Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

WHAT DO WE KNOW ABOUT CYBER ESCALATION? OBSERVATIONS FROM SIMULATIONS AND SURVEYS

NOVEMBER 2019 BENJAMIN JENSEN & BRANDON VALERIANO

Great Power Competition in a Cyber Era

Twenty-first century great power competition involves nuclear-armed states and regional powers engaged in high-stakes standoffs mixing military threats, diplomatic warnings, and economic coercion.[1] In November 2015, Russia responded to Turkey shooting down a Russian jet with a mix of denial-of-service attacks and economic threats, not military force.[2] In June 2019, the United States retaliated against Iranian aggression in the Persian Gulf, including Tehran shooting down a US drone and attacking international ships transiting the area, not with airstrikes or cruise missiles, but with a limited-objective cyber operation.[3] That same month, the United States revealed it had implanted dangerous malware on Russian electrical grids as a deterrent to interfering in

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

[1] This paper and supporting project were made possible by the generous support of the Carnegie Corporation of New York.

[2] Hugh Naylor and Andrew Roth, "NATO faces new Mideast crisis after downing of Russian jet by Turkey," *Washington Post*, November 24, 2015, https://www.washingtonpost.com/world/turkey-downs-russian-military-aircraft-near-syrias-border/2015/11/24/9e8e0c42-9288-11e5-8aa0-5d0946560a97_story.html. For an overview, see the International Crisis Behavior crisis summary: "Turkey-Russia Jet Incident," Duke University, http://people.duke.edu/~kcb38/ICB/v12summaries/2015Turkey-RussiaJetIncident.pdf.

[3] For an overview of the crisis, see Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html. Ellen Nakashima, "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers," Washington Post, June 22, 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html. Brandon Valeriano and Benjamin Jensen, "How cyber operations can help manage crisis escalation with Iran," *Washington Post*, June 25, 2019, https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

US interests.[4] Modern crises bargaining involves a mix of overt and covert cross-domain signals states use to manage escalation and provide options that might help them advance their interests short of war.

Unlike the Cold War in the twentieth century, this competition involves a new domain: cyberspace. From the United States to Russia, China, Iran, and North Korea, states are using cyber operations to exert influence and control. Whether massive military and commercial espionage campaigns[5] or international extortion rings and theft,[6] the cyber domain offers an outlet for states to advance their interests. Does the resulting cyber competition create new escalation risks? Do cyber operations alter how states respond to international crises in a way that creates incentives for decision makers to cross the Rubicon and use military force to settle disputes? This question is central to current cyber strategy debates and the idea of persistent engagement and defending forward in cyberspace.[7]

The answer is surprising: no. To date, cyber operations have tended to offer great powers escalatory offramps. They have provided signaling mechanisms that have let states shape an adversary's behavior without engaging military forces and risking military escalation.[8] Despite the uncertainty surrounding how states use new technologies for strategic ends, cyber operations tend to be stabilizing and provide options for avoiding costly, protracted conflicts.

This issue brief draws on new academic research, simulations, and survey experiments to study how cyber operations alter crisis decision-making during great power competition. Specifically, it analyzes escalation pathways and how the informed public and foreign policy actors conceptualize disruptive technologies and integrate them into larger competitive strategies. Based on the evidence, cyber operations offer a valuable escalatory offramp. Even states with more escalatory attitudes tend not to respond militarily to disputes when they have the option of imposing costs and signaling through cyberspace.

How states use cyber operations and the resulting escalation risk is a crucial area of policy-relevant research. Outside of Iran, the majority of cyber operations have been initiated by nuclear-armed states.[9] Despite popular images of lone hackers in basements, cyber operations require an investment in networks, infrastructure, and human capital or sufficient sums of money to buy capability on the black market.[10] These operations are complex instruments of statecraft that foreign policy actors integrate with other diplomatic, informa-

[4] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html. Benjamin Jensen, "What a U.S. Operation in Russia Shows About the Limits of Coercion in Cyber Space," *War on the Rocks*, June 20,2019, https://warontherocks.com/2019/06/what-a-u-s-operation-in-russia-shows-about-the-limits-of-coercion-in-cyber-space/.

[5] For an overview of Chinese cyber operations, see Jon R. Lindsay (ed.), Tai Ming Cheung (ed.), and Derek S. Reveron (ed.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015). For a discussion about how China organizes its cyber forces in relation to other strategic effects, see John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: National Defense University Press, 2018).

[6] Edith M. Lederer, "UN probing 25 North Korean cyberattacks in 17 countries," Associated Press, August 13, 2019, https://www.apnews.com/ece1c6b122224bd9ac5e4cbd0c1e1d80. For an overview of one of the Advanced Persistent Threats (APTs) associated with the North Korean cyber threat, see "Lazarus Group," MITRE, https://attack.mitre.org/groups/G0032/.

[7] Paul M. Nakasone, "A Cyber Force for Persistent Operations," Joint Force Quarterly (2019), 10-14. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," Cyber Command, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010. Brandon Valeriano and Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint, CATO Institute*, January 15, 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint. Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation, Institute for Defense Analyses*, May 2018, https://www.ida.org/research-and-publications/publications/all/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation.

[8] Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* (2017), 159-171. Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

[9] Valeriano, Jensen, and Maness, *The Evolving Character of Power and Coercion*.

[10] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," International Security (2017), 72-109. For a general overview of offensive operations, see Herbert Lin (ed.) and Amy Zegart (ed.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, DC: Brookings Institution Press, 2019).

tion, military, and economic instruments of power.[11] A combination of these instruments sends a clear signal to rival states. Cyber operations may, therefore, help stabilize great power competition in the twenty-first century.

