Unpacking Strategic Behavior in Cyberspace: A Schema-Driven Approach

This article has been accepted for publication in the Journal of Cybersecurity Published by Oxford University Press.

Miguel Alberto Gomez
Center for Security Studies, ETH
Haldeneggsteig 4, IFW, Zürich 8092, Switzerland
email: miguel.gomez@sipo.gess.ethz.ch
phone: +41 44 633 87 50

Christopher Whyte
L. Douglas Wilder School of Government and Public Affairs
Virginia Commonwealth University
Scherer Hall, 923 W. Franklin St. Richmond, Virginia 23284, USA
email: cewhyte@vcu.edu
phone: (571) 338-0442

Version Date: 09.04.2021

The contemporary literature on cybersecurity and related interstate interactions often cites the need to overcome uncertainty due to an inherent deficit of information about cyber operations. While this notion continues to appear relevant in studies that advance our understanding of state behavior in cyberspace, noticeable gaps remain. These gaps particularly stem from the limited utility of cyber operations to shift the balance of strategic power between states or to signal intent and resolve effectively. In response, this article advances a cognitive-cultural framework wherein behavior reflects preferences derived from schema usage. Using cross-national wargames, the article illustrates the schematic use of strategic culture as a basis for deriving strategic objectives and the means with which these are achieved. Consequently, the article serves as the initial foray in expanding our understanding of interstate behavior in cyberspace.

Keywords: cybersecurity, wargame, decision-making, schemas

Introduction

Scholarship on cybersecurity and state interactions in cyberspace continues to cite the perceived strategic benefits offered by cyber operations [1]. However, surprisingly little is said about the sources of stakeholder preferences on the role of cyber operations and the means by which they help secure strategic objectives. Certainly, research that pursues this question often identifies the need to overcome uncertainty emerging from the underlying characteristics of the domain as encouraging state behavior [2, 3]. From this, it is then argued that mitigating uncertainty necessitates the offensive use of cyber operations to discourage adversaries and achieve a favorable balance of power [4, 5], a position that corresponds with the "revolutionary" narrative often associated with cyberspace. But this position seems increasingly untenable, as the underlying reliance on "logic-of-the-domain" reasoning of the argument and growing empirical evidence lend credence to the idea that cyber conflict's operational dynamics are as much determined by socio-institutional context as technical characteristics.

Perhaps most significantly – and contrary to conventional expectations – available data analyses of global cyber events suggest that cyber conflict is strategically limited despite advances in material and organizational capabilities [6, 7]. Even with reduced operational requirements¹, the latent strategic potential of the method remains the purview of established powers [8, 9] and not so often, as many have long feared (e.g. Nye 2010), a weapon for the weak. Capable state actors themselves, however, appear to practice self-restraint when exercising power in cyberspace, suggesting an attempt to manage escalatory risks [4, 10]. This dynamic flies in the face of the common argument that strategic-operational preferences emerge from fears of unbounded cyber conflict.

This article does not argue that the focus of prevailing thinking on the need to overcome uncertainty is entirely insufficient, but simply that uncertainty must be thought of as a dynamic variable whose impact is determined by cultural-cognitive context rather than a static fact of engagement in cyberspace. Specifically, this article asserts that decision-makers are unsurprised by malicious behavior, as the 21st century "pollution" of the international environment with digital insecurities constitutes a new normal of global politics. They are, however, concerned with the ambiguity of the strategic environment [11-13]. Much as in other situations in foreign policymaking, this ambiguity facilitates the schematic use of strategic culture in identifying strategic objectives and the means to achieving them. Naturally, however, such efforts to address ambiguity do not necessarily produce schematic thinking that accurately captures fundamental aspects of the operational and strategic environment [14-17]. In order to objectively evaluate the environment and to mitigate the effects of schema-driven biases, decision-makers must construct and orient on accuracy goals [18-21].

This article illustrates the feasibility of this argument through the use of novel results obtained from a unique set of cross-national wargames conducted between 2019 and 2020 in Singapore and the Philippines. Our argument and the results of these simulations encapsulate several critical implications for the conduct of foreign policymaking oriented on cyber conflict, not least that socio-organizational adversary assessments must play a major role in shaping and

¹ Relative to conventional instruments operating in land, sea, and air.

reshaping key engagement strategies – like persistent engagement – over time. Consequently, the article finds itself among research that attempts to better understand strategic behavior in cyberspace by complementing system-level and technology-driven explanations with insight regarding the cognitive processes of decision-makers that dictate actions in the domain. Methodologically, we align with recent work in noting that wargaming can demonstrate the feasibility of nuanced arguments about foreign policymaking and highlight its value as a research instrument to understand the mechanism shaping individual- and group-level preferences.

The remainder of the article proceeds in four sections. The first section introduces the theoretical framework and discusses the proposed cognitive-cultural mechanism grounded in the interaction between schemas and accuracy goals. We then discuss wargame design, emphasizing relevant limitations and benefits with respect to this study. Proceeding from this, the results are presented and analyzed using thematic coding and direct comparison of the performance of the Singaporean and Philippine participants. Finally, the article concludes with a summary of its findings and its implications for both theory and policy.

Theoretical Framework

The growth of state-associated cyber operations² continues to stimulate progress in cybersecurity scholarship. Citing cyberspace as a pillar of national power [22], scholars and policymakers continue to espouse the strategic potential of cyber operations that exploit vulnerabilities to generate strategically-relevant effects. Consequently, cyber operations are conceived as the exercise of state power in pursuit of strategic objectives through cyberspace.³

In spite of this conceptualization and of advancing actor capabilities, however, the strategic utility of much cyber action remains in doubt. Iasiello [6] asserts that cyber operations are blunt instruments that fail to strategically influence adversarial behavior, with damage inflicted to and through cyberspace remaining transient [23, 24]. Moreover, though barriers to operation often seem low, resources required to achieve strategically relevant outcomes can be prohibitive, limiting the number of cyber-capable actors [8, 9]. As a result, arguments that the development of sound cyber capabilities stem from expectations of unbridled conflict rests on thin ice. And though it would be disingenuous to claim that this is not addressed by contemporary scholarship, it would be equally inappropriate to conclude that a unanimous understanding of in-domain state behavior exists.

Prevailing Arguments

A major aspect of the debate surrounding cyber operations involves questions of uncertainty and its mitigation [25, 26]. Broadly, uncertainty is understood as either resulting from informational deficits or ambiguity [27]. For cyberspace, the former emerges from inherent difficulties in retrieving data sufficient to technically attribute digital actions. By contrast, the

² The boundary between state and non-state actors in cyberspace tends to be blurred and is not addressed directly by this article. See *Cyber Mercenaries: The State, Hackers, and Power* by Tim Maurer.

³ To include activities like espionage, defacement, and degradation of capabilities.

latter arises from challenges of meaning extraction⁴ and the interpretation of behavior. While both help explain state behavior, the former dominates the cybersecurity literature [4, 28].

These deficit-based explanations highlight how interconnectedness and complexity introduces challenges in anticipating vulnerabilities and corresponding exploitation effects [29]. Compounding this unpredictability is the perceived potential for exploitation, such as in the prospect of significant cascade effects (Saltzman [5]. Schneider [30] also argues that technological dependence promotes instability given the perceived necessity of offensive actions to guarantee ongoing access to cyberspace. This engenders a sense of unknowability, unpredictability, and inevitability that motivates states to adopt the necessary steps to secure their interests and highlights the strategic potential of offensive cyber operations [25].

However, this argument is insufficient as cyber operations have yet to demonstrate their ability to shift the balance of power within the international system [10, 31]. Furthermore, others note [8, 9, 24] that these are more resource-intensive than initially conceived. Consequently, continued investment in cyber capabilities appears counterintuitive, especially for materially constrained actors [32]. True, if cyberspace is believed to offset material imbalances, it can be argued that rampant in-domain conflict is likely to follow. But even among capable actors, a degree of restraint exists which appears to be the status quo [10]. Consequently, while information deficits appear to provide a simple explanation for behavior reflecting underlying preferences, empirical backing for such a conclusion is weak at best.

By contrast, ambiguity invokes a different set of challenges and solutions. Unlike conventional instruments, cyber operations are of limited communicative value [11]. For instance, espionage operations share similarities with more damaging degradative operations. As such, distinguishing intent poses a significant challenge, meaning that preferences may not be exclusively oriented towards the mitigation of cyber operations and are instead concerned with discerning the meaning and consequences of events.

