



Research paper

Unpacking strategic behavior in cyberspace: a schema-driven approach

Miguel Alberto Gomez ^{1,*} and Christopher Whyte ²

¹Center for Security Studies, ETH, Haldeneggsteig 4, IFW, Zürich 8092, Switzerland and ²L. Douglas Wilder School of Government and Public Affairs, Virginia Commonwealth University, Scherer Hall, 923 W. Franklin St., Richmond, VA 23284, USA

*Correspondence address. Center for Security Studies, ETH, Haldeneggsteig 4, IFW, Zürich 8092, Switzerland.

Tel: +41 446338750; E-mail: miguel.gomez@sipo.gess.ethz.ch

Received 9 April 2021; revised 11 March 2022; accepted 1 April 2022

Abstract

The contemporary literature on cybersecurity and related interstate interactions often cites the need to overcome uncertainty due to an inherent information deficit about cyber operations. While this notion remains relevant in studies that advance our understanding of state behavior in cyberspace, noticeable gaps persist. These 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 of achieving these. Consequently, the article is an initial foray aimed at expanding our understanding of interstate behavior in cyberspace.

Key words: cybersecurity, wargame, decision-making, schemas

Introduction

Scholarship on cybersecurity and state interactions online ubiquitously cites the perceived strategic benefits offered by cyber operations [1]. However, the benefits of these operations and how they precisely scale to help secure strategic objectives are questions that receive different answers depending on the stakeholder. Even a cursory review of either cyber conflict scholarship or practitioner documents and statements show that while many truisms about engagement in cyberspace abound, a much greater number of underlying assumptions constitute the logical foundation upon which different cybersecurity stakeholders, from policymakers to military officers and technical operators, layer incoming information, and thereafter make decisions. Consequently, it is surprising how little is said about the sources of preferences held by these individuals on the role of cyber operations.

Research in this area focuses on how capable cyber actors are forced to try and overcome uncertainty, precisely that which emerges from the underlying characteristics of the digital domain to have

ubiquitous effects on state behavior [2, 3]. Recent scholarship and strategic posturing have often concluded that mitigating uncertainty necessitates the offensive use of cyber operations to discourage adversaries and achieve a favorable balance of power [4, 5], corresponding with the “revolutionary” narrative often associated with cyberspace. The issue with such a position is that its logic is derived from a commonly held belief that there is a “logic” of the cyberspace domain itself, i.e. architecturally detached from human inputs. However, empirical evidence lends credence to the idea that cyber conflict’s operational dynamics are fluid, as much determined by socio-institutional context as technical characteristics. Consequently, thinking about uncertainty in cyber operations as solely dependent on the reasoning of domain characteristics is no longer a tenable proposition.

This article addresses uncertainty in cyber engagement pertaining to evolving trends in global cyber conflict. Contrary to conventional expectations, available data analyses of global cyber events suggest that cyber conflict remains strategically limited despite

advances in material and organizational capabilities [6, 7]. Even with reduced operational requirements¹, its latent strategic potential remains the purview of established powers [8, 9] and not so often, as many have long feared, a weapon for the weak. Capable state actors themselves, however, appear restrained in their exercise of power through cyberspace. This results in sustained interactions well below the threshold of armed conflict, against the expectations of the early literature and pundits alike [4, 10], that introduce stakeholder preferences into the contours of foreign policymaking in a more persistent fashion than is found in other domains of interstate engagement.

In the following sections, we argue that stakeholders consider the prevailing wisdom about the logic of cyber engagement in the context of their strategic position and then lean into practices and postures that closely align with schema perceived to be beneficial. In doing so, we assert that uncertainty must be thought of more dynamically than is presently the norm in research and policy work on contestation online. Specifically, uncertainty is a dynamic variable whose impact is determined by cultural-cognitive context rather than a static fact of engagement in cyberspace. This view is additive, implying that the focus of prevailing thinking on the need to overcome uncertainty is only partly insufficient. In contrast with other work on uncertainty and risk in cyberspace, we assume 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.

Defined as *a set of beliefs held by elites concerning the strategic objective and how best to achieve it* [14], the ambiguity of the environment leads to the use of strategic culture as a cognitive schema that corresponds to intentions and those actions necessary to carry them out². Following an external stimulus (i.e. the strategic environment), these schemas are activated to shape the preferences and actions of decision-makers.

Naturally, efforts to address ambiguity do not necessarily produce schematic thinking that accurately captures the operational and strategic environment [15–18]. To objectively evaluate the environment and mitigate the effects of schema-driven biases, decision-makers must construct and orient on accuracy goals [19–22]. Motivated by the need to avoid the consequences of policy failure, decision-makers moderate schematic thinking in favor of what they perceive to be objective assessments of the strategic environment. This process that we describe is, of course, recursive, given that prior cultural postures impact the definition of strategic conditions both in and out of cyberspace.

This article illustrates the feasibility of this argument using 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 *vis-à-vis* cyber conflict, not least that socio-organizational adversary assessments play a significant role in shaping and reshaping preferences over time. Consequently, the article finds itself among research that attempts to unpack strategic behavior in cyberspace by complement-

ing system-level and technology-driven explanations with insight regarding the cognitive processes of decision-makers that influence actions in the domain³. Methodologically, we align with recent work [23–25] noting that wargames 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 introduces the theoretical framework and discusses the proposed cognitive-cultural mechanism grounded in the interaction between schemas and accuracy goals. We then discuss the wargame design, emphasizing relevant limitations and benefits for this article. 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 implications for policy, theory, and methodology.

Theoretical Framework

The growth of state-associated cyber operations⁴ continues to stimulate advancements in cybersecurity scholarship. Citing cyberspace as a pillar of national power [26], scholars and policymakers 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 to pursue strategic objectives through cyberspace⁵.

Despite this conceptualization and advancing actor capabilities, the strategic utility of cyber operations remains in doubt. Iasiello [6] asserts that cyber operations are blunt instruments that fail to influence adversarial behavior strategically, with damage inflicted to and through cyberspace remaining transient at best [27, 28]. Furthermore, although barriers to operation often seem low, the resources required to achieve strategically relevant outcomes can be prohibitive, limiting the number of cyber-capable actors [8, 9]. Consequently, interactions in cyberspace do not appear to adhere to earlier expectations of unbridled conflict [29]. Instead, while sustained, interstate exchanges in this domain are less violent than initially suggested [10]. This calls into question explanations rooted in both the technical characteristics and increasing socio-political relevance of cyberspace. Moreover, though it would be disingenuous to claim that this is not addressed by contemporary scholarship, it would be equally shortsighted to conclude that a unanimous understanding of in-domain state behavior exists.

Prevailing arguments

A significant aspect of the debate surrounding cyber operations involves uncertainty and its mitigation [30, 31]. Broadly, uncertainty is understood as either resulting from informational deficits or ambiguity [32]. The former emerges from the inherent difficulties in retrieving data sufficient to evaluate adversarial capabilities and identity. In

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

2 Much like hierarchical action schemas proposed by Meibauer [15] in which parent schemas define high-level objectives to be achieved by low-level child schemas.

3 It is important to note that cognition only forms one aspect of the decision-making process, which is the primary focus of this article. And while decision-makers do not necessarily share cognitive processes, the situation may prompt the activation of similar mechanisms.

4 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.

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

contrast, the latter arises from challenges of extracting meaning⁶ and the interpretation of behavior. While both help explain state behavior, the former dominates the cybersecurity literature [4, 33].