Escalation in Perspective

When great powers compete in the twenty-first century, the competition often involves the risk of escalation. Nuclear-armed states and malign actors like Iran, with proxies and large inventories of ballistic missiles, face dangerous consequences if a political crisis spirals out of control. This risk puts a premium on finding ways to manage escalation.

The modern study of crisis escalation emerged during the Cold War with the examination of strategic competition as a bargaining process.[12] Crises like the Berlin Airlift and the Cuban Missile Crisis involved high-stakes poker, with states signaling a willingness to assume risk as well as deny benefits to an adversary and impose costs.[13] From this perspective, when a state makes a public threat, deploys an aircraft carrier, or mobilizes troops for a large training exercise short of war, it is sending a signal to other states. These signals allow states to calibrate their crisis strategy.

Earlier studies of international crises and militarized disputes found that most states prefer a strategy of reciprocation.[14] That is, they prefer to proportionally respond to a threat to maximize their position short of escalation. These findings echo foundational game theory work and the benefits of a "tit-for-tat" strategy.[15]

By studying crisis behavior, political scientists have identified conditions that make even stabilizing reciprocation strategies likely to escalate a crisis. States that are rivals are prone to arms races and place a value on gaining an advantage in a crisis leading to an increased likelihood of escalation.[16] In addition to rivals, states with active territorial disputes and with a recent history of disputes are more prone to escalation.[17] Furthermore, even outside of rivalry, signals can be misinterpreted and lead to episodes of inadvertent escalation.[18] For example, new capabilities can alter the offense-defense balance and how decision makers weigh the cost and benefits of various foreign policy preferences.[19]

[11] For a practitioner overview of the concept of instruments of power, see J. Boone Bartholomees, Jr. (ed.), "U.S. Army War College Guide to National Security Policy and Strategy," Strategic Studies Institute, U.S. Army War College, June 2006, https://www.comw.org/qdr/fulltext/0606bartholomees.pdf. For an academic perspective on combining positive and negative inducements, see Robert J. Art (ed.) and Patrick M. Cronin (ed.), *The United States and Coercive Diplomacy*, (Washington, DC: United States Institute of Peace Press, 2003). Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*, (Washington, DC: United States Institute of Peace Press, 1991).

[12] On bargaining theory, see Thomas Schelling, *Strategy of Conflict*, (Cambridge: Harvard University Press, 1960). Thomas Schelling, *Arms and Influence*, (New Haven: Yale University Press, 1966). James D. Fearon, "Rationalist Explanations for War," *International Organization* (1995), 379-414. Dan Reiter, "Exploring the Bargaining Model of War," *Perspectives on Politics* (2003), 27-43. Robert Powell, "Bargaining Theory and International Conflict," *Annual Review of Political Science* (2002), 1-30. Glen Snyder and Paul Diesing, *Conflict Among Nations*, (Princeton: Princeton University Press, 1977).

[13] For an overview of key concepts in the early study of crisis escalation, see Herman Kahn, *On Escalation: Metaphors and Scenarios*, (Piscataway: Transaction Publishers, 2009). Ole R. Holsti, *Crisis, Escalation, War*, (Montreal: McGill-Queen's University Press 1972). Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis*, (Baltimore: John Hopkins University Press 1984). Paul K. Davis and Peter Stan, "Concepts and Models of Escalation," *RAND Corporation*, 1984, https://www.rand.org/pubs/reports/R3235.html.

[14] Alex Braithwaite and Douglas Lemke, "Unpacking Escalation," *Conflict Management and Peace Science* (2011), 111-123. Faten Ghosn, Glenn Palmer, and Stuart Bremer, "The Militarized Interstate Dispute Data Sets Version 3.0: Procedures, Coding Rules, and Description" *Conflict Management and Peace Science* (2004), 133-154.

[15] Robert Axelrod, *The Evolution of Cooperation*, (New York: Basic Books 1984).

[16] Michael Brecher, "Crisis Escalation: Model and Findings," *International Political Science Review* (1996), 215-230. Susan G. Sample, "Arms Races and Dispute Escalation: Resolving the Debate," *Journal of Peace and Research* (1997), 7-22.

[17] For an overview of the factors that increase the likelihood of crisis escalation and war, see John Vasquez (ed.), *What Do We know About War?*, (New York: Rowman & Littlefield Publishers 2012).

[18] On perception and crisis dynamics, see Robert Jervis, *Perception and Misperception in International Politics: New Edition*, (Princeton: Princeton University Press 2017). Robert Jervis, "War and Misperception," *Journal of Interdisciplinary History* (1998), 675-700. On the concept of inadvertent escalation, see Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks*, (Ithaca: Cornell University Press 1991). Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* (2017), 50-92.

[19] On the offense-defense balance see Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* (1978), 167-214. Charles L. Glaser and Chairn Kaufmann, "What is the Offense-Defense Balance and How Can We Measure It?" *International Security* (2012), 44-82. Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security* (2006), 45-83. Marco Nilsson, "Offense-Defense Balance, War Duration, and the Security Dilemma," *Journal of Conflict Resolution* (2012), 467-489.

The question is how emerging capabilities like cyber operations affect crisis stability and escalation pathways. Some see a heightened security dilemma due to the uncertainty introduced by cyber weapons.[20] In this security dilemma and spiral model of conflict more generally, actions a state takes to secure its interests, even when defensive, lead competitors to respond, increasing the risk of escalation.[21] In cyberspace, states are likely to confuse intelligence collection with more dangerous, offensive intrusions in their networks. The security dilemma is further complicated by the widespread use of proxies in cyberspace.[22] From this perspective, every action, including defensive measures and increasing intelligence operations, in cyberspace should produce insecurity that proves volatile to great power interactions.