The academic community increasingly recognizes the role of informational ambiguity in shaping digital interactions. Egloff [33] argues that forensic developments signal a shift in attributing cyber operations from a sense-making to a meaning-making activity, focused less on “who” and more on what ought to be done. Similarly, Brantly [26] acknowledges the value of behavioral information in the domain but recognizes subjectivity in its interpretation. Buchanan [11] echoes a related concern when acknowledging the subjective interpretation of cybersecurity incidents and argues that existing disputes are likely to influence judgments. Finally, Gartzke and Lindsay [34] posit that ambiguity increases in salience with respect to the target's perceived value. As such, subjective interpretations reflect the ambiguity faced by decision-makers when evaluating the strategic environment [27]. Empirically, this is surfaced by both real-world cases and experimental research.

With regards to real world events, one need look no further than the assumptions that abound soon after major events and before attribution has been revealed. In July 2020, for instance, an Israeli cyber operation purportedly resulted in an explosion at that Natanz nuclear enrichment facility in Iran. The details of the case remain obscured, but reports suggest that this was a response to earlier Iranian attempts to compromise Israel’s water distribution

⁴ For instance, the discovery of malicious code does not, by itself, communicate intent owing to similarities between malicious code that may serve different functions.

system [35]. Though claims of responsibility are yet to be made, previous incidents validate the existence of Israeli capabilities sufficient to enable this operation. Furthermore, given the existing rivalry between Israel and Iran, attributing responsibility seems reasonable and undoubtedly influenced attempts at discerning intent [36]. This cognitive mechanism is not unexpected and can be seen in other cases, such as with the cyber operations during the opening ceremony of the Pyeongchang Winter Olympics in 2018⁵ [37] and those affecting the U.S. Department of Defense (DoD) network in 1998 [38]⁶.

In experimental settings, Schneider [39] notes that hesitation in employing cyber operations during wargames is traced to the uncertainty surrounding the severity of the response. Initiators of cyber operations doubt whether an adversary can recognize the intent behind an operation. Fearing that this may be misconstrued as an attempt to escalate hostilities, initiators exercise restraint and project their beliefs on to their adversaries to ascertain possible reactions. Moreover, additional information fails to resolve questions of ambiguity (Gomez [40]). Despite complete information, decision-makers remain cognizant of other means with which cyberspace can render available information ambiguous. Consequently, decision-makers attempt to draw parallels with past incidents, employing the representativeness heuristic in the process.

While technological and procedural developments increase the availability of information [41], characteristics of the domain and the strategic environment limits the success of discerning the meaning and consequences of cyber operations. As such, contemporary cybersecurity research implicitly recognizes that cyberspace suffers from an excess of ambiguity⁷ rather than a deficit of information. Furthermore, this ambiguity provokes cognitive mechanisms that, as previously illustrated, shape preferences with respect to cyberspace.

Schemas and Cyber Operations

While a number of cognitive devices exist to overcome uncertainty, this article asserts that schemas feature prominently in the formation of preferences. Schemas are cognitive maps embedded in the subconscious that facilitates information processing and retrieval [42]. Schemas share similarities with beliefs that influence crucial cognitive processes such as (1) setting and influencing expectations, (2) establishing the plausibility of particular judgments, (3) and constraining Bayesian updating [43].

Schemas establish the range of acceptable options in response to the environment and acknowledge the continued relevance – though possibly diminished – of empirical realities faced by an actor [17]. Crucially, schemas offer a means to overcome uncertainty prevalent in the international system by functioning as templates applied to the interpretation of the material world. Consequently, ambiguity is nullified by assuming the presence and meaning of conditions that activate these schemas [44].

⁵ Initially, given the underlying strategic context, attributed to North Korea.

⁶ Thought to have originated from Iraq given its correspondence with a set of sanctions to be imposed on the Iraqi regime.

⁷ Moving forward, references to uncertainty is taken to mean the ambiguity of available information.

While different schemas develop throughout an individual's life, this article is concerned with the schematic use of strategic culture,⁸ which is a *set of beliefs held by elites concerning the strategic objective and how best to achieve it*⁹. This is akin to intentional and operational ideas identified by Kitchen [16]. The former provides normative suggestions that underlie policy goals while the latter offer means to achieve these. Consequently, strategic culture offers a set of preferences that include specific strategic objectives and how these are to be achieved. This intersection between culture and cognition is advanced by DiMaggio [50] who proposes the concept of logics of action as a set of *'representations or constraints that influence action in a given domain'* that points to a fundamental function of schemas in that these simplify complex environments and preserve limited cognitive resources [51].

Advancing schemas as a means to overcome uncertainty in cyberspace finds parallels in other aspects of strategic decisions-making. For nearly half a century, scholars recognized the value of these cognitive devices in addressing the complexity of the international environment [52]. Consequently, schemas provide an analytical lens through which state behavior is interpreted by identifying the source of preferences shaping state behavior.

While the literature does not directly reference the schematic use of strategic culture, it is surfaced in several research programs. Starting with the fundamental task of defining what constitutes cyberspace and cybersecurity, varying definitions emerging from country-specific approaches hint at the importance of these constructs. Hare [53] observes that unique socio-cultural factors govern strategic priorities and corresponding behavior in cyberspace. Relatedly, Valeriano, Jensen, and Maness [7] allude to national expressions of cyber power as instruments of foreign policy. While not directly invoking strategic culture, they trace the preferences of Russia, China, and the United States to beliefs that pre-date cyberspace. For instance, Russian operations are characterized by low-level disruptions intended to shape public opinion. Its use of propaganda and misinformation through social media and defacement reflects preferences that emerged during the period of the Soviet Union. Cyber operations from China, in comparison, prioritize achieving an information advantage over

⁸ In this case, culture is treated as an ideational construct that offers insight as to how best to achieve specific goals. While it is relevant to inquire as to the sources of schemas, discussing this substantially impacts the length and framing of this article. However, we assert that schemas are the result of socialization 45. Lau, C.-M., L.M. Kilbourne, and R.W. Woodman, *A shared schema approach to understanding organizational culture change*. Research in Organizational Change and Development, 2003. **14**. into and competition between epistemic communities 17. Bloomfield, A., *Time to Move On: Reconceptualizing the Strategic Culture Debate*. Contemporary Security Policy, 2012. **33**(3): p. 437-461.. As decision-makers are integrated into a community, they adopt the underlying organizational culture that includes specific preferences and practices oriented on community objectives. Here, these communities exist as domestic organizations (e.g., the foreign or defense ministries) that compete for influence while moving to achieve specific strategic objectives relevant to the state 46. Eyal, G. and L. Buchholz, *From the Sociology of Intellectuals to the Sociology of Interventions*. Annual Review of Sociology, 2010. **36**: p. 117 - 137.. Organizations that succeed in doing so achieve a monopoly on preferences and practices to be utilized by the state. As these are reflections of their internal organizational culture, these are then subsumed into the wider, state-level strategic culture until such time that these no longer prove to be relevant, such as during periods of crisis 47. Maitlis, S. and S. Sonenshein, *Sensemaking in Crisis and Change: Inspiration and Insights From Weick (1988)*. Journal of Management Studies, 2010. **47**(3): p. 551-580, 48. Weber, K. and M.A. Glynn, *Making sense with institutions: Context, thought and action in Karl Weick's theory*. Organization Studies, 2006. **27**(11): p. 1639-1660..

⁹ Adapted from Klein's 49. Klein, Y., *A Theory of Strategic Culture*. Comparative Strategy, 1991. **10**(1): p. 3-23. earlier definition as *"the set of attitudes and beliefs held within a military establishment concerning the political objectives of war and the most effective strategy and operational method of achieving it."*

adversaries. This is representative of classic Chinese strategic thought such as *Shih*¹⁰. While American cyber operations, finally, reflect a preference for precise and degradative operations aimed at command-and-control systems. The technological demands of this strategy highlight American strategic culture with an emphasis on an engineering approach to security and the central role of technology¹¹. Finally, Kari and Pynnöniemi [54] employ strategic culture as an analytical framework to unpack Russian threat perception vis-à-vis cyberspace and assert that the dual narratives of a besieged fortress and technical inferiority inform its approach to cybersecurity. Consequently, it could be proposed that:

Proposition 1: *Strategic culture is employed as a cognitive schema that mediates the interpretation of strategic realities and shapes strategic preferences.*

Importantly, this proposition does not invalidate the significance of material factors. Instead, it asserts that these are considered insofar as these correspond with the expectations of the schema. Unfortunately, this increases the risk of bias. As noted by Meibauer [14], strategic failure occurs when "*individuals hold on to ideas that deviate too far from reality.*" Studies highlight the tendency of individuals to accept belief-consistent information while those that are not are readily discarded [44, 55, 56]. Consequently, schema-consistent attributes trigger the adoption of seemingly suitable schemas.

