Sub-Optimal Strategies in Cyberspace

Tracing the Source of Strategic Preferences

Miguel Alberto Gomez

A dissertation submitted in fulfillment of the requirements for the degree of Doctor of Philosophy (Dr. phil.) as per the regulations of Faculty 1, Education and Social Science, at the University of Hildesheim.

HILDESHEIM, WINTER 2022/23

TABLE OF CONTENTS

ABSTRACT

Contemporary cyber conflict literature associates state behavior in cyberspace with the underlying technological and structural realities faced by policymakers. Consequently, interstate interactions in this human-made domain are perceived as an extension of strategic competition in the real-world. As such, strategic preferences vis-à-vis cyberspace adopted by policymakers are expected to enable the pursuit of their respective national interests. Empirical evidence collected over the last two decades, however, suggests a paradoxical situation that sees otherwise capable states restraining themselves while those with limited means investing in capabilities that generate modest strategic returns. Instead of assuming irrationality on the part of policymakers, the dissertation argues that such preferences result from the contextualization of technological and structural cues through the schematic use of strategic culture. Faced with the inherent uncertainty of cyberspace, policymakers resort to these heuristic mechanisms to derive meaning from the strategic environment in which they operate. Through pseudo-experimental cross-national wargames and a case study, the dissertation advances an ideational framework that explains the emergence of strategic preferences in response to cyber conflict. While not meant to discredit existing framework, it highlights the boundedness of human cognition that results in the utilization of these socio-cognitive mechanisms. Furthermore, this emphasizes the emerging behavioral turn in cyber conflict scholarship.

ACKNOWLEDGEMENTS

I would like to extend my heartfelt thanks to everyone who extended academic and emotional support during the writing of this dissertation. To begin with, I would like to express my gratitude to my supervisor Prof. Dr. Wolf Schünemann. I appreciate all the comments and insights provided in the process of conceptualizing and completing this dissertation. Specifically, I am grateful for assistance in helping me focus my thoughts and arguments that have resulted in a robust project.

I must also express my gratitude towards my partner, Dr. Eula Bianca Villar, who served as my unofficial sounding board for ideas before, during, and after this process. More importantly, she has always been there to ground me when I find myself lost and unsure of which course of action to take. Despite the challenges encountered, her support has been unwavering. Regardless of how difficult I may have been, she has never faltered, and I will always be grateful.

The staff at the Center for Security Studies also merit recognition. I would like to thank Prof. Dr. Andreas Wenger and Dr. Myriam Dunn-Cavelty for allowing me to simultaneously pursue research at the center and to complete my doctoral studies. Recognition is also extended to Dr. Govinda Clayton, Dr. Enzo Nussio, Dr. Max Smeets, Dr. Lennart Maschmeyer, and Dr. Florian Egloff, Stefan Soesanto, and Sean Cordey for their encouragement throughout this process.

I would also like to thank Dr. Christopher Whyte, Dr. Brandon Valeriano, Dr. Nadiya Kostyuk, and Dr. Ryan Shandler for providing feedback for the corresponding journal articles and whose friendship serves as a reminder of why I chose to pursue this career.

Special thanks are in order for my friends in Switzerland and the Philippines. Antonio Messina, Blanche Ladera-Puncer, Stanislav Puncer, Carla Burkhard, and Jan Burkhard; despite the pandemic, I greatly appreciated the time spent around the dinner table and climbing in and around Switzerland. To my Dungeons and Dragons group; Marc Besa, Michaela Gomez, Gabriel Gomez, Bernice Go, Rex Ferriols, Ben Bulac, and Timothy Eustaquio, thank you for agreeing to play five- to ten- hour long games (or more) in an attempt to keep me sane.

Lastly, I would also like to thank my parents Alberto Gomez and Nenelita Gomez whose selfless support and encouragement over the last thirty-six years led me to where I am today.

NOTIFICATIONS

Chapter Three, *Overcoming Uncertainty in Cyberspace* has been published in *Defence Studies*; Volume 21, Issue 1 (https://doi.org/10.1080/14702436.2020.1851603).

Chapter Four, *Unpacking Strategic Behavior in Cyberspace*, has been published in the *Journal of Cybersecurity*; Volume 8, Issue 1 (https://doi.org/10.1093/cybsec/tyac005).

Chapter Five, *Tracing Strategic Preferences in Cyberspace*, has been published in *Comparative Strategy*; Volume 42, Issue 1 (https://doi.org/10.1080/01495933.2022.2111912).

Due to licensing, only the abstracts of the above articles are included in this monograph.

STRATEGIC PREFERENCES AND CYBER CONFLICT

INTRODUCTION

Depictions of cyberspace as an enabler of national power continue to motivate cyber conflict scholarship. With the emergence of cyber-capable actors and the increasing sophistication of cyber operations[1], there is a palpable sense of urgency to understand better the preferences that shape the exercise of power in and through cyberspace. Its novelty and the enduring narrative of an existential threat to a digitized society suggest that it stands apart from conventional environments such as land, sea, air, and space (Clarke & Knake, 2014). Prominent incidents such as the disruption of Iranian nuclear centrifuges (Lindsay, 2013) and ransomware targeting healthcare facilities (Newman, 2020) further entrench this belief among the media and policy pundits. States, in response, (1) publish or revise national cybersecurity strategies (CCDCOE, 2017), (2) institute public cyberinsitutions[2] that operate defensively and/or offensively (Blessing, 2021; Kostyuk, 2021), and (3) call for the introduction of cyber norms (Forsyth & Pope, 2014).

Further complicating matters, the technological emphasis on functionality over security (Denning & Denning, 2016; Libicki, 2009; Lindsay, 2017) increases the potential for disruptions that manifest cascading effects that are not geographically bound (Saltzman, 2013). Moreover, the complexity of cyberspace hinders attempts to mitigate and predict the consequences of disruptive incidents (Kaminska, 2021; Perrow, 1984). It is estimated, for instance, that fifteen to fifty errors are found for every thousand lines of code (Mayer, 2012). This provides malicious actors ample opportunity for exploitation and fosters a sense of unknowability and unpredictability, seemingly confirmed by the surge of cybersecurity incidents over the last two decades (Dunn Cavelty, 2013). Consequently, it is unsurprising to expect states to act pre-emptively to secure their strategic interests, resulting in cyber conflict. The empirical evidence, however, appears to challenge these pessimistic expectations.