Other scholars see less risk in great power interactions and argue that there is a new stability-instability paradox with respect to cyber capabilities.[23] Cyber operations can be a tool for crisis management that prevents escalation if policy makers make a clear distinction between the physical and digital worlds, take advantage of the inherent defensive benefits afforded by cyberspace, and actively manage misperception.[24] In fact, cyber capabilities are an instrument of political warfare optimized for sub-crisis maneuvering.[25] They are as likely to be used to shape the initial stages of a crisis in a manner that produces bargaining benefits and crisis offramps as they are offensive strike packages to attack a rival state. Due to this process, *the presence of cyber response options need not escalate a crisis.*

This inference is based on a series of survey experiments and simulations conducted in 2018. Large, structured simulations offer a viable method for evaluating propositions on the nature of escalation under the context of cyber operations, and disruptive technology more generally. The emerging consensus that the cyber domain is made up of unique and unknown practices can be challenged by conducting simulations and survey experiments with diverse populations, including cyber operators. These interactive settings are a useful method for evaluating competing hypotheses, focusing data investigations, and delineating patterns otherwise unobserved.[26]

Recently, scholars have started to apply these methods to study cyber dynamics. A 2016 report by the UC Berkeley Center for Long-Term Cybersecurity used simulations and survey experiments based on the results to analyze how decision makers integrated cyber operations.[27] The study found that participants were reluctant to use high-end offensive cyber capabilities even during militarized disputes. Jacquelyn G. Schneider, a fellow at the Hoover Institution, used a longitudinal analysis of war games between 2011 and 2016 to study crisis dynamics and found that government officials were reluctant to escalate.[28] Of note, Schneider found that participants only used offensive cyber capabilities after conventional military strikes and expressed concern that using offensive cyber capabilities would increase the risk of nuclear escalation.

Measuring Attitudes Toward Escalation

This issue brief explores public attitudes toward great power competition and the potential for cyber operations to increase the risk of escalation through a cross-national simulation and survey experiments. To analyze cross-national perspectives, the research team at the Atlantic Council worked with YouGov to survey

[20] Ben Buchanan, *The Cyber Security Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press 2017).

[21] For a general overview of the security dilemma, see Shiping Tang, "The Security Dilemma: A Conceptual Analysis," *Security Studies* (2009), 587-622.

[22] Tim Mauer, *Cyber Mercenaries: The State, Hackers, and Power*, (New York: Cambridge University Press 2018).

[23] Jon R. Lindsay and Erik Gartzke, "Coercion through cyberspace: The stability-instability paradox revisited" in *The Power to Hurt: Coercion in Theory and in Practice*, Kelly M. Greenhill (ed.) and Peter J.P. Krause (ed.) (New York: Oxford University Press, 2018).

[24] Martin C. Libicki, *Crisis and Escalation in Cyberspace, RAND Corporation*, 2012, https://www.rand.org/pubs/monographs/MG1215.html. Also available in print form.

[25] Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* (2017), 159-171. Valeriano, Jensen, and Maness, *The Evolving Character of Power and Coercion*.

[26] Daniel Druckman, "Tools for Discovery: Experimenting with Simulations," Simulation & Gaming (1994), 446-455. Jonathan Wilkenfeld, Kathleen Young, Victor Asal, and David Quinn, "Mediating International Crises: Cross-National and Experimental Perspectives," *Journal of Conflict Resolution* (2003), 279-301.

[27] Benjamin Jensen and David Banks. *Cyber Operations in Conflict: Lessons from Analytic Wargames* (Berkley: Center for Long-Term Cybersecurity, 2016).

[28] Jacquelyn G. Schneider, "What War Games Tell Us About the Use of Cyber Weapons in a Crisis," *Net Politics*, Council on Foreign Relations, June 21, 2018, https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.

citizens from the United States, Russia, and Israel between December 2018 and January 2019.[29] One thousand adults were surveyed from each country and asked to participate in an international crisis simulation involving two fake countries, Green and Purple.

What the survey respondents did not know was that half of them were randomly assigned to four different treatment groups that had conditions based on 1) whether or not the triggering scenario involved a cyber incident and 2) whether or not they had cyber response options. Given the scenario treatments and their flexible response options, survey respondents outlined a proposed strategy.

The base scenario and different treatments capture the range of dynamics discussed above. First, the base scenario is escalation-prone. The states are rivals, engaged in a territorial dispute and a series of recent crises.[30] The scenarios also assumed the two states were nuclear powers with balanced military capabilities at the regional level.[31] The purpose of this scenario specification was to capture that cyber conflict is still the domain of powerful states, likely owing to the costs and organizational capacity required to generate cyber effects. It is a misnomer to call all cyber operations weapons of the weak.

The purpose of the cross-national surveys was to understand baseline escalation risks and determine if there were key cross-national differences in how different countries approached contemporary international crises involving cyber operations. The data also allows for an analysis of general strategic posture in terms of how states employ different instruments of power to de-escalate, respond proportionally, or escalate in a crisis. The scenario involved fake states, Green and Purple, in order to remove respondents from contemporary events as much as possible.

Table 1 displays each scenario treatment in relation to how respondents from different countries recommended responding to the crisis. The sample involved 2,993 responses after removing missing values. The results demonstrate statistically significant differences in respondent recommendations across the treatments. Where the cells show a number with a "+" and have blue shading or a "-" and have orange shading, it indicates where the response count is more (+) or less (-) than the expected value, and the difference is statistically significant.