For cyber operations, misperception resulting from the use of related cognitive devices surface in several studies. Schneider [39] observes the tendency of elites to frame cyber operations as provocative. Despite a favorable balance of power, participants hesitate in exercising their cyber power. In this case, the strategic environment (i.e., the balance of power) is not ignored per se. Instead, participants who opposed the use of cyber operations perceived an equivalence between these and nuclear weapons in that both are viewed as destabilizing. Relatedly, two other studies [40, 57] demonstrate that absent additional information, decision-makers reference past adversarial behavior to form attributional judgments regardless of the availability of evidence arguing otherwise. Although these studies do not explicitly link misperception with the schematic use of strategic culture, these highlight the challenges associated with related cognitive devices.

While the shortcomings of schemas may be addressed by changing its structure to fit the strategic environment, this is not easily achieved as these are resistant to alteration given the imperative of maintaining cognitive consistency [44, 58]. However, the underlying motivations of decision-makers may offer a possible solution to circumvent this limitation.

In their study of electoral behavior, Taber et al. [59] note the role of motivational goals in moderating the effects of schematic thinking. Motivational goals offer insight regarding the influence that schemas, and in this case, strategic culture, have on preferences. Motivational goals are categorized into two distinct classes; accuracy goals that emphasize the importance of correct assessments, and directional goals that encourage the maintenance of exiting

¹⁰ Strategic power, defined as '*momentum, potential energy, force, the strategic configuration of power, strategic advantage*'.

¹¹ This also raises the corollary question of whether or not emergent technologies (e.g. cyberspace) not only trigger schematic usage; but inevitably result in their change. This remains a possibility provided that such instruments introduce a significant amount of dissonance that results in a reassessment of the said schemas.

beliefs [59, 60]. The former is considered cognitively strenuous, while the latter subjectively frames the information environment to align with pre-established beliefs.

While directional goals may spontaneously emerge as a result of the information environment (i.e., uncertainty) or due to urgency (i.e., the need for closure), accuracy goals may take precedence given individual or organizational prerogatives [59, 61]. Individuals may choose to engage in deliberate and effortful cognition if this increase accuracy and minimizes negative consequences¹². Consequently, while subjective assessments resulting from schematic thinking are likely to persist, incentives exist for decision-makers to assess the strategic environment objectively.

Objectively evaluating the expectations of specific schemas, while resource-intensive, is crucial. With respect to strategic interactions in cyberspace, the entanglement of issues requires careful consideration to avoid unintended escalation and the adoption of effective strategic choices [62, 63]. Consequently, decision-makers are advantaged when undertaking an objective assessment of the environment. Inversely, an over-dependence on cognitive devices such as schemas increases the risk of failure.

The benefits of overriding schema-derived preferences are highlighted given the anarchic structures and uncertainty of the international system [64]. With complete information, bias and misperception are unlikely as decision-makers have access to complete information. However, existing structural and cognitive constraints prompt bias due to the shortcomings of schematic thinking that obscures crucial strategic considerations, resulting in suboptimal policy choices [18]. Consequently, accuracy goals function as a filter with which schema-derived preferences are evaluated.

Like schemas, accuracy goals are not explicitly identified in the cybersecurity literature. One manifestation is the recognition of interdependencies between actors and the deleterious effects of aggression in cyberspace. This is found in cyber norms research such as that from Forsyth and Pope [28] which argues that awareness of the negative consequences of aggression eventually results in the establishment of norms. Similarly, Finnemore and Hollis [65] cite the failure to acknowledge contrasting worldviews as a stumbling block to the establishment of norms in cyberspace.

At the other end of the spectrum, deterrence research echoes the importance of accuracy. As proposed by Nye [62] and Brantly [63], deterrence by entanglement requires the recognition of interdependencies between actors. Specifically, recognition of the consequences faced by both parties deters malicious behavior. Relatedly, deterrence through deception (Gartzke and Lindsay [12] calls for knowledge of an aggressor's actual – rather than assumed (i.e., schema derived) – interests to allow defenders to tailor deterrence by deception accordingly. Consequently, it can be proposed that:

Proposition 2 *Accuracy goals moderate the adoption of schema-derived preferences by encouraging the objective assessment of the strategic environment.*

In arguing that strategic preferences result from the mediating effects of schemas which are further moderated by accuracy goals, the framework coincides with the cognitive-

¹² For instance, the deployment of the armed forces in response to an emergent threat may seem less appealing if doing so may incur political costs that elites may not wish to accept.

psychological model advanced by Goldgeier and Tetlock [66]. The authors assert that preferences arise from the '*systemic slippage between policy-guiding mental representations of reality and reality itself.*' This acknowledges the boundaries of human cognition while maintaining the possibility of deliberate and effortful assessments that captures the strategic realities faced by decision-makers. Consequently, this explains instances wherein state behavior results in either strategic success or failure and reaffirms the boundedness of human cognition.

Research Design

To demonstrate the feasibility of the proposed cognitive-cultural framework, the article utilizes observations from cross-national wargames conducted between 2019 and 2020. Wargaming permits the evaluation and analysis of behavior in the face of changing strategic contexts [67-69]. For cybersecurity scholarship, the use of wargaming as a mode of inquiry has only recently been adopted by a handful of scholars¹³ [39, 70-72].

Skepticism towards wargaming stems from its perceived subjectivity [73]. Wargames are seen to favor mundane realism and external validity at the cost of experimental realism and internal validity emphasized by modern social science research [74]. This dichotomous view, however, blinds scholars to its use as a legitimate research method.

As Schneider et. al. [70] argue, the benefits of wargaming is a function of the fundamental research goals with a distinction made between experimental and observational wargames. Experimental wargames prioritize internal validity and emphasizes the randomization of samples, the difference between control and treatment groups, multiple iterations, and an abstraction of the game environment [75]. These are akin to conventional laboratory experiments aimed at testing specific mechanisms. Observational wargames, inversely, sacrifice control over confounding variables and instead leverage variations between different participant groups while holding constant the in-game scenario¹⁴ [77, 78] to obtain external validity and heterogeneity. Consequently, researchers are faced with the choice between wargaming as a test for causal mechanisms or as an inductive theory-building tool.

As such, the article finds itself employing wargaming not as an explicit test of theory but as a plausibility probe to demonstrate the feasibility of the proposed framework¹⁵. In holding the scenario and participant background constant while varying nationality, differences in strategic preferences among participants given the schematic use of strategic culture are surfaced. Inversely, if participants objectively assess the strategic environment, preferences ought to be consistent across groups. This design adopts Mill's Method of Difference in which

¹³ Although similar activities such as the annual Locked Shields exercises have regularly taken place, the use of wargaming for the purpose of research is a novel phenomenon.

¹⁴ To an extent, wargames employed in this manner are akin to artefactual field experiments and framed field experiments 76. Harrison, G.W. and J.A. List, *Field Experiments*. Journal of Economic Literature, 2004. **42**(4): p. 1009-1055..

¹⁵ As proposed by George and Bennett 79. George, A.L. and A. Bennett, *Case studies and theory development in the social sciences*. BCSIA studies in international security. 2005, Cambridge, Mass.: MIT Press. xv, 331 p., a plausibility probe is a preliminary study of untested theories to determine whether or not further testing is warranted. With respect to cybersecurity, Schneider 39. Schneider, J., *Cyber and Crisis Escalation: Insights from Wargaming*. 2017, U.S. Naval War College. adopts a comparable approach in the study of decision-making behavior relative to wargaming results from the U.S. Naval War College.

cases are similar in all but one variable and differences in the outcome is attributed to variations of the variable in question.

Scenario Structure and Gameplay

The wargame consists of three rounds where participants play the role of government officials¹⁶ in Idemore in random groups consisting of three (3) participants. The use of fictitious countries minimize the risk of priming participants to align their behavior with expectations of certain real-world countries. The design encourages participants to be more forthcoming during both gameplay and debriefing as institutional prerogatives may bias their perception and inclination to voice out their opinions (e.g., hesitancy to react negatively against an ally).

Before receiving the materials, participants complete a survey measuring policy preferences and beliefs that may influence their in-game behavior. After which, participants read a briefing packet detailing the expectations of their assigned role and how it contributes to the overall strategic objective of Idemore. This functions to distance participants from outside influence.

The scenario depicts an escalating crisis between Idemore and its neighbor, Vadare. To nullify the confounding effects of the balance of power, both countries are described as near-peer adversaries. Teams are given information on every round regarding on-going cyber operations between the two. During round one, Idemorean media suffers a series of disruptive cyber operations. By round two, the situation escalates to operations targeting critical infrastructure¹⁷. For the first two rounds, attributional evidence suggests the possible involvement of Vadare. However, this is by no means unambiguous¹⁸. In the third round, a non-state actor claims credit for the incidents.

Besides incident information, teams are given details regarding the strategic relationship between Idemore and Vadare. Of note is a developing territorial dispute with the discovery of rare earth minerals along their shared border. This adds a degree of realism as real-world cybersecurity incidents are often contextualize by the underlying strategic environment [80]. Moreover, the saliency of this issue may restrain individuals from aggressively engaging with their adversary [81].