These deficit-based explanations highlight how interconnectedness and complexity introduce challenges in anticipating vulnerabilities and their corresponding effects [34]. Compounding this unpredictability is the perceived potential for malicious exploitation and the prospect of significant cascading effects [5]. Building on this, scholars argue [35, 36] that technological dependence promotes instability given the perceived necessity of offensive actions to guarantee ongoing access to cyberspace. When one considers the ongoing shortage of cybersecurity expertise even amongst established powers [37], this engenders a sense of unknowability, unpredictability, and inevitability that motivates policy and military elites to adopt steps to secure strategic interests and highlights the potential of offensive cyber operations [30]. However, this is not unique to cyberspace with scholars such as Posen [38], who recognizes the value of adopting offensive strategies as a means of shaping the battlespace and overcoming informational deficits.

This approach, however, is insufficient as cyber operations are yet to demonstrate their ability to shift the balance of power within the international system, limiting the amount of information gathered by aggressors that attempt to shape the environment [10, 39]. Furthermore, others note [8, 9, 28] that these operations are more resource-intensive than initially conceived. Consequently, continued investment in cyber capabilities appears counterintuitive, especially for materially constrained actors [40]. Blessing [41], for instance, identifies the existence of cyber forces in 61 UN-member states. This is surprising as cyber operations, particularly those with the potential for significant damage, appear limited to a handful of states [10]. Moreover, these states appear to be operating well-below their assumed capabilities. Some posit that this restraint suggests agreed competition between cyber powers [42]. Maintaining offensive operations below a tacit threshold allows the pursuit of strategic interests and the signaling of resolve without risking escalation⁷. Jensen and Valeriano [43] propose that limited offensive operations function as conflict off-ramps between adversaries. In effect, the observed restraint serves a communicative role, potentially increasing the information available between adversaries.

While helpful, these frameworks are limited in their ability to explain the behavior of emergent actors in cyberspace or actions outside the context of established rivalries. In effect, these apply to situations wherein uncertainty due to limited information is manageable owing to established behavior patterns and expectations outside cyberspace [10].

Ambiguity, in contrast, invokes a different set of challenges and solutions. Unlike conventional instruments, some argue that cyber operations are of limited communicative value [11]. Espionage operations, for instance, share technical similarities with offense-oriented operations (i.e. the code used or the process leading to their execution appear similar without further technical analysis and the inclusion of strategic context). Consequently, distinguishing intent poses

a significant challenge such that preferences may not be oriented toward shaping the environment to gain more information regarding capabilities and identity. But is, instead, concerned with discerning the meaning of events.

As such, cybersecurity scholarship increasingly recognizes the role of informational ambiguity in shaping digital interactions. Egloff [44] argues that advances in digital forensics mark a shift in attributing cyber operations away from sense-making to meaning-making activities focused less on “who” and more on what ought to be done. Similarly, Brantly [31] acknowledges the value of behavioral information in the domain, but recognizes the subjectivity in its interpretation. Relatedly, Buchanan [11] echoes a similar concern when noting the subjective interpretation of cybersecurity incidents and argues that existing disputes are likely to influence judgments. Finally, Gartzke and Lindsay [45] posit that ambiguity increases in salience with respect to the target’s perceived value. Consequently, subjective interpretations reflect the ambiguity faced by decision-makers when evaluating the strategic environment [32]. Empirically, these concerns are surfaced in both real-world cases and experimental research.

Regarding real-world events, one needs to look no further than the assumptions that abound following severe cybersecurity incidents. In July 2020, an Israeli cyber operation purportedly resulted in an explosion at Iran’s Natanz nuclear enrichment facility. Initial reports suggest that this was in response to earlier Iranian attempts to compromise the Israeli water distribution system [46]. Although 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. This cognitive mechanism⁸, in the form of enemy images [47, 48] and the representativeness heuristic [49, 50], is not unexpected and is seen in other instances, such as with the cyber operations that targeted the opening ceremony of the Pyeongchang Winter Olympics in 2018⁹ [51] and those affecting the US Department of Defense (DoD) network in 1998¹⁰ [52].

Experimentally, Schneider [53] 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 adversaries will 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 onto adversaries to ascertain possible reactions (i.e. mirror imaging). Furthermore, additional information fails to resolve questions of ambiguity [54]. Despite the availability of information, decision-makers maintain prior beliefs and attempt to draw parallels with past incidents in the process.

While technological and procedural developments increase the availability of information and minimize uncertainty in certain situations [55], characteristics of the domain and the strategic environment obscure the meaning and consequences of cyber operations. Consequently, contemporary cybersecurity research implicitly recognizes that cyberspace suffers from an excess of ambiguity¹¹ rather

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

7 An alternative perspective holds that domain characteristics do not exacerbate escalation risks so much as they attenuate those risks; citing for instance the resilience of cyberspace as limiting the expected damage. However, this framework does not improve upon the restraint analytic proposition, offering little in the way of explaining actor-specific behavior (see [4, 37]).

8 Historical interactions between Israel and Iran lead to the creation of images that shape behavioral expectations [48]. Moreover, these images extend to interactions beyond those which initially created them [49] and are difficult to dislodge even in the face of contradictory information.

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

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

11 Moving forward, uncertainty and ambiguity are used interchangeably.

than a deficit of information that provokes cognitive mechanisms that shape preferences concerning cyberspace.

Schemas and cyber operations

While several cognitive devices exist to overcome uncertainty¹², 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 [56]. Schemas share similarities with beliefs that influence crucial cognitive processes such as (1) setting and influencing expectations, (2) establishing the plausibility of particular judgments, and (3) constraining Bayesian updating¹³ [57]. This does not suggest that other cognitive constructs do not influence decision-making in response to cybersecurity incidents [53, 58]. Instead, the article proposes that schemas explain the link between (1) available information, (2) its interpretations, and (3) preferences in response to informational ambiguity.

Schemas establish the range of acceptable options in response to the environment while acknowledging the continued relevance, though possibly diminished, of empirical realities faced by an actor [18]. Crucially, schemas offer a means to overcome uncertainty prevalent in the international system by serving as templates applied to the interpretation of the strategic environment. That said, empirical realities faced by decision-makers are interpreted through this schematic lens, such that information deemed irrelevant to the execution of the schema is excluded, while missing information is assumed to exist in keeping with schematic expectations. In doing so, ambiguity is nullified by assuming the presence and meaning of conditions and attributes that activate these schemas [59].

While different schemas develop throughout an individual's life, this article is concerned with how strategic culture¹⁴, a *set of beliefs held by elites concerning the strategic objective and how best to achieve it*¹⁵, manifests as a cognitive schema during periods of uncertainty. Specifically, when the strategic environment is ambiguous, decision-makers utilize the schematic representation of strategic culture to identify the appropriate course of action.

Although strategic culture is occasionally employed to explain state behavior, early proponents such as Snyder [60] and Gray [61]

are often accused of advancing over- and under-determined theories of state behavior—applied in cases where other explanations are insufficient, but without establishing scope conditions. Succeeding attempts adopt a Gramscian approach by separating discourse grounded in strategic culture and operational doctrine [62]. Proponents assert that strategic culture permits elites to maintain hegemony that facilitates the advancement of specific doctrines that may or may not be consistent with cultural components. This, however, does not establish the extent to which discourse influences observable behavior [63, 64].

Although recent scholarship demonstrates increased rigor for both theory and method [65], issues persist. Specifically, the literature remains silent regarding the scope conditions of strategic culture, limiting its explanatory power. Furthermore, while the definition adopted by this article acknowledges the availability of pre-established behavioral preferences, preference ranking is not addressed. Consequently, treating strategic culture as a cognitive schema in response to ambiguity may provide critical insight [17, 18, 56].