Recommended Strategic Posture

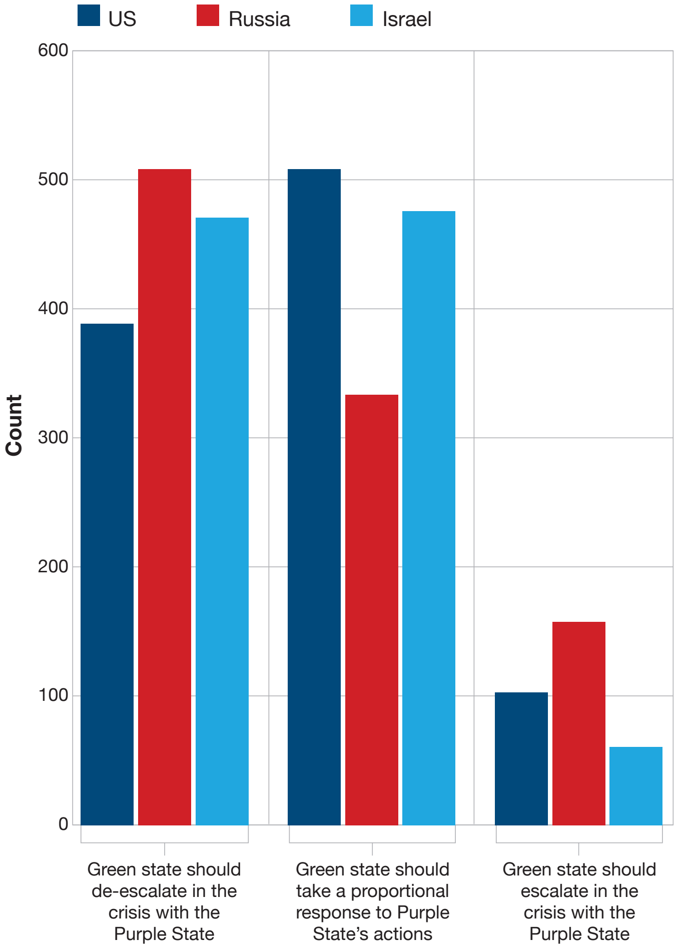

Chart: Jensen & Valeriano

[29] The surveys were conducted in English, Russian, and Hebrew. The YouGov team administered 3,285 surveys to get a sample of 3,000 matched to sampling frame on gender and age based on the Pew Research Global Attitudes Spring 2014 and 2015 Survey to include selection within strata by weighted sampling with replacements.

[30] Vasquez (ed.), *What Do We Know About War?*

[31] For an overview of the effect on military capabilities in terms of balance and type on crisis stability, see Daniel S. Geller, "Material Capabilities: Power and International Conflict" in *What Do We Know About War?*, Vasquez (ed.) (New York: Rowman & Littlefield Publishers 2012). Daniel S. Geller, "Nuclear Weapons, Deterrence, and Crisis Escalation," *Journal of Conflict Resolution* (1990), 291-310. Simon A. Mettler and Dan Reiter, "Ballistic Missiles and International Conflict," *Journal of Conflict Resolution* (2012), 854-880. D. Scott Bennet and Allan C. Stam, *The Behavioral Origins of War* (Ann Arbor: University of Michigan Press, 2004).

Looking across the scenarios, there are different national preferences associated with strategic posture. US respondents opted to de-escalate less than expected. In fact, most US respondents opted for a proportional response. Alternatively, Russian respondents escalated more than expected and de-escalated less than expected. They appear to have taken either an aggressive or passive approach, avoiding proportional responses more than expected across the scenario treatments.

Generally, the Russian respondents tended to take maximalist or minimalist approaches. Though the majority wanted to de-escalate the crises, more respondents

Table 1 **Cross-National Responses by Scenario**

Fewer responses than expected | More responses than expected

US Survey Respondants			
	De-Escalate	Proportional	Escalate
(1) Cyber Crisis Trigger & Cyber Options	92- (37.4%)	127+ (51.6%)	27 (11%)
(2) Cyber Crisis Trigger No Cyber Response Options	93- (37.3%)	135+ (54.2%)	21 (8.4%)
(3) No Cyber Crisis Trigger Cyber Response Options	103- (41.4%)	119 (47.8%)	27 (10.8%)
(4) No Cyber Crisis Trigger No Cyber Response Options	99- (39.8%)	127+ (51.0%)	23 (9.2%)
Russian Survey Respondants			
	De-Escalate	Proportional	Escalate
(1) Cyber Crisis Trigger & Cyber Options	130+ (52.0%)	78- (31.2%)	42+ (16.8%)
(2) Cyber Crisis Trigger No Cyber Response Options	127 (50.8%)	84- (33.6%)	39+ (15.6%)
(3) No Cyber Crisis Trigger Cyber Response Options	137+ (54.8%)	78- (31.2%)	35+ (14.0%)
(4) No Cyber Crisis Trigger No Cyber Response Options	116 (46.4%)	92- (36.8%)	42+ (16.8%)
Israeli Survey Respondants			
	De-Escalate	Proportional	Escalate
(1) Cyber Crisis Trigger & Cyber Options	115 (46.0%)	122 (48.8%)	13+ (5.2%)
(2) Cyber Crisis Trigger No Cyber Response Options	124 (49.6%)	111 (44.4%)	15- (6.0%)
(3) No Cyber Crisis Trigger Cyber Response Options	111 (44.4%)	127+ (50.8%)	12- (4.8%)
(4) No Cyber Crisis Trigger No Cyber Response Options	121 (48.4%)	114 (45.6%)	15- (6.0%)

N=2993
p < .01 Chi Square 108.629 (minimum expected is 103.28); no cells have a count less than five
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

