *Statistical Science* 5(1): 2–34.

Murdock J (2016) Clinton: US should use 'military response' to fight cyberattacks from Russia and China. *International Business Times*. 1 September 2016. Available at: http://www.ibtimes.co.uk/clinton-us-should-use-military-response-fight-cyber-attacks-russia-china-1579187 (accessed 27 January 2017).

Nye J (2011) Nuclear lessons for cyber security. *Strategic Studies Quarterly* 5(3): 18–38.

Obama B (2011) International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (accessed 27 January 2017).

O'Connell ME (2012) Cyber Security and International Law. *Chatham House*. Available at: https://www.chathamhsouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf (accessed 27 January 2017).

Ohlin JD, Govern K and Finkelstein C (eds) (2015) *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford, UK: Oxford University Press.

Rid T and Buchanan B (2015) Attributing Cyber Attacks. *Journal of Strategic Studies* 38(1–2): 4–37.

Sanger D (2016a) Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare. *New York Times*.

6 November 2016. Available at: https://www.nytimes.com/2016/11/07/us/politics/under-the-din-of-the-presidential-race-lies-a-once-and-future-threat-cyberwarfare.html?_r=0 (accessed 27 January 2017).

Sanger D (2016b) Obama Confronts Complexity of Using a Mighty Cyberarsenal against Russia. *New York Times*, 17 December 2016. Available at: https://www.nytimes.com/2016/12/17/us/politics/obama-putin-russia-hacking-us-elections.html (accessed 27 January 2017).

Schmitt MN (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press.

Steenbergen M, Edwards E and de Vries C (2007) Who's cueing whom? Mass–elite linkages and the future of European integration. *European Union Politics* 8(1): 13–35.

Vice Chairman of the Joint Chiefs of Staff (2010) Memorandum for the Chiefs of the Military Services: Joint Terminology for Cyberspace Operations. Available at: http://www.nsci-va.org/CyberReferenceLib/2010–11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (accessed 27 January 2017).

Volz D and Schectman J (2016) U.S. Set to announce response to Russian election hacking. *Reuters*. 29 December 2016. Available at: http://www.reuters.com/article/us-usa-russia-cyber-idUSKBN14H1SR (accessed 27 January 2017).

Williams K (2016) Clinton: Treat Cyber Attacks 'like any other attack'. *The Hill*. 31 August 2016. Available at: http://thehill.com/policy/cybersecurity/293970-clinton-treat-cyberattacks-like-any-other-attack (accessed ).

Zaller J (1992) *The Nature and Origins of Mass Opinion*. Cambridge, UK: Cambridge University Press.