First, disputes in cyberspace are yet to rise to the level of armed conflict that spills over into the physical domain. While cyber capabilities continue to deliver tactical gains (Healey, 2016), strategic outcomes remain muted (Iasiello, 2013). Moreover, while some point to the potential benefits from sustained and cumulative operations that constitute broader cyber campaigns (Harknett & Smeets, 2020), the degree to which these shift the balance of power is

[1] Defined as the offensive exercise of power in cyberspace in support of strategic objectives.
[2] Defined as *"publicly observable proactive efforts aimed at signaling its offensive and defensive cyber capabilities"* (Kostyuk, 2021, p. 2).

yet to be demonstrated. Furthermore, aggressors appear to exercise restraint when interacting with adversaries despite substantial capabilities[3] at their disposal (Borghard, 2019; Kaminska, 2021). As a preliminary explanation, scholars (Fischerkeller & Harknett, 2018; Gomez, 2018) posit that sustained state interactions surface normative expectations of acceptable behavior in cyberspace that moderate the risk of escalation. Relatedly, Maness and Valeriano (2016) propose that established rivalry dynamics apply to cyberspace and discourage destabilizing behavior. With these arguments in mind, scholars (Rid, 2012; Rovner, 2019) question the appropriateness of existing narratives that emphasize the risk of escalation in the wake of cyber conflict.

Aside from the observed restraint, only a handful of states appear to utilize cyber operations actively. The Dyadic Cyber Incident and Dispute (DICD) Dataset identifies less than ten active states between 2000 and 2016[4] (Valeriano & Maness, 2014). This is surprising given the purported ease with which offensive cyber capabilities may be acquired compared to their conventional counterparts. However, analysis of prominent cyber operations notes the substantial resources required to generate strategically meaningful effects (Borghard & Lonergan, 2017; Liff, 2012). Furthermore, while some assert that these offer an offensive advantage, defenders may impose costs on aggressors as offense necessitates foreknowledge of defensive mechanisms that may require capabilities exogenous to cyberspace to overcome[5] (Lindsay, 2013; Slayton, 2017). Moreover, a successful compromise does not exempt aggressors from further expending costly resources. For example, sustained cost imposition is prohibitively expensive as Borghard and Lonergan (2017) argue that punishment strategies are often costly and impractical. Aggressors must therefore weigh the costs associated with individual cyber operations or campaigns relative to potential strategic gains (Axelrod & Iliev, 2014; Harknett & Smeets, 2020). Collectively, these observations require a reassessment of how preferences that lead to cyber conflict come to light.

It is important to note that the above observations temper the exceptionalism surrounding cyber operations, depicting these as instruments that function within the established limits of technological and structural realities (Fischerkeller & Harknett, 2020; Harknett & Smeets, 2020; Warner, 2020). Technological constraints pertain to the unique technical features that grant scale and scope to cyber operations while at the same time limiting

[3] Both cyber and non-cyber.
[4] An updated version that extends its coverage up to 2020 is yet to be released at this time.
[5] For instance, the success of Stuxnet appears to have been predicated on the existence of a wide and efficient intelligence infrastructure (Lindsay, 2013).

their effects (Gartzke & Lindsay, 2015). Structural constraints, in turn, refer to the distribution of material capabilities within the international system, reflected through the balance of power, that enables and restricts state action (Liff, 2012; Waltz, 1979). Assuming that policymakers are rational actors, one could assert that preferences emerge from the objective evaluation of these limitations. For example, Fischerkeller and Harknett (2020) suggest that characterizing cyberspace as both an enabler of and threat to national power encourages states to proactively exercise their power in and through cyberspace to nullify the threat posed by adversaries and to secure their strategic interests. However, trends in the development and diffusion of cyber capabilities do not coincide with this expectation and challenge the techno-structural account of cyber conflict.

The United Nations Institute for Disarmament Research (UNIDIR) estimated in 2013 that 114 of the 197 UN member states had established cybersecurity programs. Of these, 47 assigned some responsibility to their armed forces (UNIDIR, 2013). By 2020, a total of 71 states were identified as having militarized cyber forces (Blessing, 2021). While it could be argued that this represents the expected security-seeking behavior, this argument falters under closer scrutiny.

While our ability to observe interstate interactions in cyberspace is limited due to the phenomenon's opaque nature, the empirical evidence only identifies a handful of actors regularly embroiled in cyber conflict (Jensen, Maness, & Valeriano, 2016). Furthermore, inequality in both access to and dependence on cyberspace results in varying threat perceptions (Gomez & Tran Dai, 2018; ITU, 2016), challenging sweeping explanations grounded on threats to national power as motivating the development and exercise of cyber capabilities. This is particularly pertinent as the costs associated with these capabilities are prohibitive. While some states may see these as status symbols (Pytlak & Mitchell, 2016), conventional instruments are more affordable and perhaps better suited for certain strategic and tactical objectives. Consequently, *the extent that preferences reflect technological and structural constraints faced by states* is the focal point of this dissertation.

However, the degree that uncertainty inhibits the objective assessment of technological and structural realities is often unacknowledged in the analysis of cyber conflict. This is surprising as uncertainty, already problematic for conventional statecraft, is amplified in the case of cyberspace (Brantly, 2021; Kaminska, 2021). Furthermore, the literature presupposes

rationality on the part of policymakers[6] (Axelrod & Iliev, 2014; Brantly, 2016; Liff, 2012; Smeets & Work, 2020). Cyber conflict scholarship, however, recognizes that uncertainty (Brantly, 2021; Buchanan, 2017; Gartzke & Lindsay, 2017; Schneider, 2017) and a shortage of expertise (Hansen & Nissenbaum, 2009), at best, hinder the careful consideration of the strategic environment, increasing the risk of misperception and miscalculation. Nonetheless, interstate interactions in and through cyberspace remain surprisingly pacific[7].

While the resilience of cyberspace may partially explain this outcome (Fischerkeller & Harknett, 2020), the context of these interactions provides crucial insight. If cyber conflict corresponds with real-world strategic competition (Maness & Valeriano, 2016), established preferences may be adapted to suit this digital environment. Consequently, the dissertation posits that behavior-shaping preferences in cyberspace are derived from entrenched beliefs resulting in distinct national modes of cyber conflict. Furthermore, it asserts that decision-makers employ strategic culture as an ideational lens that informs preferences in this human-made environment.

Employing strategic culture as an analytical device reflects the growing trend in cyber conflict scholarship which highlights the significance of immaterial factors in shaping preferences and behavior. For this dissertation, strategic culture is viewed as *"widely shared, identity-driven norms, ideas, and beliefs about the legitimate use of force by the state for the provision of security"* (Mirow, 2016, p. 34). In conceptualizing strategic culture as an ideational variable that informs the use of force in an uncertain environment such as cyberspace necessitates four (4) propositions that account for its influence. First, uncertainty is compounded by a lack of expertise among policymakers and encourages the use of cognitive shortcuts (i.e., heuristics) when interpreting techno-structural cues. Keeping in mind the emerging relationship between cyberspace, security, and power, the dissertation proposes that;

Propositions 1. Policymakers employ strategic culture as a meaning-making tool from which preferences are derived in pursuit of security.