Strategic culture as schemas

Strategic culture, as a schema, parallels intentional and operational ideas advanced by Kitchen [17]. The former provides normative suggestions that underlie policy goals, while the latter offer means to achieve these. More broadly, similarities may also be drawn with Norman's [66] action schemas, hierarchical constructs with top-level schemas establishing general goals. At the same time, those at lower levels provide the means to achieve these goals. This depiction is noteworthy as it suggests competing schemas, while still allowing for a degree of commonality across them (i.e. common top-level goals). Consequently, if strategic culture is operationalized as a schema, it offers a set of preferences that include specific strategic objectives and how to achieve these.

This intersection between culture and cognition is advanced by DiMaggio [67], 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 [68]. As such, schemas offer decision-makers a set of readily accessible preferences, moving them closer to their objective without having to expend significant cognitive resources during periods of crisis when the strategic environment is rife with uncertainty.

For example, we might consider a strategically vulnerable state (i.e. limited strategic depth and military capabilities) that survives conventional military challenges from stronger powers by consistently invoking existing alliances over its history; this preference is embedded and socialized into succeeding generations of political and military leadership owing to its continued success [69]. As the strategic environment changes over time and grows in complexity, similar events (i.e. new threats by stronger powers) trigger this established schema that, in turn, leads decision-makers toward preferences that worked in the past [70]. Even if the context is different, relevant attributes (i.e. the balance of power) activate this schema derived from established, and historical, strategic preferences.

Advancing schemas as a means of overcoming uncertainty in cyberspace overlap with other aspects of strategic decision-making. For nearly half a century, scholars recognized the value of these cognitive devices in addressing the complexity of the international environment [71]. Consequently, schemas offer an analytical lens through which the strategic environment is interpreted by identifying the source of preferences that shape state behavior.

12 Constructs such as images, heuristics, beliefs, and scripts are identified by political psychologists as means with which decision-makers overcome uncertainty while preserving precious cognitive resources.

13 Bayesian updating is the process by which previous assumptions and expectations are updated or rejected upon receiving new information.

14 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 [63] into and competition between epistemic communities [19]. As decision-makers are integrated into a community, they adopt the underlying organizational culture that includes specific preferences and practices oriented on community objectives. 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 [64]. 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 these no longer prove to be relevant such as in instances of policy failure [73].

15 Adapted from Klein's [14] 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.*"

While the cybersecurity 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, varying definitions emerging from country-specific approaches hint at the importance of these constructs. Hare [72] observes that unique socio-cultural factors govern strategic priorities and behavior in cyberspace. Relatedly, Valeriano *et al.* [7] allude to distinct national expressions of cyber power as instruments of foreign policy, tracing the preferences of Russia, China, and the USA 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. Chinese cyber operations, in comparison, prioritize achieving an information advantage over adversaries and represent classic Chinese strategic thought such as *Shih*¹⁶. Finally, cyber operations by the USA reflect a preference for precise and degradative operations aimed at command-and-control systems, highlighting US strategic culture and its emphasis on an engineering approach to security and the central role of technology¹⁷. Finally, Kari and Pynnöniemi [73] employ strategic culture as an analytical framework to unpack Russian threat perception 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:

Decision-makers employ strategic culture as a cognitive schema that mediates the interpretation of strategic realities and informs strategic preferences.

It should be emphasized that this proposition does not invalidate the significance of material factors. Asserting, instead, that these are considered insofar as they correspond with schematic expectations. That is, aspects of the strategic environment that align with a schema are utilized, while contradictory information is either ignored or interpreted to fit expectations [59]. While efficient, this increases the risk of bias. As noted by Meibauer [15], 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 the rest are readily discarded [59, 74, 75].

Returning to the hypothetical example, when the vulnerable state experiences cyber operations that seemingly originate from a stronger state, decision-makers would interpret this as a challenge to its security and would resort to invoking existing alliances to guarantee its security as this has proven successful in the past. This interpretation, however, ignores the possibility of false flag operations and may result in preferences that are ill-suited to the situation.

For cyber operations, misperception resulting from the use of related cognitive devices surfaces in several studies. Schneider [53] observes the tendency of elites to frame cyber operations as provocative. Despite a favorable balance of power, participants hesitate to initiate cyber operations. In this case, the strategic environment (i.e. the balance of power) is not ignored *per se*. Instead, participants who opposed cyber operations perceive an equivalence between these and

nuclear weapons, viewing both as destabilizing. In a separate experiment, Kreps and Schneider [76] observe a similar mechanism in non-elites from the United States. Relatedly, others [54, 77] 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 do not explicitly link misperception with the schematic use of strategic culture, these highlight the challenges associated with related cognitive devices.

While the limitations of schemas may be addressed by changing their structure to fit the strategic environment, this proves difficult as schemas are resistant to alteration given the imperative of maintaining cognitive consistency [59, 78]. However, the underlying motivations of decision-makers offer a possible solution.

While studying electoral behavior, Taber *et al.* [79] observe the role of motivational goals in moderating the effects of schematic thinking. Motivational goals offer insight into the influence of schemas on preferences. These are categorized into two distinct classes; accuracy goals that emphasize correct assessments and directional goals that encourage the maintenance of exiting beliefs [79, 80]. The former is considered cognitively strenuous, while the latter subjectively frames the information environment to align with pre-existing 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 [79, 81]. Individuals may choose to engage in deliberate and effortful cognition if this increases accuracy and minimizes negative consequences. Consequently, while subjective assessments resulting from schematic thinking are likely to persist, incentives exist for decision-makers to assess the strategic environment objectively.

Building again on the previous example, political elites may exhibit directional goals without considering the possible differences between cyber and conventional operations if there is an urgency to resolve the situation (i.e. critical infrastructure is targeted). However, accuracy goals may temper this tendency when, for instance, decision-makers realize the possibility of escalation should they act rashly. In this case, effort is spent on better understanding the context surrounding the cybersecurity incident.

Objectively evaluating the strategic environment, while cognitively demanding, is crucial. The entanglement of issues in cyberspace requires careful consideration to avoid unintended escalation and the adoption of effective strategic choices [82, 83]. Even without taking the technical aspects of the environment into account, the inclusion of cyber operations in the foreign policy toolbox necessitates careful consideration of their strategic implications. While spill over into the physical domain is yet to be observed, the strategic value of cyberspace necessitates caution when deciding on an appropriate course of action [43, 53, 84]. Consequently, decision-makers are advantaged when undertaking an objective assessment of cyberspace. Inversely, an over-dependence on cognitive devices such as schemas increases the risk of failure.

The benefits of overriding schemas are highlighted given the anarchic structures and uncertainty of the international system [85]. With complete information (i.e. no uncertainty), bias and misperception emerging from schematic use are unlikely as decision-makers are unlikely to rely on these cognitive devices. However, as such a situation is doubtful in the real world, schemas increase the risk of bias and misperception [19]. Consequently, the emergence of accuracy goals serve as a filter with which schema-derived preferences are subjected to greater scrutiny.

¹⁶ Defined as “*momentum, potential energy, force, the strategic configuration of power, strategic advantage.*”

¹⁷ This raises the corollary question of whether emergent technologies (e.g. cyberspace) not only trigger schematic usage; but inevitably result in their change. This is possible, provided that such instruments introduce significant cognitive dissonance that prompts a reassessment existing schema.