Table 2 **Recommended Strategic Posture**

Fewer responses than expected | More responses than expected

US Survey Respondants			
	United States	**Russia**	**Israel**
De-Escalate	387- (39.0%)	510+ (51.0%)	471 (47.1%)
Proportional	508+ (51.2%)	332- (33.2%)	474 (47.4%)
Escalate	98 (9.9%)	158+ (15.8%)	55- (5.5%)

N=2993
p < .01 Chi Square 108.629 (minimum expected is 103.28); no cells have a count less than five
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

wanted to escalate than we would expect by chance. This finding reflects public attitudes shaping an approach to foreign policy that either accepts risk and escalates to de-escalate, making a dangerous opening move, or seeks to avoid confrontation all together. Russian responses tended toward the extremes. While contradictory on the surface, this posture potentially suggests a nuanced approach to escalation that mimics a strategic decision-making calculus of selecting options that represent the best chance of success at any possible time.[32]

Of note, escalatory responses were the least frequently occurring posture across each country. As seen in Table 2, even Russian respondents, the most escalatory, opted to escalate (158, 15.8%) less than other response postures (i.e., de-escalate and proportional). Across the scenarios, Israeli respondents (55, 5.5%) were the least escalatory and the results are statistically significant. US respondents (387, 39%) opted to de-escalate less than expected, while Russian respondents (510, 51%) opted to de-escalate more than expected.

Looking across all countries, the presence of cyber triggering events and cyber response options did not seem to alter escalation preferences outside of Russia. Revisiting Table 1, the presence of cyber response options (i.e., Treatments 1 and 3) saw Russian respondents de-escalating more frequently than expected. In other words, when Russian respondents had cyber response options it increased their preference for de-escalation. Israeli respondents, meanwhile, escalated less than expected when there was no cyber triggering event associated with the crisis.

The findings in Table 1 are critical as they cast doubt on perspectives that see the cyber domain as inherently escalatory.[33] While there is an internal logic to ideas such as the cyber security dilemma, survey results cast doubt on the inherent instability of cyber competition. [34]Cyber operations appear less as instruments of escalation and more as signaling mechanisms that provide crisis offramps and help states shape adversary behavior short of armed conflict.[35]

Table 3 breaks down de-escalatory options and shows the variance between how different nationals replied when cyber options were available. When respondents chose to de-escalate the crisis, there were key cross-national differences.

[32] Dan Reiter and Allan C. Stam, *Democracies at War* (Princeton: Princeton University Press, 2002).

[33] Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* (2013), 7-40. Lin (ed.) and Zegart (ed.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.*

[34] Ben Buchanan, *The Cyber Security Dilemma: Hacking, Trust, and Fear Between Nations*, (New York: Oxford University Press, 2017).

[35] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* (2017), 452-481.
Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* (2013), 41-73.
Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited" in *The Power to Hurt: Coercion in Theory and in Practice*, Kelly M. Greenhill (ed.) and Peter Krause (ed.) (New York: Oxford University Press, 2018).

Table 3 **De-Escalatory Response Dynamics**

Fewer responses than expected | More responses than expected

	Diplomatic Talks		Press Conference		Military Pullback		Track Three	
	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber
United States	157 (23.1%)	142 (20.6%)	78 (11.5%)	48 (7%)	91+ (13.4%)	75+ (10.9%)	62 (9.1%)	25- (3.6%)
Russia	220+ (32.4%)	211 (30.7%)	105+ (15.4%)	85+ (12.4%)	53- (7.8%)	46- (6.7%)	96+ (14.1%)	69 (10%)
Israel	192- (28.2%)	165 (24.0%)	73- (10.7%)	56 (8.1%)	96 (14.1%)	73 (10.6%)	68- (10.0%)	58 (8.4%)

N=680 cyber treatments; 688 non-cyber treatments
p < .01
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

First, Russian respondents (220, 32.4%) opted to seek diplomatic talks more than expected, while fewer Israelis did (192, 28.2%). While the most frequent US response across cyber and non-cyber option treatments was to publicly call for diplomatic talks, the response that occurred more than expected compared to other countries across non-cyber (91, 13.4%) and cyber (75, 10.9%) was a military pullback accompanied with increased intelligence collection. Russian respondents, on the other hand, selected a military pullback in both cyber (46, 6.7%) and non-cyber (53, 7.8%) less than expected. The opposite was true for public press conferences. What does this mean? Cyber operations may not have a clear, direct effect on Russian military posture or lead to increased diplomacy.

Table 4 looks at the cyber options survey respondents used to de-escalate the crisis. When survey respondents had cyber response options (i.e., Treatments 1 and 3) they could use to de-escalate the crisis, two dynamics manifested. As seen in Table 4, despite concerns over the 2016 US election, US respondents showed no additional interest in working with social media firms to remove propaganda compared with their Russian counterparts.[36] Russians opted to work with social media firms to remove propaganda more than expected (69, 10%). Israelis opted to counter propaganda less than expected (25, 3.6%). It is likely that US respondents either did not see social media as a viable threat, despite evidence that the use of targeted ads and content is corrosive, or had no confidence in the corpora-