For every round, teams respond to developments by choosing from a fixed set of policy responses that range from inaction to military readiness¹⁹. The choices are based on a list of actions believed to be available to states facing similar real-world situations. It is important to note that previous choices influence events in succeeding rounds and reflect the consequential nature of interstate relations.

¹⁶ These roles are the defense minister, the foreign affairs minister, and the information and communications technology minister. The exact description and expectation for each role is found in Online Appendix.

¹⁷ During the second round, participants are chosen at random and are either told that the national tax system or the national healthcare system was infected with ransomware. This is done to test whether a variation in target types affects the overall decision-making process as conformed in a number of studies.

¹⁸ In keeping with the challenge of attribution, the information provided in the scenario does not provide teams with absolute certainty as to the culpability of Vadare. Moreover, additional information in the form of the strategic relationship between the two countries increases ambiguity surrounding attribution.

¹⁹ The list of response options is available in Online Appendix.

The wargame requires approximately two-hours to complete after which participants are debriefed. The debriefing questions are open-ended to allow participants to expound on their answers and to pursue relevant avenues of discussion. The debriefing was patterned after the Experience, Identify, Analyze, and Generalize (EIAG) model [82]. These are recorded with the consent of the participants and are transcribed for later analysis.

During gameplay, non-participatory observation is carried out by research assistants recruited for the activity. The number of research assistants varies based on the location of the wargame. At the very least, two observers are available to move between groups to observe their respective decision-making processes and discussion²⁰. Observers are instructed to pay special attention to (1) the use of in-game information, (2) the use of external information, (3) references to past experience, (4) employed to overcome uncertainty, and (5) sources and justification of preferences. Before gameplay, observers are given a copy of the debriefing questions to provide them with additional guidance.

Recruitment

Participants are recruited from a pool of individuals with military, policy, and cybersecurity expertise. Participants work in government or are part of an external organization that functions in an advisory or educational capacity (i.e., think tanks). While they may not have direct involvement with foreign policy decision-making, their experience parallels those that may be involved in such processes, making them suitable proxies compared to undergraduate students or the general public [83].

To recruit participants, we approached these organizations and pitched the wargame as an opportunity to test their knowledge and capability to respond to cybersecurity issues. In exchange, we provided access to the wargame material and held closed-door seminars discussing the lessons learned from the wargame. To address privacy concerns, personally identifiable information is not collected. Furthermore, reported results only identify the countries in which the participants are based instead of specific organizations.

Data Analysis

Data is derived from (1) in-game policy choices, (2) post-game debriefing, and (3) non-participant observer notes. These enable the analysis of team-specific discussions and allows the identification of the motivations that drive observable team-behavior.

Analysis of in-game policy choices is focused on its effects on the strategic relationship between Idemore and Vadare. As such, the analysis is concerned with both the form (e.g., do nothing versus retaliate) and strategic implications (e.g., status-quo versus escalation) of these choices. Moreover, these choices represent the means with which strategic objectives are achieved (e.g., exercising cyber power to signal resolve). Surfacing the link between choices and objectives, while not a definite test of the mechanism, strengthens the plausibility of the proposed framework.

²⁰ At best, a research assistant is assigned to each group.

Readers should note that, unlike the in-game policy choices and non-participant observations, the post-game debriefing is analyzed at the country-level. Consequently, the decisions made by teams and their discussions are interpreted in the broader context of the debriefing.

To identify country-level preferences, debriefing transcripts are thematically coded using the typology proposed by Kitchen [16] wherein preferences manifest as intentional and operational ideas. As mentioned previously, intentional ideas are normative beliefs representing specific foreign policy goals while operational ideas offer the means with which these are achieved. Consequently, in-game policy choices equate to operational ideas while intentional ideas manifest as themes that emerge during debriefing. Both intentional and operational ideas represent a schema from which preferences are derived to respond to the strategic environment.

Observations and Analysis

Wargames were conducted between August 2019 to May 2020 with teams from Singapore and the Philippines. Comparisons drawn between these two are ideal given that they (1) are regional neighbors that share a colonial history, (2) are engaged in regional cybersecurity programs, and (3) are increasingly dependent on cyberspace for socio-political and economic advancement. Consequently, one could assume that preferences during gameplay are comparable between the two.

In total, the behavior of eleven teams are analyzed; seven from the Philippines and four from Singapore²¹. Gameplay and debriefings were conducted in English and took approximately three hours to complete. In the case of Singapore, the wargame was held virtually in light of the COVID-19 pandemic.

As previously mentioned, a brief survey is distributed to measure preferences and beliefs that may influence in-game behavior. Using a modified version of Miggiotto and Wittkopf's [84] instrument, only two teams are shown to support militant foreign policies²². Interestingly, teams that opted for assertive policy choices supported cooperative foreign policies. Besides policy preference, risk acceptance may also influence behavior [85]. The survey found that teams from both countries are risk averse. Finally, domain expertise also influences perception and preferences for in-domain behavior [57, 86, 87]. Teams from Singapore appear knowledgeable while the majority of these from the Philippines (4 out of 7) had comparable levels of expertise with cybersecurity.

In-Game Policy Choices

In-game behavior for Singaporean and Philippine teams are comparable during the first round. During this round, teams are informed that cyber operations are disrupting systems operated by the Idemorean media. Moreover, the discovery of rare earth minerals along the shared border is increasing tensions between Idemore and Vadare.

²¹ 21 Individuals from the Philippines and 12 from Singapore.

²² One from each country. Moreover, these are the teams that decide to act more cautiously during gameplay.

<i>Team</i>	<i>Response (1)</i>	<i>Response (2)</i>	<i>Response (3)</i>
SG.1	Watch & Wait	Criminal Indictment	Suspend Decision
SG.2	Private Attribution	Military Standby	Continue Decision
SG.3	Watch & Wait	Military Standby	Continue Decision
SG.4	Watch & Wait	Criminal Indictment	Suspend Decision
PH.1	Private Attribution	Criminal Indictment	Suspend Decision
PH.2	Watch & Wait	Cyber Offensive	Suspend Decision
PH.3	Watch & Wait	Cyber Offensive	Suspend Decision
PH.4	Watch & Wait	Yield	Suspend Decision
PH.5	Watch & Wait	Military Standby	Suspend Decision
PH.6	Watch & Wait	Military Standby	Continue Decision
PH.7	Private Attribution	Military Standby	Continue Decision

Figure 1. In-Game Policy Choices

Uniformly, teams adopted a cautious approach and chose to either suspend further action in the hopes of gaining more information or attributed privately through diplomatic channels. Over two-thirds of teams from Singapore and the Philippines chose the former; acknowledging the limited information and the risk of escalation. Consequently, cautious behavior during the first round reflects findings from both observational studies and formal models [10, 88].

Behavior deviated by the second round when threats to Idemorean critical infrastructure appear. Additionally, information is provided suggesting a possible campaign of coercion initiated by Vadare. As seen in Figure 1, over two thirds (5) of the Philippine teams chose to either retaliate using cyber operations (2) or placed their military on alert (3). However, only half (2) of the Singaporean teams decided to place their military on alert.

For the Philippine teams, policy choices and the critical infrastructure targeted in the second round appear to be unrelated. Teams were just as likely to adopt an assertive posture regardless of whether the healthcare or tax system was affected. In contrast, the Singaporean teams adopted a seemingly paradoxical approach. Bucking the expectations of the early cybersecurity literature [89], the military was placed on alert when the tax, rather than the healthcare system, was targeted.

By the third round, behavioral divergences further solidified. When informed that a non-state actor claimed responsibility for the incidents, the majority of Philippine teams that responded assertively in the preceding round suspended their decision. Inversely, Singaporean teams chose to continue with placing their military on alert.

Teams from both countries appear to adopt distinct approaches in response to the strategic environment despite facing identical scenarios. While the Philippines was more assertive once critical infrastructure is threatened, they exercised restraint with the arrival of new information. Singapore, in contrast, appeared committed to their decision despite the availability of possibly disconformity evidence. While this suggests a difference in preferences, these variations alone do not confirm the existence of unique strategic objectives.

Strategic Objectives

During debriefing, teams were asked to identify their strategic goal(s). This line of questioning traces the underlying intentional idea(s) shaping their policy choices in each round. In doing so, themes surfaced during debriefing, supported by in-game observations, provides a link between strategic objectives and the means of achieving these.

For the Philippine teams, the prominent intentional ideas are (1) the need to defend and (2) attribution. One participant explains that, “[The] first [thing] that comes to my mind is to defend, and to find out solid evidence...” An emphasis on defense, however, does not suggest a desire for dominance over an adversary. In-game observations note that retaliatory cyber operations or placing the military on alert functions as communicative devices. Participants argue that these signal readiness and deters future threats.