As with 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. Forsyth and Pope [33] argue that awareness of the negative consequences of aggression eventually results in the establishment of norms. Similarly, Finnemore and Hollis [86] cite the failure to acknowledge contrasting worldviews as a stumbling block to establishing norms in cyberspace. While not mentioning accuracy goals specifically, both cite the need for decision-makers to carefully consider the strategic consequences of cyber operations, and how the actors involved may differ in their interpretations of the issue.

At the other end of the spectrum, deterrence research echoes the importance of accuracy. Both Nye [82] and Brantly [83] note that deterrence by entanglement requires recognizing interdependencies between actors. Specifically, recognition of the consequences discourages malicious behavior. Relatedly, deterrence through deception [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.

With these in mind, careful consideration of the strategic environment within and outside cyberspace appears beneficial. While there may be truth to the argument that agreed competition among powers results in a tacit set of rules (i.e. a type of schema) owing to repeated interactions [4], one cannot conclude that emergent cyber powers recognize this view. Similarly, established powers operating in cyberspace without the benefit of context from prior interactions are left uncertain of adversarial intent. This highlights the risks associated with operating within a given mindset without considering views held by adversaries [87]. Consequently, it can be proposed that:

Proposition 2

Accuracy goals moderate the adoption of schema-derived preferences by motivating decision-makers to objectively assess the strategic environment.

In arguing that strategic preferences result from the mediating effects of schemas that are further moderated by accuracy goals, the framework reflects the cognitive-psychological model advanced by Goldgeier and Tetlock [88], who posit the “*systemic slippage between policy-guiding mental representations of reality and reality itself*.” This acknowledges the limitations of human cognition, while maintaining the possibility of deliberate and effortful assessments that considers strategic reality. 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 analysis of behavior in the face of changing strategic contexts [89–91]. The use of wargaming as a mode of inquiry is only recently being adopted by a handful of cybersecurity scholars [25, 53, 92, 93]. Skepticism toward wargaming stems from its perceived subjectivity [94]. Wargames are seen to favor mundane realism and external validity, while sacrificing experimental realism and internal validity emphasized by modern social science research [95].

As Schneider *et al.* [25] argue, the benefit of wargaming is a function of the underlying research goals, with a distinction between experimental and observational wargames. The former prioritizes internal validity and emphasizes the randomization of samples, control and treatment groups, multiple iterations, and an abstraction of

the game environment [96] to test individual mechanisms. The latter, inversely, sacrifices control over confounding variables and, instead, leverages variations between participant groups, while holding constant the in-game scenario [97, 98] to obtain external validity and heterogeneity. Consequently, researchers must decide between wargaming as a test for causal mechanisms or an inductive theory-building exercise.

As such, the article employs wargaming not as a definitive test of theory, but as a plausibility probe that demonstrates the feasibility of the proposed framework¹⁸. In holding the scenario and participant background constant while varying nationality¹⁹, the strategic preferences among participants, given the activation of strategic culture as a schema, are surfaced. Inversely, if participants objectively assess the strategic environment, there should be little to no variation observed. This design adopts Mill's Method of Difference in that cases are similar in all but one aspect, with differences in the observed outcome attributed to variations in the independent variable.

Readers should note that this design raises two conceptual challenges: sub-cultures internalized by participants that stem from their real-world affiliations and the appropriateness of nationality as a proxy for strategic culture. Contemporary strategic culture scholarship surfaces the existence of multiple competing sub-cultures within a given state [18, 69], raising questions of which and whose sub-culture matters. However, one could argue that commonalities emerge following established patterns of behavior in response to the strategic environment²⁰ from which individual sub-cultures later surface as a result of contrasting organizational prerogatives [69, 70]. Krause [99] reaffirms this when noting the futility of distinguishing between different levels of culture as “*all share overlapping elements*.” For example, while the need to prevent escalation is widely accepted, solutions may vary between those with a diplomatic or military background. These shared elements may account for the perceived appropriateness of specific policies despite organizational differences and address concerns regarding variation across sub-cultures and the use of nationality as a viable proxy for strategic culture [70].

Scenario structure and gameplay

The wargame consists of three rounds where participants play the role of Idemorean government officials²¹ in randomized teams consisting of three participants. The use of fictitious countries minimizes the risk of priming participants to align their behavior with the expectations of real-world states [47]. This encourages participants to be more forthcoming during gameplay and debriefing as institutional prerogatives may bias their perception and inclination to voice their opinions.

18 A plausibility probe is a preliminary study of untested theories to determine whether further testing is warranted [102]. For cybersecurity, Morgan [56] adopts a comparable approach in the study of decision-making behavior relative to wargaming results from the US Naval War College.

19 It should be noted that the article does not equate nationality with strategic culture *per se*. Instead, this acknowledges that while multiple sub-cultures exist [19, 73], these share commonalities with one another owing to shared experiences and worldviews of individuals. Moreover, as strategic cultures are operationalized as schemas, it should also be noted that these are hierarchical, with lower-level schemas sharing similarities with those on top [15].

20 Which includes socio-political, economic, and geographic constraints.

21 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 the online Appendix.

Before gameplay, participants complete a survey measuring policy preferences and beliefs that may influence in-game behavior. After this, participants read a briefing packet detailing the expectations of their assigned role and their contribution to the strategic objectives of Idemore. The detail provided in this packet is unique and purposefully does not conform to obvious real-world rivalrous relationship parallels, distancing 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 having comparable levels of power (i.e. economic and military). Teams are given information at every round about ongoing cyber operations. During round one, Idemorean media suffers a series of disruptive cyber operations. The situation escalates in the second round, with operations targeting critical infrastructure²². For the first two rounds, attributional evidence suggests the possible involvement of Vadare. However, this is by no means unambiguous²³. By the third round, a non-state actor claims credit for the incidents.

Besides incident information, teams are given details of 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 contextualized by the underlying strategic environment [100]. Furthermore, the saliency of this issue may restrain individuals from aggressively engaging with their adversary [101].

For every round, teams respond to developments by choosing from a fixed set of policy responses that range from inaction to military readiness²⁴. The choices are based on a list of plausible policy options available to states in the real world. It is important to note that previous choices influence events in succeeding rounds and reflect the consequential nature of interstate relations.

The wargame requires ~2 h to complete and is followed by a debriefing. These questions are open-ended to allow participants to expound on their answers and pursue relevant avenues for discussion. The debriefing is patterned after the Experience, Identify, Analyze, and Generalize (EIAG) model [102], and is recorded with the participants' consent and transcribed for later analysis.

During gameplay, non-participatory observation is carried out by research assistants. The number of observers varies based on the location of the wargame. At the very least, two are available to move between groups to observe their respective decision-making processes and discussion²⁵. 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 employed to overcome uncertainty, and (4) sources and justification of preferences²⁶. 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 be directly involved with foreign policy decision-making, their experience parallels those involved in such processes, making them suitable proxies compared to undergraduate students or the general public [24, 103].

To recruit participants, we approached relevant organizations and pitched the wargame as an opportunity to test their knowledge and capability in response to a cybersecurity incident. In exchange, we provided access to the material and held closed-door seminars discussing the lessons learned. 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.

An immediate critique from this approach is that these individuals may reflect distinctive sub-cultures based on their professional backgrounds. While the article does not discount this possibility, these may overlap with one another [69]. For instance, foreign policy and military specialists may have distinct approaches to a particular issue [104, 105]. However, both are likely to share beliefs regarding their country's respective interests. This reflects the hierarchical nature of strategic culture and is also applicable to its depiction as a schematic device, as mentioned in the theoretical framework.