Publicly Call for Diplomatic Talks to Reduce Tension

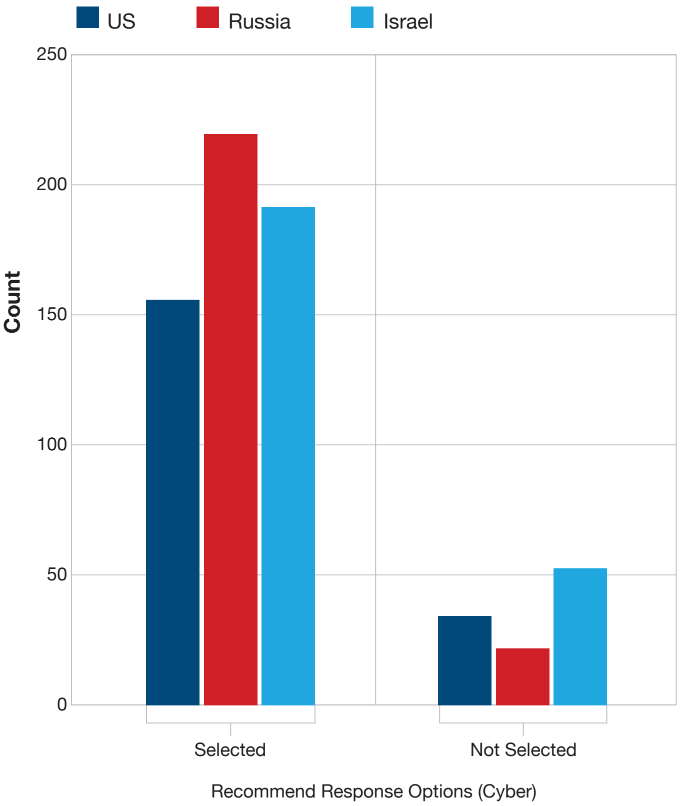

Chart: Jensen & Valeriano

[36] On the 2016 US presidential election and Russian cyber strategy, see Benjamin Jensen, Brandon Valeriano, and Ryan Maness "Fancy bears and digital trolls: Cyber strategy with a Russian twist," *Journal of Strategic Studies* (2019), 212-234.

Table 4 **Cyber De-Escalatory Response Dynamics**

Fewer responses than expected

More responses than expected

	Public Call to Limit Offensive Cyber	Work with Social Media Firms to Remove Propaganda	Warn of Risk of Cyber Escalation	Work with Industry to Harden Networks
United States	45 (6.5%)	36 (5.2%)	38 (5.5%)	37- (5.4%)
Russia	55 (8.0%)	69+ (10%)	59 (8.6%)	60- (8.7%)
Israel	40 (5.8%)	25- (3.6%)	46 (6.7%)	88+ (12.8%)

N=688 cyber treatments
p < .01
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

tions taking action at the behest of the government. Alternatively, and indicative of growing digital authoritarianism and the intersection of business and political interests, Russian respondents may have greater confidence that social media companies will purge divisive content when ordered by the government.

Second, both US and Russian respondents did not seek out key public-private partnerships and work with industry to harden networks as a means of limiting targets, signaling defensive capabilities and resilience, and de-escalating the crisis. US (37, 5.4%) and Russian (60, 8.7%) respondents hardened networks less than expected. On the other hand, Israeli (88, 12.8%) respondents hardened networks more than expected. This fits with the broader cooperation between the Israeli government and cybersecurity firms, and represents a point of risk in both Russia and the United States.[37]

Returning to Table 3, the primary US survey respondent mechanism for de-escalating a crisis was diplomatic talks (142, 20.6%) when cyber options were available, but a military pullback occurred higher than expected (75, 10.9%). Similar to the failure to harden networks against future cyber attacks, US respondents (25, 3.6%) opted to reach out to rival states through Track III diplomacy less than expected, compared to Russians and Israelis. In fact, Russian respondents appeared interested in Track I (220, 34.2%) and Track III (96, 14.1%) diplomacy more than expected when no cyber options were available.

US respondents seemed to draw a divide between government responses and private sector responses. This divide is a policy issue. The networks that connect the modern world are predominantly private networks, owned and operated by businesses. Defending these networks presents a collective action problem and challenges traditional notions of security.

Proportional Response Dynamics

Table 5 breaks down proportional response options and shows the differences between how different nationals replied when cyber options were available. There are key differences across countries and based on the availability of cyber response options. US respondents (110, 16.6%) opted to conduct a show of military force more than expected when they lacked cyber response options (i.e., Treatments 2 and 4). The findings echo recent speculation that cyber options gave the United States a means of sending a signal to Iran short of using armed force in the summer of 2019 crisis in the Strait of Hormuz.[38] While this usage suggests a capability of cyber operations to signal short

[37] Nick Kolyohin, "Spotlight: Israel invites more int'l cooperation in cyber sector," Xinhua, January 30, 2019, http://www.xinhuanet.com/english/2019-01/30/c_137787354.htm.

[38] Valeriano and Jensen, "How cyber operations can help manage crisis escalation with Iran."

Table 5 **Proportional Response Dynamics**

Fewer responses than expected

More responses than expected

	Backchannel		Propaganda (Black/Gray)		Show of Force		Targeted Individual Sanctions	
	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber
United States	179 (27.0%)	144 (22.1%)	28- (4.2%)	19- (2.9%)	110+ (16.6%)	66 (10.1%)	125+ (18.9%)	88+ (13.5%)
Russia	100- (15.1%)	72- (11.1%)	33 (5.0%)	23 (3.5%)	90+ (13.6%)	59+ (9.1%)	57 (8.6%)	35 (5.4%)
Israel	160 (24.1%)	158+ (24.3%)	58+ (8.7%)	42+ (6.5%)	43- (6.5%)	33- (5.1%)	63 (9.5%)	32- (4.9%)

N= 663 non-cyber treatments; 651 cyber treatments
p < .01
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

Table 6 **Cyber Proportional Response Dynamics**

Fewer responses than expected

More responses than expected

	Website Defacement	Plant Social Media Stories	Increase Cyber Defenses	Signal Risk of Cyber-Enabled Electronic Warfare
United States	21 (3.2%)	14- (2.2%)	130 (20.0%)	74- (11.4%)
Russia	8 (1.2%)	19 (2.9%)	88 (13.5%)	47 (7.2%)
Israel	25 (3.8%)	27 (4.1%)	145 (22.3%)	117+ (18.0%)

N= 680 non-cyber treatments; 688 cyber treatments
p < .05
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

of war and lends credence to the idea of defending forward, the utility of cyber operations to stop military retaliation and threats is limited. In fact, regardless of whether they had cyber options available, Russian respondents used military shows of force as a proportional response more than expected. Cyber response options offer a means of signaling escalation risk, but with limited deterrent value. They are weak instruments of coercion.