Throughout gameplay, teams recognized the ambiguity surrounding attribution. This is prominent in the first round but tapers off as the situation developed. Of note is the absence of references to the ambiguity of the information environment in relation to the strategic objective(s) of the Philippine teams during debriefing. Relatedly, references to uncertainty regarding attribution became less salient once critical infrastructure was affected. This, however, does not imply the absence of strategic caution.

During gameplay, the Philippine teams justified their choices by citing an equivalence with Vadarean behavior that signals a shift towards an aggressive strategic posture. Consequently, they viewed their policy choices as non-escalatory and in keeping with the status-quo. For teams that chose not to be assertive, this behavior appears to be influenced by the aforementioned need to maintain the status-quo without necessarily having to match the actions of their adversary. Despite these differences, both recognized the need for defense while minimizing the risk of escalation and suggests a critical assessment of the strategic environment. However, the lack of emphasis on the ambiguity of the information hints at subjectivity on the part of the participants. Moreover, retaliatory cyber operations was framed as an ideal communicative instrument on the assumption of its lower cost vis-à-vis conventional tool. However, no information is provided to support this belief.

Collectively, the defensive posture adopted by the Philippine teams is envisioned as a deterrent strategy. The lack of distinction between incidents targeting the healthcare or tax systems, however, is puzzling. Even with limited expertise, the qualitative difference between targets and the consequences of actions against these is recognizable [87]. Fortunately, follow-up discussions offer further clarification.

Teams are asked how the severity of an incident was assessed and its influence over their interpretation of the strategic environment. For the Philippines, this evaluation is driven by both (1) the target of malicious behavior and (2) and the corresponding consequences. However, it is important to note that no explicit distinction made regarding the nature of the target (i.e., whether it has a direct bearing on human life). When asked, participants note that a cybersecurity incident is considered severe when it manifests national-level effects. Specifically, *“if it is a national threat level, it should involve more serious action like implanting malware, more serious damage, explosion, fire – that would be costly, something like that.”* Another participant explains that, *“If the infrastructure of utilities, electricity, water, transportation—if the attack affects the economy of the country, I will do everything to resolve it.”*

A crucial observation from these answers is the peculiar absence of a “red line” with respect to the loss of life. It appears that teams are forced into action when critical infrastructure, collectively, is under threat. Moreover, this signals a clear shift in the strategic relationship between the parties involved. As one participant notes, *“there’s denial of service already on our critical information and infrastructure, that [is] why I think the incident has already escalated.”*

Consequently, the strategic objective of the Philippine teams reflected by in-game policy choices and debriefing responses is one of projecting an assertive defensive posture to deter future threats while minimizing the risk of escalation. This aligns with what might be seen as the conventional wisdom of the geo-strategic position of the Philippines’ – an actor of middling capability set amidst several more capable actors and several overarching contentious intra-regional relationships.

Singaporean teams, in contrast, placed less importance on immediately responding and instead emphasized (1) risk avoidance and (2) strategic stability as their objectives throughout gameplay. As one participant reports, their goal was to *“acquire the highest amount of stability, with the highest amount of risk avoidance, and strategic caution as we could.”* Of interest is the assertion that their preferences were shaped by their national identity. During debriefing a participant explained that *“we probably used some sort of cultural or national ideas...”* Furthermore, another went on to say that *“since my group was composed of Singaporeans and above all we colleagues—we came to the time order that corresponds to Singapore...”*

Pursuing risk avoidance and strategic stability intersects Singaporean history as well with references to the 1991 *Pukul Habis* incident wherein Malaysia and Indonesia staged joint military exercises in close proximity to the Singaporean border²³. Given this reference, the decision to put the military on alert reflects the need to deter threats while minimizing the risk of escalation. From the perspective of teams supporting this approach, both cyber operations and economic sanctions were viewed as escalatory while yielding to demands or imposing criminal indictments were either unacceptable or ineffective.

Relatedly, teams that favored criminal indictments based their decision on the above-mentioned objectives albeit viewed from a different perspective. One team, for instance, points to the ambiguous attribution as limiting their choices, arguing that a criminal indictment is *“narrow enough”* to achieve their objective of deterrence without risking escalation. This divergence, however, is unsurprising as those that favored criminal indictments were theoretically at greater risk given the exploitation of the healthcare system.

Unlike the Philippine teams, ambiguity surrounding attribution continued to shape in-game discussions throughout gameplay. Although this may reflect caution among participants, unease towards the consequences of certain policy options (e.g., retaliation through cyberspace) remains unsubstantiated given the near-peer status between Idemore and

²³ In 1991, a joint military exercise between Malaysia and Indonesia near the Singaporean border resulted in the mobilization of the Singapore Armed Forces (SAF) 90. Boey, D., *A strong and silent keeper of the peace*, in *The Straits Times*. 2008, Singapore Press Holdings: Singapore.. This incident was unknown to the research team and similarities between it and the wargame scenario are purely coincidental.

Vadare. As proposed by Liff [91], the strategic situation enables greater freedom of action. Relatedly, Jensen and Valeriano [92] find that cyber operations function as conflict off-ramps. While this behavior echoes Schneider's findings that cyber operations are perceived as escalatory; it is unclear how the belief that military mobilization is less threatening than economic sanctions or retaliation cyber action emerged.

As with the Philippine teams, both the target and consequences of incidents contribute significantly to preference selection. However, thresholds are better defined for the Singaporean teams such that *"...there would be probably two sets of criteria...One would be when these cyber actions are affecting really either directly and in a life-threatening way the population, but in a much more systematic and hospital—that would affect the well-being of the—would become life-threatening to a population on a big scale. Or in terms of capability, an attack on a nation that would target in a direct or successful way, directly the defense and security capability, instead of attacking hospital, all the activities of the police, maybe the activities of the armed forces themselves that would be paralyzed."*

Interestingly, the salience of these thresholds coincides with the availability of information. As one participant explains, *"we did not have enough information to go into it. We were very cautious..."* This caution is reflected in the attributional challenge associated with cyber operations which is more prominent for the Singaporean teams with one participant arguing that *"because the scenario was so ambiguous, I wasn't actually sure who the originator of the attack was. It couldn't have been an act of war because it wasn't clear who the perpetrator was. I guess that limited our response."* Consequently, while teams from both countries were concerned with risk avoidance, Singaporean teams appear to have prioritized this along with strategic stability over the need for immediate action. As such, one could describe their strategic objective as one of restrained defense communicating resolve while avoiding further escalation.

The Role of Culture

Given the observed behavioral divergences, can this be traced to the schematic use of unique strategic cultures? Although the proposed framework addresses some of the core concerns involving the analytical use of strategic culture, caution is necessary. Specifically, both the theoretical framework and wargame design do not negate the possibility of multiple sub-cultures resulting in a plurality of schemas.

Rather than a single strategic culture, scholarship acknowledges the presence of sub-cultures [93] resulting from the competition between epistemic communities whose influence over policy fluctuates in response to the strategic environment [47, 48]. Consequently, preferences held by certain communities exerts greater influence if these result in strategic success. Inversely, failure triggers renewed competition, causing changes in preferences.

In the case of the Philippines, the prioritization of defense and immediate action reflects aspects of Philippine strategic culture. De Castro [94] argues that its archipelagic geography increases its vulnerability to foreign invasion. The plurality of islands in conjunction with resource constraints results in a preference for asymmetrical warfare and reliance on existing alliances. During gameplay, the decision by teams to either put their military on alert or to

resort to cyber operations as an asymmetric tool reflects this need for action while minimizing the risk of direct and costly engagement.

Relatedly, the inability to distinguish between categories of critical infrastructure and the severity of effects echoes the broad definition of national security in the Philippines as *“a state or condition wherein the people’s welfare, well-being, ways of life; government and its institutions; territorial integrity; sovereignty; and core values are enhanced and protected”* [95]. If cyberspace is perceived as an enabler of national development, it is unsurprising that disruptions to critical infrastructure – whether or not resulting in the loss of life – is viewed as a threat to national security. Consequently, this framing motivates defensive action. As noted in the latest iteration of the National Security Policy, *“The Philippines must demonstrate to the world that we are capable of protecting and defending what is ours, and that we shall fully assert and exercise our sovereign rights as a truly independent nation...”* [95]. It is unsurprising, then, that actors responsible for national defense align their actions with this objective. Within the wargame, the language used by the Philippine teams is reminiscent of this with recurring references to sovereignty and national defense.