[6] While not explicit, theories of interstate interactions in cyberspace tend to assume that actors behave within the boundaries of the technological and structural constraints that contextualize their interactions.
[7] This is not to say that conflict does not exist. Instead, conflict occurs well below of what would be considered armed conflict.

However, the use of strategic culture does not spontaneously occur and results from the embeddedness of policymakers in the latent socio-cultural and historical milieu of a particular state. Through a socio-discursive process, individuals adopt these underlying beliefs. Policy construction, however, involves a plurality of actors across different groups (e.g., technology, foreign policy, and defense) with distinct sub-cultures that may result in competing preferences. This configuration results in overlaps and divergences across these groups regarding their preferences and beliefs. Consequently, the dissertation proposes that;

Proposition 2. Policymakers exhibit shared preferences when socialized into a common strategic culture.

Proposition 3. Policymakers belonging to different epistemic communities may hold distinct preferences, though the possibility of shared preferences exists.

While policymakers may be beholden to these ideational constructs, this is not a foregone conclusion. They may be motivated to think more objectively, acknowledging the technological and structural constraints when accuracy is required. This pertains to the need to avoid costs (e.g., personal or organizational) resulting from the misinterpretation of environmental cues. For instance, in situations where policy failure following misperceptions results in substantial national or organizational implications. Consequently, the dissertation proposes that;

Proposition 4. Accuracy goals limit the range of preferences derived from strategic culture by encouraging the objective evaluation of technological and structural cues.

Through cross-national simulations involving policy, military, and cybersecurity experts and an in-depth single case study, the dissertation demonstrates that strategic culture is employed to overcome uncertainty during periods of crisis and peace to surface strategic preferences. This, however, should not be interpreted as an attempt to displace existing techno-structural frameworks that inform our understanding of cyber conflict. The dissertation, instead, complements these by acknowledging the significance of ideational constructs in broadening our understanding of interstate behavior in cyberspace. This framework, visualized in Figure 1, highlights the potential for the *"systemic slippage between policy-guiding*

representations of reality and reality itself" (Goldgeier & Tetlock, 2001, p. 79) that explain deviations in observed state behavior thus far.

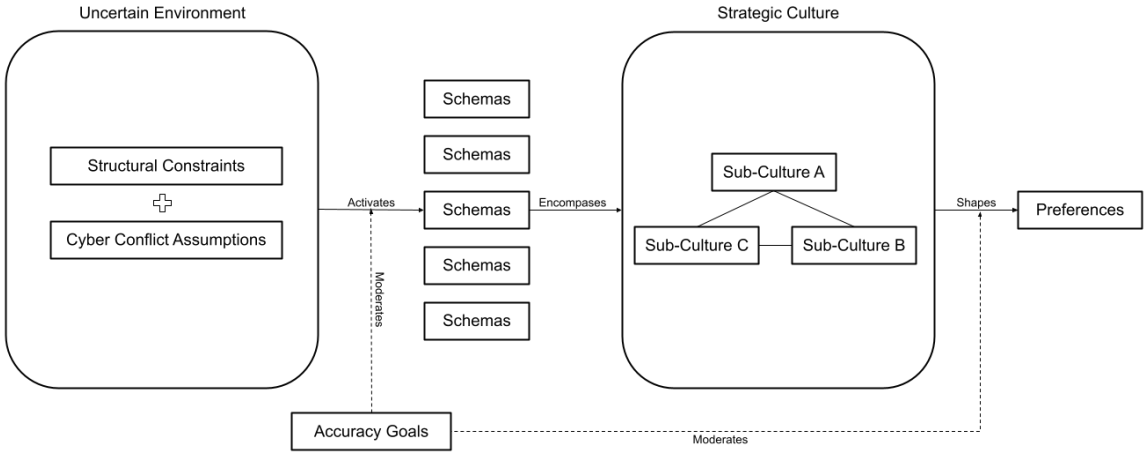

Figure 1 Mechanism Visualization

Moving forward, the remainder of this chapter is divided into three further sections. Immediately following this, a discussion surrounding the nature of cyber conflict is presented. This emphasizes gaps in the cyber conflict literature, beginning with technologically deterministic explanations followed by arguments that consider structural constraints. It then surfaces the emergence of ideational variables that shape preferences regarding the expression of power through cyberspace. Proceeding from this, the chapter highlights the dissertation's theoretical and policy contributions and its implications for the field of cybersecurity and beyond. The chapter concludes with a summary of each of the chapters that constitute the dissertation.

TECHNO-STRUCTURAL ACCOUNTS OF CYBER CONFLICT

Attempts to unpack state preferences towards the use of cyber operations depict cyberspace as an enabler of national power that may be threatened in pursuit of strategic goals (Clarke & Knake, 2014; Kuehl, 2009). While scholars such as Arquilla and Ronfeldt (1993) proffer the military and societal impact of cyber operations as a function of increasing societal dependence, it was not until the disclosure of prominent cybersecurity incidents that its strategic potential shifted from academic speculation to a possible reality. Saltzman (2013), for instance, argues that exploiting the interconnectivity of cyberspace results in cyber operations manifesting greater mobility and effects relative to their conventional counterparts. Enabled by the accessibility of offensive tools and anonymity, states are assumed to readily shift their

interactions from the physical into the digital domain, transforming it into a conflict-prone environment (Clarke & Knake, 2014; Forsyth & Pope, 2014). This belief is encouraged by persistent media narratives detailing the existential threat of malicious behavior in cyberspace (Jarvis, Macdonald, & Whiting, 2017). Unsurprisingly, states began to develop strategies and the requisite technical and organizational capabilities to exploit the domain (Dunn Cavelty, 2012). Nevertheless, despite revolutionary aspirations buoyed by media reporting and political rhetoric, the strategic effects of cyber operations are far more modest than initially claimed.

While progressively advanced operations continue to be reported, sophistication does not ensure the desired strategic outcomes. The DICD notes that less than 5% of cyber operations conducted between 2000 and 2017 achieved their strategic objectives[8] despite a tactical success[9] rate of 90% (Valeriano & Maness, 2014). Consequently, the cyber conflict literature over the last decade exhibits increasing skepticism towards the strategic utility afforded by cyber operations. Iasiello (2013), for instance, observes that these have not influenced adversarial behavior in a significant and lasting manner, leading him to characterize these as "dull" foreign policy instruments. Challenges to its revolutionary claims call into question attributes that differentiate it from its conventional counterparts. Specifically, (1) lower barriers to entry, (2) attributional challenges, and (3) the perceived offensive advantage it affords.