However, the article does not discount the possibility of organizational prerogatives influencing preference selection. To account for this possibility, we disassociate participants from their professional roles using the fictitious scenario. The design aims to control the influence of organizational prerogatives, while not actively hindering the use of schemas grounded in their respective strategic culture.

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 for the identification of the motivations that drive the observed team behavior.

Analysis of in-game policy choices is focused on their effects on the strategic relationship between Idemore and Vadare. Consequently, the analysis is concerned with the form (e.g. do nothing versus retaliate) and strategic implications (e.g. status quo versus escalation) of these choices. 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 an actual test of the mechanism, this strengthens the plausibility of the proposed framework.

Readers should note that, unlike in-game policy choices and non-participant observations, the post-game debriefing is analyzed at the country level. Consequently, teams' decisions and 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 [17], 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. Together, these represent a hierarchical schema from which strategic preferences are derived to pursue a strategic objective.

22 During the second round, participants are chosen at random and are either told that the national tax system or the national healthcare system was disrupted by ransomware. This tests whether variation in target type affects the decision-making process.

23 The information does not provide teams with absolute certainty as to the culpability of Vadare. Furthermore, additional information in the form of the strategic relationship between the two countries increases ambiguity *vis-à-vis* attribution.

24 The list of response options is available in the online Appendix.

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

26 Non-participatory observers note participant behavior manually or, in certain cases, recorded in-game discussions. In the case of the latter, some of the discussions had to be translated into English.

<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.

Observations and Analysis

Wargames were conducted between August 2019 and 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 advancement²⁷. Consequently, one could assume that preferences during gameplay are comparable between the two.

The behavior of 11 teams is analyzed: seven from the Philippines and four from Singapore²⁸. Gameplay and debriefings were conducted in English and took ~3 h to complete. For Singapore, the wargame was held virtually due to the COVID-19 pandemic and the corresponding travel restrictions.

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 [106] instrument, only two teams are shown to support militant foreign policies²⁹. Interestingly, teams that opted for assertive policies showed support for cooperative foreign policies. Besides policy preference, risk acceptance may also influence behavior [107]. The survey found that teams from both the Philippines and Singapore are risk-averse. Finally, domain expertise also facilitates perception and preferences for in-domain behavior [77, 108, 109]. Teams from Singapore appear knowledgeable, while most of those from the Philippines (four out of seven) had comparable expertise with cybersecurity.

In-game policy choices

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

Broadly, 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, 110].

Behavior deviated by the second round when threats to Idemorean critical infrastructure appeared in the form of attacks against the national healthcare or tax systems. Additionally, information is provided suggesting a possible campaign of coercion initiated by Vadare. As seen in Fig. 1, over two-thirds (five) of the Philippine teams chose to either retaliate using cyber operations (two) or placed their military on alert (three). However, only half (two) of the Singaporean teams followed suit.

For the Philippine teams, policy choices and the critical infrastructure targeted in the second round appear unrelated. Teams were just as likely to adopt assertive policies regardless of whether the healthcare or tax system was affected. In contrast, the Singaporean teams adopted a seemingly paradoxical approach, opting to place the military on alert when the risk of significant damage (e.g. potential loss of life) was low in instances where the tax, rather than the healthcare system, was assaulted.

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

Both Singaporean and Philippine teams appear to adopt distinct approaches to the strategic environment despite facing identical scenarios. While the Philippines was more assertive once critical infrastructure was threatened, they exercised restraint with the arrival of new information. Singapore, in contrast, appeared committed to their decision despite the availability of possibly disconfirming evidence. While this suggests a difference in preferences, these alone do not confirm the existence of unique strategic objectives.

Strategic objectives

During debriefing, teams were asked to identify their strategic goal(s) to trace the underlying intentional idea(s) shaping policy choices in each round. By doing so, themes surfaced during debriefing,

²⁷ Additional wargames were conducted with participants from Taiwan, Switzerland, and the USA. However, space considerations and comparability issues resulted in these not being included in this article.

²⁸ A total of 21 individuals from the Philippines and 12 from Singapore.

²⁹ One from each country. Moreover, these are the teams that decide to act more cautiously during gameplay.

supported by in-game observations, provide a link between strategic objectives and the means of achieving these.

The main ideas for the Philippine teams 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 this signals 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 Philippine teams’ strategic objective(s) 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 toward 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 seems influenced by the need to maintain the status quo without 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 were framed as an ideal communicative instrument assuming 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 [109]. 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) the corresponding consequences. However, it is essential to note that no explicit distinction is made regarding the nature of the target (i.e. whether it has a direct bearing on human life). 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” concerning 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 geostrategic 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 national identity shaped their preferences. 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 with references to the 1991 *Pukul Habis* incident, wherein Malaysia and Indonesia staged joint military exercises near the Singaporean border³⁰. 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 abovementioned objectives, albeit viewed differently. One team, for instance, cites 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 more significant 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 suggest caution among participants, unease toward the consequences of specific policy options (e.g. retaliation through cyberspace) remains unsubstantiated given the near-peer status between Idemore and Vadare. As proposed by Liff [111], the strategic situation enables greater freedom of action. Relatedly, Jensen and Valeriano [43] find that cyber operations function as conflict off-ramps. While this behavior echoes Schneider’s findings [53] that cyber operations are perceived as escalatory; it is unclear how the belief that military mobilization is less threatening than economic sanctions or retaliatory 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*

30 In 1991, a joint military exercise between Malaysia and Indonesia near the Singaporean border resulted in the mobilization of the Singapore Armed Forces (SAF) [117]. This incident was unknown to the research team and similarities between it and the wargame scenario are purely coincidental.

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 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 strategic culture? Although the proposed framework addresses some of the core concerns involving the analytical use of strategic culture, caution is necessary. Specifically, both the proposed 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 [69] resulting from the competition between groups (e.g. epistemic communities) whose influence over policy fluctuates in response to the strategic environment [112, 113]. Consequently, preferences held by specific communities exert more significant 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 [114] argues that its archipelagic geography increases its vulnerability to foreign invasion. In conjunction with resource constraints, the plurality of islands result 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 lack of distinction 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*" [115]. If cyberspace is perceived as an enabler of national development, it is unsurprising that disruptions to critical infrastructure—whether resulting in the loss of life or not—are 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...*" [115]. 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 mirrors distinct features of Singaporean strategic culture. Given its geographic and material vulnerability, lacking both strategic depth and natural re-

sources, Singaporean strategic culture is characterized by a "*profound continuity and an acute sense of vulnerability*" [116]. As noted by Acharya [117], this encourages the (mistaken) belief that Singaporean foreign policy is heavily influenced by a realist perspective. 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 by the simultaneous use of deterrence and diplomacy [118]. 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 developing and expanding its military capabilities, while simultaneously deterring threats to its security [119]. Complementing this, Singapore actively engages in diplomatic activities that establish stable and positive relationships [120].

This cautious yet pragmatic approach toward 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 of projecting strength, but not at the cost of escalating the situation. 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 Singapore illustrates two distinct approaches (operational ideas) in pursuit of a single goal (intentional idea).

These results suggest that strategic culture, at least for the Philippines and Singapore, is activated as a schematic device when these incidents limit the ability of decision-makers to derive meaning (e.g. intent) from these incidents in the context of interstate relations. This is unsurprising, given the extent to which cyberspace is entangled in salient national security issues. During gameplay, references to adversarial intentions concerning the cybersecurity incidents and the current strategic environment produced a significant amount of ambiguity. Consequently, participants gravitated to preferences established in their respective strategic cultures as a means of overcoming this ambiguity as these, in their experience, provide the strategic outcomes they desire.