Similarly, the behavior of the Singaporean teams mirror distinct features of Singaporean strategic culture. Given its geographic and material vulnerability, lacking both strategic depth and natural resources, Singaporean strategic culture is characterized by a *“profound continuity and an acute sense of vulnerability”* [96]. As noted by Acharya [97], this encourages the (mistaken) belief that Singaporean foreign policy is heavily influenced by a realist perspective. Upon inspection, however, its strategic outlook and behavior are more nuanced and not influenced exclusively by the tenets of realism and *realpolitik*.

Plainly stated, Singaporean strategic behavior is best characterized as the simultaneous use of both deterrence and diplomacy [98]. While there is no doubting the military prowess of the city state within the region, great care is taken to avoid appearing overly aggressive in the development and expansion of its military capabilities while simultaneously deterring threats to its security [99]. Complementing this, Singapore actively engages in diplomatic activities that establish stable and positive relationships [100].

This cautious yet pragmatic approach to national security is readily observed throughout gameplay. Even with teams that opted to place their militaries on alert, emphasis is given to pursuing a diplomatic solution while maintaining a posture of strength. For instance, one team argues that keeping the military on alert *“buys them time”* without necessarily escalating the situation and enabling continued diplomatic overtures.

Relatedly, teams that decided not to adopt an assertive posture cite the importance projecting strength, but not at the cost escalating the situation – especially given the pervasive ambiguity. These participants argue that the decision to issue criminal indictments, while not as assertive, addresses the need to deter (future) malicious behavior. Consequently, the case of the Singapore illustrates two distinct approaches (operational ideas) in pursuit of a single goal (intentional idea).

Information Processing and Accuracy Goals

While the framework asserts that preferences are the result of the schematic use of strategic culture, it further argues that accuracy goals moderate the extent to which these are adopted. Since accuracy goals motivate the precise assessment of the environment, their presence influences the manner and extent that information is processed and whether these activate or reinforce available schemas.

Consequently, analysis is focused on how uncertainty is resolved and the valuation of information. It is important to note that while participants recognized the uncertainty of the environment, distinct approaches are employed that influence the preferences that surface. For the Philippine teams, overcoming uncertainty involved the comparison and exchange of information. With respect to attribution, available evidence may emphasize the culpability of a certain actor while exonerating another, *"we will have candidates as to who the perpetrators are, and eliminate by means of the gravity of their contribution to the offense. If they don't have anything to do with it, we will eliminate them."* Significantly, participants did not gravitate towards a particular type of evidence and emphasized the need to *"consider everything"* and went so far as to argue that *"...we have a staple of assessments to evaluate, [we] look at advantages and disadvantages..."* Besides judging informational value, participants recognize the importance of exchanging information. As one participant explains, *"We will consider other agencies, for confirmation, get the details and complete structure of data, and come up with conclusion..."* and *"I think we will do collaboration with other decision-makers..."*

While these suggest the deliberate assessment of information, they do not indicate how information is valued and interpreted. For the Philippine teams, informational value is associated with role. As one participant explains, *"...from the point of view of the policy expert, is the information useful, or is it just there to confuse us? For cyber, it's more on figures. We scale the situation based on our point of view"* These distinctions extend to the responsibilities and objectives associated with these roles, *"[the] military group would be concerned with about protecting the sovereignty of the area, for cyber, it's about intelligence, offensive, defensive..."*

These cleavages are acknowledged by participants who recognize the importance of an independent arbiter *"because different groups (military, cyber, policy) have different perspectives."* However, there is no evidence to suggest that compromises were made to bridge contrasting perspectives. Instead, teams appear to have assigned one (or more) individual to arbitrate; *"our policy guy balances and weighs in on things, he tells us if it is a major threat, a national threat, or just a simple attack..."* relatedly, *"in the military and cyber group, their organizations have people who make the final decision..."* The absence of an impartial arbiter is problematic in terms of the emergence of accuracy goals. Directional goals may dominate if judgement is deferred to an individual with prior objectives and priorities in an uncertain environment, resulting in the perpetuation of these preferences [101]. Consequently, accuracy goals may only exert minimal influence.

For Singaporean teams, comparison and sharing are also viewed as important; *"...there was never a question that we would not need to share information or coordinate, etc."* Furthermore, uncertainty was expected, and teams made the most of the situation, *"we have to make the best decision that we can based on incomplete information or those that are*

completely unrelated.” Where the Singaporean teams differ is with respect to how information was valued.

Although role expectations remain, these are less pronounced and do not function as the primary frame through which information is valued. Instead, information is processed in the context of the relationship between the two countries. For instance, as the scenario progressed, one participant explains that their team did not choose to escalate since “...*the evidence suggests strongly that it was coming from [Vadare] but because of how we assess the power balance, we didn’t seem to have any significant advantage.*” Relatedly, another participant reflects that “...*I agree that probably if it’s not of—sort of a competition between two similar countries—but if there was an imbalance between them, it could have changed the dynamic...*”

On the one hand, this approach contributes to an objective assessment of the strategic environment that may result in preferential shifts, “...*If the power balance was different, it could have at least affected how we pursued this case.*” On the other hand, the emphasis on structure, especially for Singapore, may trigger specific schemas given the alignment between the available information and features of Singaporean strategic culture [44]. As previously mentioned, the pervasive sense of vulnerability calls for careful consideration of the strategic environment. Consequently, features of the wargame may activate schemas based on Singaporean strategic culture, suppressing accuracy goals in the process.

With this in mind, the extent to which accuracy goals temper the schematic use of strategic culture for these teams is difficult to establish. While evaluating the information based on the relationship between Vadare and Idemore contextualizes these events, doing so may activate schemas – as was seen with reference to the 1991 incident. Interestingly, this highlights a situation in which schemas and related cognitive structures may be advantageous. Gigerenzer [102] argues that cognitive shortcuts contribute to the accurate assessments of the information environment provided that these are ecologically rational. Phrased differently, benefits are realized (e.g., faster evaluation of an uncertain environment) if these cognitive shortcuts match the information environment they attempt to model.

While the near-peer relationship depicted in the wargame differs from Singapore’s relationship with its neighbors, some Singaporean teams recognized the interdependency that exist between Vadare and Idemore²⁴. Although not explicitly stated, this may result in parallels being drawn with Singapore’s own dependence on water from Malaysia which shaped its policy preferences post-independence [98]. Consequently, this increases the likelihood of using schemas that may be suitable for this particular situation.

A Cognitive-Cultural Approach to Cybersecurity

Though this article does not offer a definitive test of theory, it nevertheless makes a much-needed contribution insofar as the observations from the simulation clearly illustrate the importance of strategic culture as a schematic device. Despite facing identical scenarios, preferences were influenced by nationally-defined expectations with respect to strategic objectives. While this doesn’t preclude objective assessments of the strategic environment, it

²⁴ The scenario mentions that both Idemore and Vadare have an existing economic relationship based on agriculture and oil. However, no mention is made regarding the overdependence of one country on the other.

suggests that the tendency of decision-makers is to drift between reality and enduring mental representations.

In the case of the Philippines, a broad definition of national security and its experience with conflict encourages an assertive approach to cybersecurity incidents. This is manifested in attempts to defend its national security by means of an assertive but measured displays of power and by leveraging the perceived asymmetric benefits of cyber operations. In contrast, the Singaporean preference for the simultaneous use of deterrence and diplomacy is noticeable given the stated objectives of risk avoidance and strategic stability. Consequently, the decision to place their military on alert or issue criminal indictments reflects the need to discourage malicious behavior while simultaneously reducing the risk of escalation and keeping diplomatic channels open.

Although claiming that strategic behavior in cyberspace is solely attributable to the schematic use of strategic culture is unrealistic, the results do speak to the importance of these mechanisms in shaping the development of in-domain strategic preferences. Furthermore, with contemporary research calling into question “logic-of-the-domain” types of explanation for interstate behavior in cyberspace, an opportunity exists to enrich the theoretical underpinnings of the nascent field of cybersecurity.

The argument and probe provided in this article contain several critical implications for policy and practice. Naturally, one such implication is that strategic posture must be flexible to the inputs of those processes that attempt to contextualize adversary perspectives, including open-source, human and other intelligence gathering. This should be reflected as well in training and pedagogy on security in the digital domain, as the inclination towards certain forms of cyber-nationalistic posturing is surely inculcated during professional learning. Indeed, these areas of national defense process should be the focus of follow-on research. And another implication is quite simply that consistent self-assessment – particularly by independent parties – of operational assumptions is required to prevent the inculcation of harmful schema-selection practices resulting in the pervasion of bias in decision-making settings.

A final implication worth mentioning is that failure to recognize the degree to which uncertainty must be thought of as a dynamic variable whose impact is determined by cultural-cognitive context rather than a static fact of engagement in cyberspace could bring dire consequences. After all, where theories of victory and standard practice often harden over time for any institution, with cyber conflict deviant assumptions can be hard-wired into elements of the toolkit on several fronts. Particularly where future cyber conflict is likely to be shaped in no small way by advances in machine learning, defense institutions would do well to pay close and immediate attention to the dual threat of uncertainty on optimal practice found in (1) capabilities’ design features or requirements and (2) assumptions made about adversaries’ own schematic approach to digital warfare.