The ease with which offensive cyber capabilities are proliferated distinguishes these from their conventional counterparts. Sources include exploits purchased on the grey or black markets, security tools repurposed for malicious use, implicit or explicit engagement with criminal or hacktivist organizations, and services offered by the private sector. While these reduce startup costs for aggressors, this comes at the cost of both scope and scale. For example, Liff (2012) cautions that readily accessible tools are likely to only affect poorly secured systems (i.e., low hanging fruit). Maschmeyer (2021) builds on this argument by emphasizing the compromise required to achieve immediate effects sacrifices control over and the intensity of operations – constraining their strategic potential. Relatedly, Borghard and Lonergan (2017) posit that sustained operations are impractical owing to the need to invest in costly cyber capabilities, the value of which diminishes over time (Axelrod & Iliev, 2014).

[8] While some may argue that information obtained from the exfiltration of confidential information is strategically relevant, a difference exists between gaining access to this resource and utilizing it to gain a strategic advantage (Gilli & Gilli, 2019).
[9] Tactical success pertains to successfully compromising the target system.

With these in mind, achieving significant strategic effects through cyber means requires the availability of resources comparable to, if not greater than, those of conventional operations. Pytlak and Mitchell (2016), for instance, note that the capabilities vital to operating effectively in cyberspace entail expertise analogous to that of nuclear weapons programs. Relatedly, investigations following the discovery of Stuxnet illustrate that resources both within and outside cyberspace were necessary for its development and execution (Lindsay, 2013). Consequently, arguments espousing the cost-effectiveness of cyber operations overlook the relationship between strategic outcomes and investment in technological and organizational capabilities.

Apart from developmental and operational costs, the advantages afforded by anonymity were initially misstated as well. While Lin (2016) concedes to the extent that cyber operations are attributable to individuals and authorizing bodies, the problem is not insurmountable. Advancements in digital forensics and the plurality of intelligence sources enable the analysis of technical, operational, and strategic evidence that contribute to the accuracy of attribution (Egloff, 2020; Rid & Buchanan, 2015). Moreover, the resources required for complex operations further limit the number of plausible aggressors.

Aside from the availability of evidence, anonymity may also be detrimental for certain operations (Poznansky & Perkoski, 2018). While the underlying characteristics of cyberspace enable states to engage with adversaries covertly (Carson, 2018), this is not beneficial in all instances. Coercion, for example, requires the coercer to identify both themselves and their demands. Anonymity, however, inhibits this communicative act (Borghard & Lonergan, 2017). In other cases, aggressors may wish to be identified in a bid to signal existing capabilities (Brown & Fazal, 2021). Consequently, attribution has evolved from a sense-making process where victims struggle to establish the identity of an aggressor to meaning-making where discerning intent is of foremost concern (Egloff, 2020).

The preceding discussion weakens arguments favoring the offensive advantage that cyber capabilities are expected to provide. An offensive advantage, briefly, pertains to the benefits afforded by technological developments that grant the offense a distinct advantage over defense (Van Evera, 1998). Early cyber conflict scholarship acknowledged the inherent technological vulnerabilities, ready access to malicious tools, and anonymity as tilting the likelihood of success in favor of aggressors. However, reduced developmental costs and anonymity are often overstated, as shown above. Furthermore, while defense is difficult owing to vulnerability in the underlying technology, aggressors still require an understanding of

existing defensive mechanisms (Slayton, 2017). Moreover, defenders can impose costs by utilizing deception to lure aggressors into a false sense of security that allows for the development of appropriate countermeasures (Gartzke & Lindsay, 2015).

With these in mind, the benefits of cyber operations appear far less revolutionary than initially portrayed, such that states are less preoccupied with overpowering adversaries than they are with achieving strategic advantage. Consequently, the explanatory framework of strategic competition aptly describes the character of cyber conflict (Warner, 2020). Proponents argue that cyberspace represents a *"global warehouse of and gateway to troves of sensitive, strategic assets that translate into wealth and power"* (Fischerkeller & Harknett, 2020). However, its inherent vulnerability suggests that economic, political, social, and military capabilities may be at risk. This obliges states to respond in anticipation of adversarial exploitation. Fortunately, the resilience of cyberspace enables persistent interactions without destabilizing the strategic environment (Fischerkeller & Harknett, 2020; Warner, 2020). This results in two preferences for utilizing cyber operations; as instruments for signaling intent or those that shape the strategic environment (Buchanan, 2020).

While coercion through cyberspace continues to receive its share of criticism, the communicative potential of cyber operations as a means of managing competition and escalatory risk has merit. Jensen and Valeriano (2019b) posit that these offer conflict off-ramps, allowing decision-makers to demonstrate resolve while minimizing the risk of escalation. In this vein, the strategy of defend forward reflects the concept of persistent engagement where sustained interactions communicate the boundaries of acceptable behavior (Fischerkeller & Harknett, 2019). Relatedly, signaling does not necessitate offensive action. For instance, the establishment of public cyberinstitutions functions as a costly signal to deter potential aggressors[10] (Kostyuk, 2021).

Contrasting these methods, cyber operations may also shape the strategic environment by manipulating the conditions in which adversaries operate without resorting to bold displays of capability (Lindsay & Gartzke, 2014). Scholars of this persuasion (Maschmeyer, 2021; Rid, 2012; Rovner, 2019) liken cyber conflict to espionage, subversion, and sabotage rather than warfare. Over the last two decades, empirical evidence confirms this assessment with only a handful of highly visible and degradative operations (Valeriano & Maness, 2014). Consequently, Harknett and Smeets (2020) advocate that academics and policymakers must

[10] Although it is important to note that there are limits to this approach with respect to certain aggressors.

distance themselves from the notion that strategic utility is only achieved through ostentatious displays of (cyber) capabilities. Recent events, particularly disinformation campaigns during national elections and the COVID-19 pandemic, demonstrate the value of the subtle and cumulative exercise of power in shaping the strategic environment.

Whether employed to shape or signal, contemporary cyber conflict scholarship assumes that preferences emerge in response to techno-structural constraints imposed on states in pursuit of their strategic objectives, resulting in a *cyber fait accompli* (Fischerkeller & Harknett, 2020; Forsyth & Pope, 2014). Consequently, the exercise of power in and through cyberspace reflects the core assumptions of structural realism while keeping in mind the limits and possibilities afforded by the domain. Although this depiction captures aspects of state behavior in this domain, shortcomings exist; take the case of tacit bargaining and agreed competition for instance.