Two additional dynamics are on display in Table 5. Russian respondents, regardless of treatment, were not interested in using backchannels to signal a rival state during a crisis. Israeli respondents showed a preference, regardless of treatment, to use black and gray propaganda to discredit their rival more than expected. These results are intriguing given the preference Russia has shown for active disinformation campaigns. There appears to be a difference between public attitudes and government responses in Russia.

Last, Israeli respondents (32, 4.9%) opted to use individual sanctions less than expected when they had cyber options available. Cyber options offer a means of signaling escalation risk short of reverting to more traditional coercive instruments like economic sanctions. Of note, Israeli respondents appear to have taken advantage of this dynamic, increasing their use of backchannel diplomatic warnings (158, 24.3%) more than expected when cyber response options were available.

Table 6 looks at the cyber options survey respondents used to respond proportionally to the crisis. When survey respondents had cyber response options (i.e., Treatments 1 and 3), two dynamics manifested. First, the US respondents opted to manipulate social media (14, 2.2%) and signal the risk of cyber-enabled economic warfare (74, 11.4%) less than expected. This finding could signal a public preference in the United States for preserving an open, free set of digital connections free of state manipulation in either the information or economic sphere. Second, Israeli respondents (117, 18.0%) selected to threaten cyber-enabled economic warfare more than expected. These findings show Israeli respondents seeing a viable role for threatening cross-domain coercion and cyber-enabled economic warfare, illustrating how cyber operations can spill over into other domains.

Escalation Response Dynamics

Table 7 analyzes escalatory response options and shows the variance between how different national respondents replied when cyber options were available. There are key differences across countries and based on the availability of cyber response options. First, it is important to note that responses favoring escalation were rare across all three countries, likely owing either to the presence of nuclear weapons and/or the fact that the survey was the first time the participants were introduced to the crisis. Of note, US respondents (19, 12.3%) used limited military strikes to escalate more than expected when they lacked cyber response options. When cyber options were present, US respondents (10, 6.4%) used diplomatic expulsions less than expected. In other words, cyber options gave US respondents more flexibility to respond to a crisis.

Israeli respondents altered their escalatory responses based on the presence of cyber options. Unlike the US respondents, Israelis (9, 5.8%) opted for limited military strikes more than expected when cyber options were available. When they lacked cyber options, Israelis opted for economic embargoes (8, 5.2%) and diplomatic expulsions less than expected. Returning to Table 2, Israel had less escalatory responses than expected (55, 5.5%). This low incidence has to be taken into account when analyzing how Israeli respondents opted to escalate and the revealed preference for using military force even when viable cyber options are present.

Table 8 looks at the cyber options survey respondents used to signal escalation in the crisis. The findings are limited. While the distribution of responses is different, and the difference is statistically significant, the major divergence is that US respondents (8, 5.1%) opted to attack nuclear command-and-control infrastructure less than expected. Of note, this response option was the preferred method of Russian cyber response (24, 15.4%), but the findings are not statistically significant and reflect an even distribution across the available options. Though not statistically significant, the findings also show a preference across countries for not using espionage to reveal sensitive political secrets, which on the surface would be less escalatory than launching limited attacks against critical infrastructure and key economic networks like the financial markets. When examined in relation to Table 7, all three states preferred cyber activities targeting the economy to full economic embargoes. This finding implies a need to develop strategies to protect critical commercial networks as a means of denying options to rival states in a crisis.