Finally, from a methodological standpoint, the findings presented in this article demonstrate the feasibility of wargaming as a useful instrument of research. Whereas experimental designs are increasingly offering opportunities to test theories pertinent to cybersecurity, observational wargames contribute to the equally important task of theory building where, despite growing interest in the field, cybersecurity continues to fall short of expectations.

The growing importance placed on cyberspace as an instrument of national power requires a rigorous understanding of how preferences emerge in response to strategic developments within this domain. While the use of schemas has become a mainstay over the past half-century and although skepticism continues to abound regarding the analytic value of strategic culture, these should not deter researchers from employing these tools to gain a better understanding of state behavior in this man-made domain.

References

1. Harknett, R.J. and M. Smeets, *Cyber campaigns and strategic outcomes*. Journal of Strategic Studies, 2020.
2. Axelrod, R. and R. Iliev, *Timing of cyber conflict*. Proceedings of the National Academy of Sciences, 2014. **111**(4): p. 1298-1303.
3. Rovner, J., *Cyber War as an Intelligence Contest*, in *War on the Rocks*. 2019, Texas National Security Review.
4. Fischerkeller, M.P. and R.J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation*. Orbis (Summer 2017), 2018. **61**(3): p. 381-393.
5. Saltzman, I., *Cyber posturing and the offense-defense balance*. Contemporary Security Policy, 2013. **34**(1): p. 40-63.
6. Iasiello, E., *Cyber attack: A dull tool to shape foreign policy*, in *2013 5th International Conference on Cyber Conflict*, K. Podins, J. Stinissen, and M. Maybaum, Editors. 2013, IEEE: Tallinn. p. 451-470.
7. Valeriano, B., B. Jensen, and R.C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*. 2018, New York: Oxford University Press.
8. Slayton, R., *What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*. International Security, 2017. **41**(3): p. 72-109.
9. Pytlak, A. and G.E. Mitchell, *Power, rivalry, and cyber conflict: an empirical analysis*, in *Conflict in cyber space : theoretical, strategic and legal perspectives*, K. Friis and J. Ringsmose, Editors. 2016, Routledge: London. p. 65-82.
10. Maness, R.C. and B. Valeriano, *The Impact of Cyber Conflict on International Interactions*. Armed Forces & Society, 2016. **42**(2): p. 301-323.
11. Buchanan, B., *The Cybersecurity dilemma: Hacking, trust and fear between nations*. 2017, London: Hurst & Company.
12. Gartzke, E. and J.R. Lindsay, *Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace*. Security Studies, 2015. **24**(2): p. 316-348.
13. Lin, H.S., *Attribution of malicious cyber incidents: From soup to nuts*. 2016.
14. Meibauer, G., *Interests, Ideas, and the Study of State Behaviour in Neoclassical Realism*. Review of International Studies, 2019: p. 1 - 17.
15. Dueck, C., *Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy*. Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy, 2006: p. 1-224.
16. Kitchen, N., *Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation*. Review of International Studies, 2010. **36**(1): p. 117-143.
17. Bloomfield, A., *Time to Move On: Reconceptualizing the Strategic Culture Debate*. Contemporary Security Policy, 2012. **33**(3): p. 437-461.
18. Kertzer, J.D. and J. Renshon, *Putting Things in Perspective: Mental Simulation in Experimental Political Science*. 2015.
19. Kertzer, J.D., R. Brutger, and K. Quek, *Strategic Empathy and the Security Dilemma: Cross-National Experimental Evidence from China and the United States*. 2018.
20. Baker, J., *The Empathic Foundations of Security Dilemma De-escalation*. Political Psychology, 2019. **40**(6): p. 1251-1266.
21. Keller, J.W. and Y.E. Yang, *Empathy and Strategic Interaction in Crises: A Poliheuristic Perspective*. Foreign Policy Analysis, 2009. **5**(2): p. 169-189.

22. Kuehl, D.T., *From Cyberspace to Cyberpower: Defining the Problem*, in *Cyberpower and National Security*, F.D.S. Kramer, Stuart H.; Wentz, Larry, Editor. 2009, Potomac Books: Dulles. p. 24-42.
23. Borghard, E.D. and S.W. Loneragan, *The Logic of Coercion in Cyberspace*. Security Studies, 2017. **26**(3): p. 452-481.
24. Lindsay, J., *Stuxnet and the Limits of Cyber Warfare*. Security Studies, 2013. **22**(3): p. 365-404.
25. Dunn Cavelt, M., *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*. International Studies Review, 2013. **15**(1): p. 105-122.
26. Brantly, A.F., *The decision to attack: military and intelligence cyber decision-making*. Studies in security and international affairs. 2016, Athens, GA: The University of Georgia Press. xvi, 226 pages.
27. Rathbun, B.C., *Uncertain about uncertainty: Understanding the multiple meanings of a crucial concept in international relations theory*. International Studies Quarterly, 2007. **51**(3): p. 533-557.
28. Forsyth Jr, J.W. and M.B.E. Pope, *Structural Causes and Cyber Effects Why International Order is Inevitable in Cyberspace*. Strategic Studies Quarterly, 2014. **8**(4).
29. Perrow, C., *Normal accidents : living with high-risk technologies*. Princeton paperbacks. 1984, Princeton, N.J.: Princeton University Press. x, 451 p.
30. Schneider, J., *The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War*. Journal of Strategic Studies, 2019. **42**(6): p. 841-863.
31. Healey, J., *Winning and losing in cyberspace*, in *2016 8th International Conference on Cyber Conflict*, N. Pissanidis, H. Rõigas, and M. Veenendaal, Editors. 2016, IEEE: Tallinn. p. 37-49.
32. UNIDIR, *The Cyber Index: International Security Trends and Realities*, U.N.I.f.D. Research, Editor. 2013, United Nations Institute for Disarmament Research: Geneva. p. 9-90.
33. Egloff, F., *Public Attribution of Cyber Intrusion*. 2020.
34. Gartzke, E. and J.R. Lindsay, *Thermonuclear cyberwar*. Journal of Cybersecurity, 2017. **3**(1): p. 37-48.
35. Baram, G. and K. Lim. <https://www.timesofisrael.com/report-israeli-cyberattack-caused-iran-nuclear-site-fire-f35s-hit-missile-base/>. 2020 05.06.2020 [cited 2020 15.07]; Available from: <https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/>.
36. Herrmann, R.K., et al., *Images in international relations: An experimental test of cognitive schemata*. International Studies Quarterly, 1997. **41**(3): p. 403-433.
37. Rascagneres, P. and M. Lee, *Who Wasn't Responsible for Olympic Destroyer?*, in *Talos Intelligence*. 2018, Talos.
38. Power, R. *The Solar Sunrise Case: Mak, Stimpy, and Analyzer Give the DoD a Run for Its Money*. InformIT 2000 30.10.2000 [cited 2018 01.11]; Available from: <http://www.informit.com/articles/article.aspx?p=19603&seqNum=4>.
39. Schneider, J., *Cyber and Crisis Escalation: Insights from Wargaming*. 2017, U.S. Naval War College.
40. Gomez, M.A., *Past behavior and future judgements: seizing and freezing in response to cyber operations*. Journal of Cybersecurity, 2019. **5**(1): p. tyz012.