Information processing and accuracy goals

While the framework asserts that preferences result from the schematic use of strategic culture, it also posits 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 involves the comparison and exchange of information. For attribution, available evidence may emphasize the culpability of a specific 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 toward a particular type of evidence and stressed 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 imply 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 judgment is deferred to an individual with prior objectives and priorities in an uncertain environment, perpetuating these preferences [121]. Consequently, accuracy goals may only exert minimal influence.

For Singaporean teams, comparison and sharing are also viewed as necessary; “...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 explained 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 [59]. 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.

Consequently, 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 seen in the 1991 incident. Interestingly, this highlights a situation in which schemas and related cognitive structures may be advantageous. Gigerenzer [122] argues that cognitive shortcuts contribute to the accurate assessments of the information environment provided that these are ecologically rational, i.e. to say, that 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 between Vadare and Idemore³¹. Although not explicitly stated, this may have resulted in parallels drawn with Singapore's dependence on water from Malaysia, which shaped its policy preferences post-independence [118]. Consequently, this increases the likelihood of using schemas that may be suitable for this 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 wargame illustrate the importance of strategic culture as a schematic device. Despite facing identical scenarios, preferences appear to have been influenced by the underlying strategic culture, which defined the path toward achieving strategic objectives. While this does not preclude objective assessments of the strategic environment, it suggests the tendency of decision-makers 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 toward cybersecurity incidents. This is manifested in attempts to defend national security through an assertive but measured display 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 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.

Building on this, recent developments in cybersecurity scholarship pointing to a normalization of interaction in cyberspace emphasizes the importance of scholarship that surfaces the role of psychological and cultural-level factors. While the literature over the past two decades continues to evolve past arguments citing the exceptional nature of cyberspace, its involvement in long-standing strategic interactions and the continued use of cyber operations as an adjunctive foreign policy instrument [10, 123] requires us to ask the question of “how” cyberspace and cyber operations are perceived rather than just whether strategic effects are possible through these tools.

31 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.

While authors such as Harknett and Fischerkeller [4] argue that constant interactions may result in agreed competition wherein the “rules of the road” are recognized by parties involved, this does not preclude the possibility that decision-makers could continue framing these interactions in the context of pre-existing schemas. Research by Valeriano *et al.* [7] point to this possibility when they acknowledge distinct national approaches to cyberspace. Moreover, Healey [87] notes that these unspoken rules may not apply to states only recently strategically employing cyberspace. In this case, uncertainty encountered in the process is likely surmounted using devices such as schemas.

Consequently, the argument and probe provided in this article contain several critical implications for policy, practice, theory, and methodology. Concerning both policy and practice, 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 in training and pedagogy on security in the digital domain, as the inclination toward certain forms of cyber-nationalistic posturing is undoubtedly inculcated during professional learning. Indeed, these areas of national defense process should be the focus of follow-on research. Furthermore, 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.

Additionally, concerning both policy and practice, it is worth mentioning 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. Mainly, 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’ schematic approach to digital warfare.

These points apply to both established and emerging cyber powers. In the case of the former, these serve to remind decision-makers of the risk of not evaluating the sources of individual preferences and practices and the bias that may ensue from this lack of criticality. For the latter, emergent powers are called to assess the extent to which lessons learned from domains outside cyberspace readily apply to this domain. In turn, this allows for the creation of organizations and processes that can effectively operate within this space.

Theoretically, the article surfaces several questions and possible avenues for further research. Most salient among these is the role of multiple sub-cultures in influencing decision-making and preference selection. Although the literature asserts that a dominant strategic culture emerges through the competitive interaction of relevant organizations [69, 124], the fact that policymaking is rarely left to a single individual suggests the continued influence of sub-cultures reflected in individual organizational prerogatives. While the behavior of a state may be distinct, one cannot dismiss the possibility that individual groups would continue to push for a change. Although the wargame is not expressly designed to test for this possibility, a modification in the stated role of the individual participants, such as forming groups composed of individuals with similar professional

backgrounds and comparing this to others that differ, may surface this dynamic.

The article also questions how strategic culture, manifested as schemas, may influence accuracy goals. Phrased differently, are accuracy goals external to schematic thinking, or is there a possibility for a bi-directional relationship. Under this condition, the suitability of schema-derived preferences is no longer a question of whether a schema is used, but is instead a function of the schema itself. Theoretically, this reinforces the outlook of cognitive and political psychologists who are cautious in labeling cognitive shortcuts as problematic and argue that the efficacy of these constructs is a matter of their suitability to the environment (i.e. ecological rationality) [122]. Future iterations of this wargame can test for this possibility by involving participants from states known for their strategic caution and comparing the results from those known to be more willing to engage in risk-taking to pursue their objectives.

Finally, from a methodological standpoint, the findings presented in this article demonstrate the feasibility of wargaming as a valuable research instrument. 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. Moreover, wargaming, and experiments by extension, provide scholars with access to data to study an inherently opaque phenomenon owing to its national security implications.

The growing importance of cyberspace as an instrument of national power requires a rigorous understanding of how preferences emerge in response to strategic developments within this domain. While schemas have 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 better understand state behavior in this human-made domain.

Supplementary Data

Supplementary data available at [Cybersecurity Journal](https://doi.org/10.1080/01402390.2020.1732354) online.

Acknowledgments

The authors would like to thank the participating organizations in the Philippines and Singapore without whom this project would not have been possible. Furthermore, the authors would also like to extend their gratitude to the area editor and the anonymous reviewers for their insightful comments that contributed to the improvement of this article.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

1. Harknett R, Smeets M. Cyber campaigns and strategic outcomes. *J Strat Stud.* 2020. 1–24.10.1080/01402390.2020.1732354
2. Axelrod R, Iliev R. Timing of cyber conflict. *Proc Natl Acad Sci* 2014; 111: 1298–303.