Tacit bargaining and agreed competition depict an environment wherein an implicit understanding among actors in cyberspace defines the limits of acceptable behavior, resulting in persistent interactions that remain below the threshold of armed conflict (Fischerkeller & Harknett, 2019). As its proponents contend, this ensures the stability of the environment, which allows for strategic competition between states to proceed while mitigating the risk of escalation. While the rationale is sound, stability is predicated on (1) limited operational effects and (2) familiarity with behavioral norms (i.e., tolerated operations).

Managing the effects of cyber operations requires compromises that constrain strategic utility, for which Maschmeyer (2021) points to a trilemma involving speed, intensity, and control. Prioritizing control, crucial for avoiding unintended consequences, comes at the cost of intensity and speed that may adversely affect the operation's strategic objectives (Borghard & Lonergan, 2017). Similarly, decision-makers may abandon restraint if they believe that their window of opportunity is closing[11] (Axelrod & Iliev, 2014) or that the intended target is unwilling or incapable of responding (Edwards, Furnas, Forrest, & Axelrod, 2017). Furthermore, considering the transient effects of cyber operations, states with significant conventional capabilities may not see the need for caution when engaging with weaker actors (Liff, 2012). Suppose states objectively respond to the technological and structural constraints imposed on them. In that case, stability cannot be guaranteed if this places them in a

[11] While the logic of "use it or lose it" as it applies to cyber operations continues to be challenged, states must continue to consider the risk that the longer they wait, the higher the chances are that the vulnerabilities they wish to exploit are discovered and mitigated.

disadvantaged position relative to their adversaries (Schneider, 2019). Moreover, this logic is predicated on the objective interpretation of the strategic environment.

Strategic constraints aside, maintaining behavioral norms suggests that states are cognizant of (1) the existence of such norms and (2) the consequences of violations. These conditions, however, are contingent on a host of factors. Foremost amongst these is the ability to discern adversarial intent as not violating certain norms. Buchanan (2017) observes that identifying intent following the discovery of malicious code is difficult owing to the similarities between mundane and significantly disruptive operations. Furthermore, the underlying strategic context and the location of the compromise may lead targets to assume escalatory intent where none exists (Gartzke & Lindsay, 2017). This is concerning as both simulations and experiments demonstrate the existence of bias. Schneider (2017), in a series of wargames, observes the tendency of decision-makers to employ mirror imaging – projecting their own beliefs and expectations onto adversaries. Similarly, Gomez (2019a, 2019c) demonstrates the use of established enemy images in discerning intent despite evidence suggesting otherwise.

While cyber conflict scholarship continues to temper exaggerated claims involving the exercise of power in and through cyberspace, existing frameworks require further development to explain the emergence of preferences in response to strategic competition. To this end, recent scholarship highlights distinct national modes of cyber conflict that address these shortcomings. Just as neoclassical realists turn to ideational variables (among others) to explain why states fail to recognize structural cues (Rathbun, 2008), a comparable phenomenon in cyberspace may cause policymakers to adopt ill-suited preferences.

If cyber conflict serves as an extension of established strategic competition between states, then strategic culture may function as an ideational tool informing policymakers of the *"legitimate use of force by the state for the provision of security"* (Mirow, 2016, p. 34). At present, the cyber conflict literature makes little mention of strategic culture. However, scholars increasingly link behavior in cyberspace with established preferences that pre-date this domain. For instance, Valeriano, Jensen, and Maness (2018) attribute national styles to Russia, China, and the United States when analyzing operational preferences in cyberspace. Russia, they observe, utilizes low-level disruptive operations to shape public opinion. Moreover, its dissemination of propaganda and misinformation through cyberspace reflects behavior that coalesced during the period of the Soviet Union (Rid, 2020). Chinese cyber operations, in contrast, prioritize achieving an information advantage over adversaries,

reflecting classic Chinese strategic thought, such as *Shih*[12]. U.S. cyber operations, finally, are characterized by a preference for precise and degradative operations aimed at command-and-control systems. The technical requirements of these operations reflect U.S. strategic culture and its predisposition towards an engineering approach to security and the centrality of technology.

Similarly, Kari and Pynnöniemi (2019) explicitly employ strategic culture as an analytical framework to understand Russian threat perception. They assert that the dual narratives of Russia as a besieged fortress and its perceived technical inferiority are prominent in its approach to cybersecurity. Relatedly, simulations and experimental research also surface the schematic use of strategic culture. Observations by Schneider (2017) in wargames suggest actions linked to preferences established in other domains (i.e., land, sea, and air) are projected onto cyberspace. Similarly, in an ongoing series of cross-national wargames, Gomez and Whyte (2022) trace participant behavior to schemas developed for scenarios exogenous to the fictitious environment employed.

Although these studies point to preferences that emerge from distinct national experiences, three fundamental questions remain unanswered. First, the cyber conflict literature does not provide the conditions in which strategic culture is adopted over the objective assessment of technological and structural cues. This speaks to wider concerns with strategic culture being both under- and over-determined, requiring the establishment of scope conditions (Lantis, 2002). Second, transmission, maintenance, and change in strategic culture require further elaboration. While the early literature assumes strategic culture to be a given (Gray, 2005; Johnston, 1998; Snyder, 1977), recent scholarship notes the importance of agency in its diffusion and evolution (Libel, 2020; Lock, 2010). Moreover, the plurality of actors involved in policymaking entails considering the possibility of multiple sub-cultures and subsequent contestation. Finally, reconciling the difference between this proposed ideational approach and the dominant techno-structural perspective needs to be addressed. The integration of concepts such as culture runs the risk of being criticized as a post-hoc, or at worse ad-hoc, attempt to explain variations in state behavior. Consequently, strategic culture must be integrated in a manner that does not fundamentally alter the underlying assumptions of existing frameworks.

[12] Strategic power, defined as *"momentum, potential energy, force, the strategic configuration of power, strategic advantage"* (Valeriano et al., 2018, p. 150).

The embeddedness of cyberspace in socio-political and economic processes requires consideration of factors beyond technology and structure. Furthermore, this proposed approach reflects a growing interest in cyber conflict scholarship that emphasizes the significance of micro- and meso-level factors. Advancing the argument that strategic culture serves as a source of preferences enriches the discipline's theoretical toolbox while tempering excesses that characterized it during its formative years.