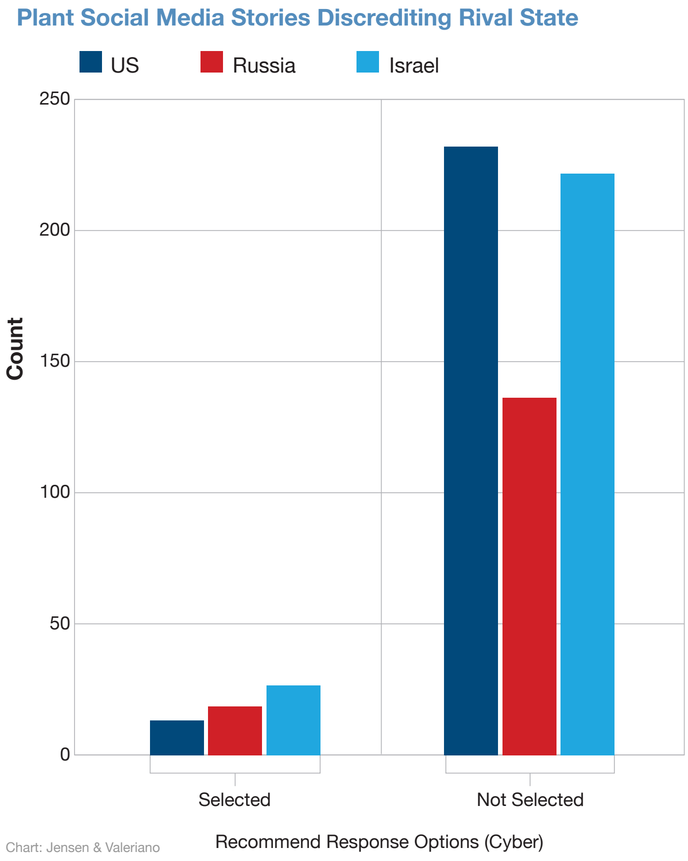

Chart: Jensen & Valeriano

Table 7 **Escalation Response Dynamics**

Fewer responses than expected

More responses than expected

	Expel Diplomats		Publicly Call for War		Limited Military Strikes		Full Economic Embargo	
	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber	No Cyber	Cyber
United States	17 (11.0%)	10- (6.4%)	10 (6.5%)	10 (6.4%)	19+ (12.3%)	7 (4.5%)	26 (16.8%)	13 (8.3%)
Russia	40+ (25.8%)	35+ (22.4%)	28 (18.1%)	12 (7.7%)	15- (9.7%)	6- (3.8%)	40 (25.8%)	19 (12.2%)
Israel	5- (3.2%)	4a (2.6%)	12 (7.7%)	9 (1.5%)	10 (6.5%)	9+ (5.8%)	8- (5.2%)	7 (4.5%)

N= 155 non-cyber treatments; 156 cyber treatments.
p < .01
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)

Chart: Jensen & Valeriano

Implications

Cyber operations are not inherently escalatory. They offer states indirect methods for responding to crises short of war, an approach the military strategist Herman Kahn in his classic study of escalation called sub-crisis maneuvering.[39] Based on the survey results, it appears that cyber operations did not alter the offense-defense balance or exacerbate the security dilemma. Respondents preferred de-escalation more than escalation even when they had cyber options with which to respond. Escalation was not the norm.

Important differences in cyber strategy emerge at the national level. This issue brief demonstrates that countries have different ways of responding to crises when cyber options are available. Of note, US respondents conducted a show of force less when cyber options were available. Russian respondents used traditional diplomatic methods like public talks and Track III engagements when they did not have viable cyber options to send a signal to a rival state. Tellingly, Russians also showed an interest in working to limit the ability of rival states to use social media to shape public discourse during a crisis. Though the state that showed the lowest incidence of escalation, when Israelis did ramp up pressure, respondents showed a willingness to combine force with cyber operations and threaten economic targeting via cyberspace more than either Russian or US respondents.

These findings, though preliminary, have important policy implications. First, policy makers should treat cyber operations less like escalatory weapons of war and more like espionage and long-term shaping activities. Such operations have historically been means of gaining valuable intelligence, sabotaging adversary networks, and signaling capabilities in crises.[40] This issue brief shows that public attitudes approach cyber operations in a similar manner.

Second, a connected global economy and citizens whose personal and political lives rely on networks necessitate new ways of thinking about grand strategy in the twenty-first century. The findings in this issue brief illustrate an informed public grappling with different ways of integrating cyber operations into coercive diplomacy. While escalation was rare, options such as active disinformation campaigns and cyber-enabled economic warfare illustrate where a relatively stable domain of covert action could pull decision makers to the precipice. There needs to be a framework for establishing new norms in cyberspace that clarifies key red lines, enables restraint, and ensures that tacit bargaining in the digital domain does not destroy our way of life.

Establishing such a framework requires a strategic dialogue within great powers like the United States that engages partners, allies, and the private sector. Bipartisan initiatives like the Cyberspace Solarium

[39] Kahn, *On Escalation*.

[40] Valeriano, Jensen, and Maness, *The Evolving Character of Power and Coercion*.

Table 8 **Cyber Escalatory Response Dynamics**

Fewer responses than expected | More responses than expected

	Cyber Degradation (Critical Infrastructure)	Cyber Espionage (Exposed Leadership Secrets)	Cyber Degradation (Nuclear C2)	Cyber Degradation (Economy)
United States	11 (7.1%)	6 (3.8%)	8- (5.1%)	21 (13.5%)
Russia	17 (10/9%)	13 (8.3%)	24 (15.4%)	20 (12.8%)
Israel	8 (5.1%)	6 (3.8%)	10 (6.4%)	11 (7.1%)

N= 155 non-cyber treatments; 156 cyber treatments
p < .05
+ = count more than expected where critical value is +/- 1.96 (adjusted residual)
- = count less than expected where critical value is +/- 1.96 (adjusted residual)
a = cell counts less than 5 cannot be used to factor chi square tests

Chart: Jensen & Valeriano

Commission show a path forward.[41] Great power competition should not hijack or threaten the networks that enable life, liberty, and the pursuit of happiness in the twenty-first century. While states and other malign actors will leverage these networks for covert campaigns and criminal activity, their safety and integrity is a core interest for many countries.

About the authors:

Benjamin Jensen, PhD is a nonresident senior fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. He holds a dual academic appointment as a professor of strategic studies at the School of Advanced Warfighting, Marine Corps University, and as a scholar-in-residence at American University's School of International Service.

Brandon Valeriano, PhD is the Donald Bren Chair of Military Innovation at the Marine Corps University. Along with Benjamin Jensen and Ryan Maness he is the author of *Cyber Strategy: the Evolving Character of Power and Coercion* (Oxford University Press 2018).

[41] US Sen. Angus King (I-ME) and US Rep. Mike Gallagher (R-WI), "Announcing the Cyberspace Solarium Commission," *Lawfare*, August 19, 2019, https://www.lawfareblog.com/announcing-cyberspace-solarium-commission.

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org