3. *Cyber War as an Intelligence Contest*. <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/> (6 April 2022, date last accessed).
4. Fischerkeller M, Harknett R. Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *Cyber Def Rev* 2019; 267–87.
5. Saltzman I. Cyber posturing and the offense-defense balance. *Contemp Secur Pol* 2013; 34: 40–63.
6. Iasiello E. Cyber attack: a dull tool to shape foreign policy. In: Podins K, Stinissen J, Maybaum MS (eds), *Proceedings of the 2013 Fifth International Conference on Cyber Conflict*. Tallinn: IEEE, 2013, 451–70.
7. Valeriano B, Jensen B, Maness R. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press, 2018.
8. Slayton R. What is the cyber offense-defense balance? Conceptions, causes, and assessment. *Int Secur* 2017; 41: 72–109.
9. Pytlak A, Mitchell G. Power, rivalry, and cyber conflict: an empirical analysis. In: Friis K, Ringsmose J (eds), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, London: Routledge, 2016, 65–82.
10. Maness R, Valeriano B. The impact of cyber conflict on international interactions. *Armed Forces Soc* 2016; 42: 301–23.
11. Buchanan B. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. London: Hurst & Company, 2017.
12. Gartzke E, Lindsay J. Weaving tangled webs: offense, defense, and deception in cyberspace. *Secur Stud* 2015; 24: 316–48.
13. Lin H. Attribution of malicious cyber incidents: from soup to nuts. *J Int Aff* 2016; 70: 75–137.
14. Klein Y. A theory of strategic culture. *Comp Strat* 1991; 10: 3–23.
15. Meibauer G. Interests, ideas, and the study of state behaviour in neoclassical realism. *Rev Int Stud* 2019; 46: 1–17.
16. Dueck C. *Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy*. Princeton: Princeton University Press, 2006.
17. Kitchen N. Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation. *Rev Int Stud* 2010; 36: 117–43.
18. Bloomfield A. Time to move on: reconceptualizing the strategic culture debate. *Contemp Secur Pol* 2012; 33: 437–61.
19. Kertzer J, Renshon J. Putting things in perspective: mental simulation in experimental political science. 2015; 1–60. https://people.fas.harvard.edu/~jkertzer/Research_files/PT%20Web%20version.pdf.
20. Kertzer J, Brutger R, Quek K. *Strategic Empathy and the Security Dilemma: Cross-National Experimental Evidence from China and the United States*. New Haven: Department of Political Science, Yale University, 2018.
21. Baker J. The empathic foundations of security dilemma de-escalation. *Pol Psychol* 2019; 40: 1251–66.
22. Keller J, Yang Y. Empathy and strategic interaction in crises: a poliheuristic perspective. *Foreign Pol Anal* 2009; 5: 169–89.
23. Valeriano B, Jensen B. Wargaming for social science. *SSRN Pap* 2021; 14.
24. Lin-Greenberg E, Pauly R, Schneider J. Wargaming for international relations research. *Eur J Int Secur* 2022; 28: 83–109.
25. Schechter B, Schneider J, Shaffer R. Wargaming as a methodology: the international crisis wargame and experimental wargaming. *Simul Gam* 2021; 52: 513–26.
26. Kuehl D. From cyberspace to cyberpower: defining the problem. In: Kramer F, Stuart H, Wentz L (eds), *Cyberpower and National Security*. Dulles: Potomac Book, 2009, 24–42.
27. Borghard E, Loneragan S. The logic of coercion in cyberspace. *Secur Stud* 2017; 26: 452–81.
28. Lindsay J. Stuxnet and the limits of cyber warfare. *Secur Stud* 2013; 22: 365–404.
29. Clarke R, Knake R. *Cyber War*. New York: Ecco, 2010.
30. Dunn-Cavelty M. From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *Int Stud Rev* 2013; 15: 105–22.
31. Brantly A. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia Press, 2016.
32. Rathbun B. Uncertain about uncertainty: understanding the multiple meanings of a crucial concept in international relations theory. *Int Stud Quart* 2007; 51: 533–57.
33. Forsyth J, Pope M. Structural causes and cyber effects why international order is inevitable in cyberspace. *Strat Stud Q* 2014; 8: 112–28.
34. Perrow C. *Normal Accidents: Living With High-Risk Technologies*. Princeton: Princeton University Press, 1984.
35. Schneider J. The capability/vulnerability paradox and military revolutions: implications for computing, cyber, and the onset of war. *J Strat Stud* 2019; 42: 841–63.
36. Lindsay J. Restrained by design: the political economy of cybersecurity. *Digit Pol Regul Gov* 2017; 19: 493–514.
37. Hansen L, Nissenbaum H. Digital disaster, cyber security, and the copenhagen school. *Int Stud Quart* 2009; 53: 1155–75.
38. Posen B. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Ithaca: Cornell University Press, 1986.
39. Healey J. Winning and losing in cyberspace. In: *Proceedings of the 2016 Eight International Conference on Cyber Conflict (CyCon)*. 2016. 37–49. Washington, DC: IEEE.
40. United Nations Institute for Disarmament Research. *The Cyber Index: International Security Trends and Realities*. Geneva: United Nations Institute for Disarmament Research, 2013.
41. Blessing J. The global spread of cyber forces, 2000–2018. In: *Proceedings of the 2021 Thirteenth International Conference on Cyber Conflict (CyCon)*. 2021: 233–55. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)..
42. Fischerkeller M, Harknett R. Deterrence is not a credible strategy for cyberspace. *Orbis* 2017; 61: 381–93.
43. Jensen B, Valeriano F. What do we know about cyber escalation? Observations from simulations and surveys. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-escalation-observations-from-simulations-and-surveys> (6 April 2022, date last accessed).
44. Egloff F. Public attribution of cyber intrusion. *J Cybersecur* 2020; 6: tyaa012.
45. Gartzke E, Lindsay J. Thermonuclear cyberwar. *J Cybersecur* 2017; 3: 37–48.
46. Foreign Policy. Israel and iran just showed us the future of cyberwar with their unusual attacks. <https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/> (6 April 2022, date last accessed).
47. Herrmann R, Voss J, Schooler T. *et al*. Images in international relations: an experimental test of cognitive schemata. *Int Stud Quart* 1997; 41: 403–33.
48. Holsti O. Cognitive dynamics and images of the enemy. *J Int Affairs* 1967; 21: 16–39.
49. Brantly A. Risk and uncertainty can be analyzed in cyberspace. *J Cybersecur* 2021; 7: tyab001.
50. Kahneman D, Tversky A. On the psychology of prediction. *Psychol Rev* 1973; 80: 237–51.
51. Virus Bulletin. Who wasn't responsible for olympic destroyer?. <https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Rascagneres-Mercer.pdf> (6 April 2022, date last accessed).
52. informIT. The solar sunrise case: mak, stimp, and analyzer give the dod a run for its money. <http://www.informit.com/articles/article.aspx?p=19603&seqNum=4> (6 April 2022, date last accessed).
53. Schneider J. *Cyber and Crisis Escalation: Insights from Wargaming*. US-ASOC Futures Forum. Newport: U.S. Naval War College, 2017.
54. Gomez M. Past behavior and future judgements: seizing and freezing in response to cyber operations. *J Cybersecur* 2019; 5: tyz012.
55. Rid T, Buchanan B. Attributing cyber attacks. *J Strat Stud* 2015; 38: 4–37.
56. Morgan F. *Compellence and the Strategic Culture of Imperial Japan Implications for Coercive Diplomacy in the Twenty-First Century*. Westport: Praeger, 2003.