THEORETICAL AND POLICY CONTRIBUTIONS

Through the questions that it aspires to address, the dissertation offers theoretical, methodological, and policy contributions that further the development of cyber conflict scholarship. The dissertation reflects the emergent trend that moves the level and unit of analysis below that of the state and system. Starting with a novel experiment designed by Gross, Canetti, and Vashdi (2017), the literature recognizes the value of individual-level attributes in shaping perception and behavior. This is not particularly surprising. Despite being a technologically defined environment, perceptions of security and threat remain contingent on the lived experience of individuals that operate within cyberspace (Gomez & Whyte, 2021). Kreps and Schneider (2019) note that the domain is perceived as an environment apart from land, sea, air, and space, resulting in distinct perceptions of how states are expected to interact. Building on this, the continued shortage of expertise risks the emergence of ill-fitting policies and hyperbolic narratives (Hansen & Nissenbaum, 2009). Consequently, research that unpacks the underlying mechanism shaping perceptions is crucial for how and why specific policies emerge and are adopted.

Aside from cyber conflict scholarship, the dissertation also builds on fourth generation strategic culture scholarship. Establishing the scope conditions within which policymakers employ strategic culture as an ideational instrument demonstrates that this provides the necessary context when adopting specific behavior-shaping preferences. In doing so, the arguments advanced are not exclusive to cyberspace and may apply to other strategically relevant domains that suffer from an excess of uncertainty. Furthermore, the dissertation also surfaces the dynamics between sub-cultures and how this influences the adoption of preferences. With technologies such as cyberspace increasingly decentralizing expertise and decision-making, it becomes crucial to have a firm understanding of how different communities interact and possibly contradict one another during policy deliberations.

It should be noted that the theoretical contributions advanced are further strengthened by the methodological approach employed. A fundamental shortcoming of cyber conflict scholarship is the shortage or inaccessibility of data. The opaque nature of this phenomenon limits our ability to understand better the decision-making processes that shape policy. In response, scholars are increasingly resorting to experiments (Gomez & Whyte, 2021; Kostyuk & Wayne, 2021; Shandler, Gross, & Canetti, 2021) and simulations (Jensen & Valeriano, 2019b; Schechter, Schneider, & Shaffer, 2021; Schneider, 2017) to surface these mechanisms. To this end, adopting cross-national simulations reflects this trend within the scholarly community and enables greater generalizability of its theoretical contributions.

Finally, and regarding its policy relevance, the dissertation offers two fundamental lessons to both established and emergent state actors in cyberspace. As with issues surrounding intelligence, uncertainty increases the risk of bias as policymakers gravitate towards embedded preferences that may not suit the strategic environment. For established state actors, this drives the need to have processes in place to ensure that individuals do not remain locked into degenerative practices that, while useful in the past, may not adequately address the issues of the present. Relatedly, the lack of both experience and expertise may prompt emergent actors to revert to treating cyberspace, or other emergent technologies, as an extension of the current strategic environment without considering possible divergences. In both cases, bias is minimized by establishing processes to review whether preferences correspond with the demands of the environment.

Tangential to this, the dissertation is a reminder that other actors (e.g., potential adversaries) may themselves be susceptible to bias and misperception. As such, policymakers benefit from recognizing the possibility that other actors may behave in accordance with prior beliefs rather than an objective interpretation of the environment. Recognizing this possibility enables tailoring policies that do not inadvertently provoke misperception.

The dissertation's theoretical, methodological, and policy contributions collectively offer a direct, real-world impact. In establishing a framework that instrumentalizes strategic culture as an ideational instrument, it acknowledges the impact of individuals when it comes to the adoption of preferences that are later reflected by policy. Doing so alleviates the exceptionalism that persists among academics and policymakers. Moreover, the use of simulations to highlight the risk of misperception and its consequences provides a pedagogic tool that relevant organizations may use to avoid perpetuating biases that result in policy failure.

CHAPTER SUMMARIES

As the dissertation is constructed around three separate articles, a summary of how each of the corresponding chapters relates to one another is necessary. Readers interested in the core arguments should proceed directly to the third, fourth, and fifth chapters as these present the underlying theoretical framework and the empirical evidence that support it.

Related Literature and Theoretical Orientation

This chapter reviews related literature and establishes the epistemological and ontological perspective adopted throughout the dissertation and is partitioned into four sections. The first reiterates the dissertation's objective of identifying the sources of strategic preferences in cyberspace. Noting that contemporary scholarship depicts cyber conflict as an extension of strategic competition, this section surfaces gaps in the existing literature, emphasizing how policymakers appear to interpret structural and technological cues that surround cyber conflict inaccurately.

Moving forward, the article presents structural realism as the foundation guiding much of cyber conflict scholarship. The section acknowledges that the limitations encountered when applying this framework to explain paradoxical state behavior call for the inclusion of ideational variables that function as an interpretative lens through which policymakers contextualize the environment. The section unpacks the concept of ideas and their externalized expression that complement our understanding of interstate relations.

These arguments are further developed in the following section that presents the concept of strategic culture as a manifestation of a particular belief system. Employing strategic culture to explain state preferences and behavior is neither new nor uncontroversial. Consequently, time is spent addressing the fundamental critiques of it being simultaneously over- and under-determined, as well as its excessive continuity and the possibility of multiple sub-cultures. Strategic culture is operationalized as a cognitive schema externalized through a discursive process to overcome these challenges. Once externalized and accepted, policymakers employ it heuristically to overcome uncertainty inherent in interstate relations. This establishes the necessary scope conditions in which strategic culture, as a schema, exerts a causal effect on preferences. Furthermore, this surfaces the possibility of multiple schemas

that compete with one another as a means of achieving hegemony, introducing the potential for a change in strategic culture.

The chapter concludes by returning to the question of cyber conflict and ideational frameworks to explain behavior-shaping preferences vis-à-vis cyber conflict. This section notes that while scholars have either implicitly or explicitly cited the role of strategic culture over the past five years, the causal mechanism linking the interpretation of structural and technical cues with behavior-shaping preferences remains unspecified. This provides the foundation for introducing the proposed theoretical framework.

Overcoming Uncertainty in Cyberspace

This chapter introduces the theoretical framework employed throughout the dissertation. Proceeding from the review of related literature, it establishes that uncertainty is a defining characteristic of cyberspace. Furthermore, it argues that uncertainty manifests as the ambiguity of information instead of its deficit, as implied by the literature. Technological and procedural developments over the last two decades provide crucial information regarding cybersecurity incidents. Voluminous information, however, does not resolve questions of ambiguity, especially in terms of the underlying intent. This asserts that the accumulation of information alone is not a viable strategy for overcoming uncertainty. The chapter then proposes that policymakers utilize cognitive schemas to extract meaning from their environment. Specifically, these schemas are cognitive manifestations of strategic culture. This treatment of strategic culture addresses critiques of it being over- and under-determined. As a schema, strategic culture is employed when facing uncertainty. Under more favorable conditions, individuals are expected to evaluate the environment more objectively.