41. Rid, T. and B. Buchanan, *Attributing Cyber Attacks*. Journal of Strategic Studies, 2015. **38**(1-2): p. 4-37.
42. Morgan, F.E., *Compellence and the strategic culture of imperial Japan implications for coercive diplomacy in the twenty-first century*. 2003, Westport, Conn.: Praeger. 294 S.
43. Jervis, R., *Understanding beliefs and threat inflation*. American Foreign Policy and the Politics of Fear: Threat Inflation since, 2009. **9**(11): p. 16-39.
44. Larson, D.W., *The role of belief systems and schemas in foreign policy decision-making*. Political Psychology, 1994: p. 17-33.
45. Lau, C.-M., L.M. Kilbourne, and R.W. Woodman, *A shared schema approach to understanding organizational culture change*. Research in Organizational Change and Development, 2003. **14**.
46. Eyal, G. and L. Buchholz, *From the Sociology of Intellectuals to the Sociology of Interventions*. Annual Review of Sociology, 2010. **36**: p. 117 - 137.
47. Maitlis, S. and S. Sonenshein, *Sensemaking in Crisis and Change: Inspiration and Insights From Weick (1988)*. Journal of Management Studies, 2010. **47**(3): p. 551-580.
48. Weber, K. and M.A. Glynn, *Making sense with institutions: Context, thought and action in Karl Weick's theory*. Organization Studies, 2006. **27**(11): p. 1639-1660.
49. Klein, Y., *A Theory of Strategic Culture*. Comparative Strategy, 1991. **10**(1): p. 3-23.
50. DiMaggio, P., *Culture and Cognition*. Annual Review of Sociology, 1997. **23**(1): p. 263 - 287.
51. Rathbun, B.C., et al., *Taking Foreign Policy Personally: Personal Values and Foreign Policy Attitudes*. International Studies Quarterly, 2016. **60**(1): p. 124-137.
52. Jervis, R., *Perception and misperception in international politics*. New edition. ed. 1976, Princeton: Princeton University Press. pages cm.
53. Hare, F., *The Cyber Threat to National Security: Why Can't We Agree?* Conference on Cyber Conflict, Proceedings 2010, 2010: p. 211-225.
54. Kari, M.J. and K. Pynnöniemi, *Theory of strategic culture: An analytical framework for Russian cyber threat perception*. Journal of Strategic Studies, 2019: p. 1 - 29.
55. Holsti, O.R., *The belief system and national images: A case study*. Journal of Conflict Resolution, 1962. **6**(3): p. 244-252.
56. Crocker, J., S.T. Fiske, and S.E. Taylor, *Schematic bases of belief change*, in *Attitudinal judgment*. 1984, Springer. p. 197-226.
57. Gomez, M.A., *Sound the alarm! Updating beliefs and degradative cyber operations*. European Journal of International Security, 2019: p. 1 - 19.
58. Welch, D.A., *Painful choices: a theory of foreign policy change*. 2011, New Jersey: Princeton University Press.
59. Taber, C.S., M. Lodge, and J. Glathar, *The motivated construction of political judgments*, in *Citizens and politics: Perspectives from political psychology*, J.H. Kuklinski, Editor. 2001, Cambridge University Press: Cambridge. p. 198-226.
60. Ford, T.E. and A.W. Kruglanski, *Effects of epistemic motivations on the use of accessible constructs in social judgment*. Personality and Social Psychology Bulletin, 1995. **21**(9): p. 950 - 962.
61. Kruglanski, A.W. and D.M. Webster, *Motivated closing of the mind:" Seizing" and" freezing."* Psychological review, 1996. **103**(2): p. 263.
62. Nye, J.S., *Deterrence and dissuasion in cyberspace*. International Security, 2017. **41**(3): p. 44-71.
63. Brantly, A.F., *Entanglement in Cyberspace: Minding the Deterrence Gap*. Democracy and Security, 2020: p. 1 - 24.

64. Fearon, J.D., *Rationalist Explanations for War*. International Organization, 1995. **49**(3): p. 379-414.
65. Finnemore, M.H., Duncan B., *Constructing Norms for Global Cybersecurity*. American Journal of International Law, 2016. **110**(3): p. 425-479.
66. Goldgeier, J.M. and P.E. Tetlock, *Psychology and International Relations Theory*. Annual Review of Political Science, 2001. **4**: p. 67 - 92.
67. Smith, R., *The Long History of Gaming in Military Training*. Simulation & Gaming, 2010. **41**(1): p. 6-19.
68. Kriz, W.C., *Historical Roots and New Fruits of Gaming and Simulation*. Simulation & Gaming, 2017. **48**(5): p. 583-587.
69. Caffrey, M.B., *On wargaming: How wargames have shaped history and how they may shape the future*. 2019, Newport, NJ: Naval War College Press.
70. Schechter, B., J. Schneider, and R. Shaffer, *Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming*. Simulation & Gaming, 2021.
71. Jensen, B. and B. Valeriano, *The Cyber Character of Crisis Escala*, in *International Studies Association Annual Convention*. 2019, International Studies Association: Toronto.
72. Gomez, M.A. and C. Whyte, *Cyber Wargaming: Grappling with Uncertainty in a Complex Domain*. Defense Strategy and Assessment Journal, 2020. **10**(1): p. 98-139.
73. Perla, P.P., *The Art of Wargaming: A Guide for Professionals and Hobbyists*. 1990, Annapolis: Naval Institute Press.
74. Falk, A. and J.J. Heckman, *Lab Experiments Are a Major Source of Knowledge in the Social Sciences*. Science, 2009. **5952**(326): p. 535-538.
75. McDermott, R., *Experimental methodology in political science*. Political Analysis, 2002: p. 325-342.
76. Harrison, G.W. and J.A. List, *Field Experiments*. Journal of Economic Literature, 2004. **42**(4): p. 1009-1055.
77. Morton, R.B. and K.C. Williams, *Experimental Political Science and the Study of Causality: From Nature to the Lab*. 2010, New York: Cambridge University Press.
78. Gerber, A.S. and D.P. Green, *Field experiments: Design, analysis, and interpretation*. 2012, New York: W W Norton.
79. George, A.L. and A. Bennett, *Case studies and theory development in the social sciences*. BCSIA studies in international security. 2005, Cambridge, Mass.: MIT Press. xv, 331 p.
80. Valeriano, B. and R.C. Maness, *Cyber war versus cyber realities : cyber conflict in the international system*. 2015, Oxford ; New York: Oxford University Press. xiv, 266 pages.
81. Mauslein, J.A. and J. Pickering, *Rivalry Type and Cyber Operations: "Hot" Rivalries, "Cold" Rivalries, and Cyber Incidents, 1990–2009*. Peace Economics, Peace Science and Public Policy, 2021.
82. Stadsklev, R., *Handbook of Simulation Gaming in Social Education*. 2013, Scotts Valley: CreateSpace Independent Publishing Platform.
83. Mintz, A., S.B. Redd, and A. Vedlitz, *Can we generalize from student experiments to the real world in political science, military affairs, and international relations?* Journal of Conflict Resolution, 2006. **50**(5): p. 757-776.
84. Maggiotto, M.A. and E.R. Wittkopf, *American public attitudes toward foreign policy*. International Studies Quarterly, 1981. **25**(4): p. 601-631.

85. Kertzer, J.D., *Resolve, time, and risk*. International Organization, 2017. **71**(S1): p. S109-S136.
86. Kostyuk, N. and C. Wayne, *The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public*. Journal of Global Security Studies, 2020.
87. Shandler, R., M.L. Gross, and D. Canetti, *A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel*. Contemporary Security Policy, 2021: p. 1-28.
88. Edwards, B., et al., *Strategic aspects of cyberattack, attribution, and blame*. Proceedings of the National Academy of Sciences, 2017: p. 201700442.
89. Clarke, R.A. and R.K. Knake, *Cyber war*. 2014: Tantor Media, Incorporated.
90. Boey, D., *A strong and silent keeper of the peace*, in *The Straits Times*. 2008, Singapore Press Holdings: Singapore.
91. Liff, A.P., *Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war*. Journal of Strategic Studies, 2012. **35**(3): p. 401-428.
92. Jensen, B. and B. Valeriano, *What Do We Know About Cyber Escalation? Observations from Simulations and Surveys*, in *Issue Brief*. 2019, Scowcroft Center for Strategy and Security.
93. Libel, T., *Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy*. Defence Studies, 2016. **16**(2): p. 137 - 156.
94. De Castro, R.C., *Philippine Strategic Culture: Continuity in the Face of Changing Regional Dynamics*. Contemporary Security Policy, 2014. **35**(2): p. 249-269.
95. NSC, *National Security Policy for Change and Wellbeing of the Filipino People*, N.S. Council, Editor. 2017, National Security Council: Manila.
96. Er, L.P., *Singapore Security Outlook 2017: Between a Rock and a Hard Place*, in *Security Outlook of the Asia Pacific Countries and Its Implications for the Defense Sector*. 2018, The National Institute for Defense Studies: Tokyo.
97. Acharya, A., *Rethinking Singapore's Foreign Policy*, in *Singapore's Foreign Policy: The Search for Regional Order*. 2008, World Scientific: Denver. p. 1-10.
98. Matthews, R. and N.Z. Yan, *Small country 'total defence': a case study of Singapore*. Defence Studies, 2007. **7**(3): p. 376-395.
99. MINDEF, *Factsheet - About Total Defence*, M.o. Defence, Editor. 2004, Ministry of Defence: Singapore.
100. Capie, D., *Structures, shocks and norm change: explaining the late rise of Asia's defence diplomacy*. Contemporary Security Policy, 2013. **35**(1): p. 1-26.
101. Saunders, E.N., *No Substitute for Experience: Presidents, Advisers, and Information in Group Decision Making*. International Organization, 2017. **71**: p. S219-S247.
102. Gigerenzer, G., *Why Heuristics Work*. Perspectives on Psychological Science, 2008. **3**(1): p. 20-29.