57. Jervis R. Understanding beliefs and threat inflation. In: Thrall A, Cramer J (eds). *American Foreign Policy and the Politics of Fear: Threat Inflation Since 9/11*. New York: Routledge, 2009, 16–39.
58. Gomez M. Sound the alarm! updating beliefs and degradative cyber operations. *Eur J Int Secur* 2019; 4: 190–208.
59. Larson D. The role of belief systems and schemas in foreign policy decision-making. *Pol Psychol* 1994; 15: 17–33.
60. Snyder J. *The Soviet Strategic Culture. Implications for Limited Nuclear Operations*. Santa Monica: RAND Corporation, 1977.
61. Gray C. National style in strategy: the American example. *Int Secur* 1981; 6: 21–47.
62. Johnston A. Thinking about strategic culture. *Int Secur* 1995; 19: 32–64.
63. Klein B. Hegemony and strategic culture: American power projection and alliance defence politics. *Rev Int Stud* 1988; 14: 133–48.
64. Lin H, Kerr J. *On Cyber-Enabled Information/Influence Warfare and Manipulation*. Stanford: Center for International Security and Cooperation, 2017.
65. Legro J. *Cooperation Under Fire: Anglo-German Restraint During World War II*. Ithaca: Cornell University Press, 1995.
66. Norman D. Categorization of action slips. *Psychol Rev* 1981; 88: 1–15.
67. DiMaggio P. Culture and cognition. *Ann Rev Sociol* 1997; 23: 263–87.
68. Rathbun B, Kertzer J, Refler J, et al. Taking foreign policy personally: personal values and foreign policy attitudes. *Int Stud Quart* 2016; 60: 124–37.
69. Libel T. Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy. *Def Stud* 2016; 16: 137–56.
70. Mirow W. *Strategic Culture, Securitisation and the Use of Force*. New York: Routledge, 2016.
71. Jervis R. *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976.
72. Hare F. The cyber threat to national security: why can't we agree?. In: *Proceedings of the 2010 Conference on Cyber Conflict*. 2010; 211–25. Tallinn: Cooperative Cyber Defence Centre of Excellence.
73. Kari M, Pynnöniemi K. Theory of strategic culture: an analytical framework for Russian cyber threat perception. *J Strat Stud* 2019; 1–29.10.1080/01402390.2019.1663411
74. Holsti O. The belief system and national images: a case study. *J Confl Resol* 1962; 6: 244–52.
75. Crocker J, Fiske S, Taylor S. Schematic bases of belief change. In: Eiser R (ed). *Attitudinal Judgement*. New York: Springer, 1984.
76. Kreps S, Schneider J. Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *J Cybersecur* 2019; 5: tyz007.
77. Gomez M. Sound the alarm! Updating beliefs and degradative cyber operations. *Eur J Int Secur* 2019; 4: 190–208.
78. Welch D. *Painful Choices: A Theory of Foreign Policy Change*. Princeton: Princeton University Press, 2011.
79. Taber C, Lodge M, Glathar J. The motivated construction of political judgments. In: Kuklinski J (ed). *Citizens and Politics: Perspectives from Political Psychology*. Cambridge: Cambridge University Press, 2011, 198–226.
80. Ford T, Kruglanski A. Effects of epistemic motivations on the use of accessible constructs in social judgment. *Personal Soc Psychol Bull* 1995; 21: 950–62.
81. Kruglanski A, Webster D. Motivated closing of the mind: “seizing” and “freezing”. *Psychol Rev* 1996; 103: 263–83.
82. Nye J. Deterrence and dissuasion in cyberspace. *Int Secur* 2017; 41: 44–71.
83. Brantly A. Entanglement in cyberspace: minding the deterrence gap. *Democr Secur* 2020; 16: 210–33.
84. Hansel M. Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks. *J Int Relat Dev* 2016; 21: 523–51.
85. Fearon J. Rationalist explanations for war. *Int Organ* 1995; 49: 379–414.
86. Finnemore M, Hollis D. Constructing norms for global cybersecurity. *Am J Int Law* 2016; 110: 425–79.
87. Healey J. The implications of persistent (and permanent) engagement in cyberspace. *J Cybersecur* 2019; 5: tyz008.
88. Goldgeier J, Tetlock P. Psychology and international relations theory. *Ann Rev Pol Sci* 2001; 4: 67–92.
89. Smith R. The long history of gaming in military training. *Simul Gam* 2010; 41: 6–19.
90. Kriz W. Historical roots and new fruits of gaming and simulation. *Simul Gam* 2017; 48: 583–7.
91. Caffrey M. *On Wargaming: How Wargames Have Shaped History and How they May Shape the Future*. Newport: Naval War College Press, 2019.
92. Jensen B, Valeriano B. The cyber character of crisis escalation. In: *Annual Meeting of the International Studies Association*. Toronto: International Studies Association, 2019.
93. Gomez M, Whyte C. Cyber wargaming: grappling with uncertainty in a complex domain. *Def Strat Assess J* 2020; 10: 98–139.
94. Perla P. *The Art of Wargaming: A Guide for Professionals and Hobbyists*. Annapolis: Naval Institute Press, 1990.
95. Falk A, Heckman J. Lab experiments are a major source of knowledge in the social sciences. *Science*, 2009. 326: 535–8.
96. McDermott R. Experimental methodology in political science. *Pol Anal* 2002; 10: 325–42.
97. Morton R, Williams K. *Experimental Political Science and the Study of Causality: From Nature to the Lab*. New York: Cambridge University Press, 2010.
98. Gerber A, Green D. *Field Experiments: Design, Analysis, and Interpretation*. New York: W W Norton, 2012.
99. Krause K. Conclusions: security culture and the non-proliferation, arms control and disarmament agenda. In: Krause K (ed). *Culture and Security: Multilateralism, Arms Control, and Security Building*. London: Frank Cass Publishers, 1999, 219–39.
100. Valeriano B, Maness R. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.
101. Mauslein J, Pickering J. Rivalry type and cyber operations: “hot” rivalries, “cold” rivalries, and cyber incidents, 1990–2009. *Peace Econ Peace Sci Publ Pol* 2021; 27: 169–95.
102. Stadskev R. *Handbook of Simulation Gaming in Social Education*. Scotts Valley: CreateSpace Independent Publishing Platform, 2013.
103. Mintz A, Redd S, Vedlitz A. Can we generalize from student experiments to the real world in political science, military affairs, and international relations?. *J Confl Resol* 2006; 50: 757–76.
104. Kruglanski A, Orehek E, Dechesne M, et al. Lay epistemic theory: the motivational, cognitive, and social aspects of knowledge formation. *Soc Personal Psychol Compass* 2010; 4: 939–50.
105. Yee A. The causal effects of ideas on policies. *Int Organ* 1996; 50: 69–108.
106. Maggiorio M, Wittkopf E. American public attitudes toward foreign policy. *Int Stud Quart* 1981; 25: 601–31.
107. Kertzer J. Resolve, time, and risk. *Int Organ* 2017; 71: S109–S36.
108. Kostyuk N, Wayne C. The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. *J Glob Secur Stud* 2021; 6: ogz077.
109. Shandler R, Gross M, Canetti D. A fragile public preference for cyber strikes: evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemp Secur Pol* 2021; 42: 135–62.
110. Edwards B, Fumas A, Forrest S, et al. Strategic aspects of cyberattack, attribution, and blame. *Proc Natl Acad Sci* 2017; 114: 2825–30.
111. Liff A. Cyberwar: a new ‘absolute weapon’? The proliferation of cyber-warfare capabilities and interstate war. *J Strat Stud* 2012; 35: 401–28.
112. Maitlis S, Sonenshein S. Sensemaking in crisis and change: inspiration and insights from Weick (1988). *J Manag Stud* 2010; 47: 551–80.
113. Weber K, Glynn M. Making sense with institutions: context, thought and action in Karl Weick's Theory. *Organ Stud* 2006; 27: 1639–60.
114. De Castro R. Philippine strategic culture: continuity in the face of changing regional dynamics. *Contemp Secur Pol* 2014; 35: 249–69.
115. National Security Council. *National Security Policy for Change and Wellbeing of the Filipino People*. Manila: National Security Council, 2017.

116. Er L. 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*. Tokyo: National Institute for Defense Studies, 2018.
117. Acharya A. *Singapore's Foreign Policy: The Search for Regional Order*. Denver: World Scientific, 2008.
118. Matthews R, Yan N. Small country 'total defence': a case study of Singapore. *Def Stud* 2007; 7: 376–95.
119. Ministry of Defence. *Factsheet – About Total Defence*. Singapore: Ministry of Defence, 2004.
120. Capie D. Structures, shocks and norm change: explaining the late rise of Asia's defence diplomacy. *Contemp Secur Pol* 2013; 35: 1–26.
121. Saunders E. No substitute for experience: presidents, advisers, and information in group decision making. *Int Organ* 2017; 71: S219–47.
122. Gigerenzer G. Why heuristics work. *Persp Psychol Sci* 2008; 3: 20–9.
123. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to Earth. *Int Secur* 2013; 38: 41–73.
124. Pirani P. Elites in action: change and continuity in strategic culture. *Pol Stud Rev* 2016; 14: 512–20.