The chapter also tackles the existence of sub-cultures. These are pronounced for cyber conflict owing to the plurality of actors involved. The choice to adopt a schematic approach, however, resolves this concern. The chapter proposes that policymakers are members of different epistemic communities, each with their own schema reflecting a distinct sub-culture. During policy deliberation, different schemas may compete to gain prominence over others. This position is maintained until it is of no added value (e.g., policy failure), and the process of contestation begins once more.

The chapter closes by asserting that schematic thinking among policymakers is not a foregone conclusion. Apart from an optimum information environment, dependence on

schemas is tempered by accuracy goals. These are a form of motivated cognition that aspires to interpret information accurately. Whether driven by organizational prerogatives, individual values, or self-interest, accuracy goals encourage objectivity that limits the influence of schematic thinking and, consequently, the appeal of preferences rooted in strategic culture.

The proposed theoretical framework operates across two distinct phases. The internal phase establishes the nature of and conditions in which strategic culture is used schematically and constitutes the cognitive dimension of the theory. This is empirically tested through cross-national wargames. The external phase discusses the presence of multiple sub-cultures and the possibility of conflict between these that highlight latent social dynamics. This is empirically tested through a case study of how cybersecurity is integrated into Philippine national security.

Unpacking Strategic Behavior in Cyberspace

This chapter presents the first empirical test of the proposed theoretical framework and aims to ascertain whether strategic culture is adopted as a schematic device to overcome ambiguity during periods of crisis and determines whether the presence of accuracy goals tempers schematic thinking. Noting the difficulty surrounding access to either policymakers or relevant decision-making artifacts, the chapter utilizes pseudo-experimental cross-national wargames depicting a fictitious crisis between two near-peer states, Idemore and Vadare.

The wargame presents a situation wherein cyber conflict erupts between these two states during an emergent crisis involving the discovery of natural resources. Presented across three different rounds of gameplay, cybersecurity incidents occur alongside diplomatic overtures and possible militarization. Participants engage with the scenario in teams of three, each assuming the role of an Idemorean official (e.g., the defense minister). Teams are offered a set of policy options for every round to respond to developments. Selected policy options influence in-game developments for the succeeding rounds. This progression aims to replicate real world cyber conflict. Moreover, the gameplay was designed such that participants experience pronounced ambiguity levels that increase the likelihood of schematic thinking.

Participants consist of military, policy, and cybersecurity specialists from participating states that serve as proxies for pollical elites. Although the wargames involved individuals from Singapore, the Philippines, the United States, Taiwan, and Switzerland, only the first two

results are analyzed in this chapter[13]. This is done to control for possible variations, noting that the Philippines and Singapore are (1) comparable in terms of their geographic location (i.e., regional neighbors), (2) colonial history, and (3) perceptions of cyberspace.

To test whether strategic culture is used schematically, in-game response, non-participant observation, and debriefing interviews are collectively analyzed. If strategic culture is used schematically, perspectives and preferences associated with Philippine or Singaporean strategic culture should correspond with those adopted in-game, resulting in distinct cross-national behavior. Inversely, if the wargame is approached objectively (i.e., without exogenous priors), then behavior should be consistent irrespective of nationality. Relatedly, accuracy goals are significant if explicit mention is made regarding the need for the objective assessment of the situation that overrides preferences derived from the schematic use of strategic culture.

The wargame finds that the preferences and behavior of teams from the Philippines and Singapore correspond with their respective strategic culture. The former adopts an assertive posture, emphasizing the need to demonstrate resolve in the face of threats. This is reminiscent of how the Philippines historically addressed challenges to its national security. While similarly recognizing the need to communicate resolve, the latter is more circumspect and opts to leave the possibility of a negotiated settlement open simultaneously. This echoes the Singaporean preference for pursuing both deterrence and diplomacy as a means of managing its national security

Concerning accuracy goals, however, the findings are mixed. Although participants from the Philippines recognized the need to objectively evaluate the information, their tendency to defer their decisions to a single individual increase the risk of perpetuating established preferences (i.e., bias). For the Singaporean teams, it is difficult to disassociate their stated need for accuracy with their identity and, in effect, strategic culture. In other words, it is unclear whether the need for accuracy is exogenous of the employed schema.

Tracing Strategic Preferences in Cyberspace

This chapter complements the one preceding it by testing the presence of sub-cultures and possible contestation in the development of strategic preferences. The chapter employs a single case study involving the integration of cybersecurity as a component of Philippine

[13] Although comparable results are observed in these other instances.

national security in recent years. Although single case studies are criticized for their limited generalizability, this is not necessarily problematic in this situation.

The Philippines, and cyber conflict in general, is seen as a hard test (i.e., least likely case) for the proposed framework. Faced with enduring and salient external security concerns, the exercise of cyber capabilities by the Philippines is expected to be a function of its pronounced material imbalances vis-à-vis adversaries. The Philippines, as such, should employ cyber operations to complement its limited conventional capabilities to signal resolve when challenged. This preference should be reflected in official policy documents and echoed by its policy elites. Furthermore, the appearance of cyber conflict over the last twenty years serves as an "external shock" that challenges the viability of established preferences due to cyberspace's novelty. Moreover, the integration of cybersecurity as a component of national security is a recent development. Limited experience should encourage the Philippines to seek guidance from communities with possibly divergent perspectives in terms of security and how best to achieve it. Consequently, the chapter argues that these conditions make the prospect of preferences derived from strategic culture unlikely.

To test this argument, the chapter triangulates evidence from policy documents, interviews with policy elites, and third-party reporting. The policy documents used include but are not limited to (1) the National Security Policy, (2) the National Defense Strategy, (3) the National Military Strategy, and the (4) the National Cybersecurity Plan. Relatedly, the policy elites interviewed are from the (1) Department of National Defense, (2) Department of Foreign Affairs, and the (3) Department of Information Communication and Technology. With an emphasis on national security, policy documents and individuals responsible for law enforcement were excluded.

The corresponding analysis finds that the Philippines' approach towards cyber conflict is purely defensive. While respondents and text from relevant policy documents echo the findings from the preceding chapter regarding the demonstration of resolve, this is reflexive and is structured to be unprovocative from the perspective of potential adversaries. Similarly, while the institution of the Armed Forces of the Philippines Cyber Group (AFP-CYG) as a dedicated cyber unit suggests the projection of power, its organizational structure and authorities limit this possibility. Lastly, the tendency of Philippine administrations to leverage the capabilities of non-state actors to augment cyber capabilities reinforces its preference for a non-provocative defensive strategy.

These characteristics appear to correspond with aspects of Philippine strategic culture, most notably its preference for conflict avoidance. Furthermore, its siloed approach towards cybersecurity surfaced during interviews and reflected in the National Cybersecurity Plan suggests contrasting preferences among relevant actors and indicates possible contestation at the domestic level. Interestingly, however, no such disputation appears to have occurred in the institution and continuing work of the Association of Southeast Asian Nations (ASEAN) Cybersecurity Expert Working Group instituted by and actively participated in by the Philippines. Noting the divergent perspectives regarding cybersecurity in the region, one would expect that this forum functions as a platform on which states advocate for their respective strategic interests in cyberspace. This, however, is not the case, as noted by respondents who participate in this forum. Nevertheless, this cordiality may instead reflect aspects of the regional culture that ASEAN members internalized.

Given the adoption of a defense- and resilience-oriented approach towards cyber conflict within ASEAN, this represents preferences such as non-confrontation and conflict avoidance that characterize strategic culture within the region. Consequently, the chapter surfaces an interesting dynamic wherein regional strategic culture influences interactions among member states that limit contestation during the formulation of regional preferences. However, this top-down process does not necessarily resolve disputes that may occur domestically, resulting in distinct national strategies in response to cyber conflict across the region.

Conclusion

This chapter consolidates the arguments advanced by the dissertation thus far and provides further avenues for research. This is divided into four sections, with the first summarizing the findings presented in empirical chapters. It takes this opportunity to link the four propositions that constitute the theoretical framework with the results from cross-national wargames and the single case study involving Philippine cybersecurity policy. In effect, this section provides a top-level view of how the fundamental arguments of the dissertation relate to one another.

The chapter then introduces the dissertation's theoretical, methodological, and policy implications. The dissertation places itself squarely amidst the behavioral turn characterizing recent cyber conflict scholarship. It notes the value of studying individual-level variables and

how this relates to phenomena at higher analysis levels. Relatedly, the dissertation represents the increasing use of experimental and pseudo-experimental methodologies. Noting the opaque nature of the phenomenon, scholars are turning to these techniques to understand better how policymakers and the public respond to cyber conflict. The chapter concludes by highlighting the need to consider the policy consequences of dependence on schematic thinking. Noting that the utility derived from heuristics is contingent on how these correspond with reality, it calls for interventions to minimize the risk of misperception and bias among policymakers.

RELATED LITERATURE AND THEORETICAL ORIENTATION

INTRODUCTION

Cyber conflict is increasingly characterized as an expression of strategic competition between states (Fischerkeller & Harknett, 2020; Valeriano & Maness, 2015; Warner, 2020) whereby behavior-shaping preferences are assumed to emerge through the objective assessment of technical and structural cues. However, the empirical evidence available does not appear to meet this expectation consistently. First, capable state actors are expected to employ cyber operations if doing so is strategically favorable. This should not be interpreted as an endorsement of cyber conflict. Instead, it suggests that those with the requisite capabilities should pursue strategic objectives if the potential (strategic) gains outweigh the costs. For instance, US operations targeting the Internet Research Agency (IRA) following electoral interference from Russia appeared unnecessarily restrained despite the initiator's underlying capabilities (Borghard, 2019). Second, the number of emergent actors investing in cyber capabilities despite their limited threat exposure is puzzling given the associated material and organizational overhead (Borghard & Lonergan, 2017; Pytlak & Mitchell, 2016; Slayton, 2017). Furthermore, the limited effects thus far raise questions whether these actors should spend precious resources on such an endeavor. Finally, cybersecurity issues involve several actors, including technical and non-technical experts. This necessitates asking whether perceptions of the environment are shared or emerge through competition between those with (potentially) divergent perspectives (Dunn Cavelty, 2013; Hansen & Nissenbaum, 2009).

Nevertheless, objectivity cannot be ruled out entirely despite these possible contradictions. Sustained interstate interactions provide insight into adversarial intent and capabilities (Brantly, 2021; Maness & Valeriano, 2016). Furthermore, technological developments enhance defensive and forensic capabilities, limiting impact and increasing the reliability of attribution (Rid & Buchanan, 2015). These allow policymakers to learn from experience, facilitating strategically sound choices despite the boundedness of the information environment. Nevertheless, the literature has yet to convincingly engage with two fundamental challenges that shape cyber conflict scholarship; its inherent complexity (Brantly, 2020, 2021; Gartzke & Lindsay, 2015) and the continued shortage of expertise (Brantly, 2021; Hansen & Nissenbaum, 2009).

Both complexity and limited expertise increase the uncertainty encountered by policymakers. Complexity obstructs the ability to predict the consequences of disruption (Kaminska, 2021; Perrow, 1984) while the shortage of expertise skews expectations of what is

achievable via cyber means and result in hyperbolic narratives (Hansen & Nissenbaum, 2009). Nevertheless, this is not a unique phenomenon as uncertainty is a defining feature of the international system (Rathbun, 2007). In response, policymakers adopt a priori expectations of state behavior, such as those that frame structural realism, to overcome this limitation.

Structural realism[1], from which cyber conflict scholarship draws heavily (Arquilla & Ronfeldt, 1993; Forsyth & Pope, 2014; Saltzman, 2013), depicts an anarchic self-help system wherein states are uncertain of adversarial intent. Responding to the distribution of power reflected in the ordering of the system, states pursue policies that work towards a relative advantage over others (Waltz, 1979). Applying this logic to the study of cyber conflict, the early literature recognized the growing technological dependence on and inherent vulnerabilities of cyberspace, exposing states to the malicious actions of capable actors. As argued by Forsyth and Pope (2014) and more recently by Schneider (2019), this creates a capability-vulnerability paradox that could result in greater instability. Advancing a related argument, Fischerkeller and Harknett (2020) point to the possibility of a *cyber fait accompli* demanding that states compete strategically in cyberspace to support their interests. Reinforcing these arguments, state behavior over the past decade suggests that states respond to these expectations by developing cyber strategies and capabilities following significant incidents and sustained interstate interactions (Blessing, 2021; NATO, 2019). Consequently, it seems that states pattern their behavior on the perceived strategic implications of cyber conflict. This, however, does not adequately explain instances wherein they appear to behave sub-optimally, as previously argued.

Divergent state behavior pre-dates and extends beyond cyber conflict such that scholars proposed that factors other than the system's structure and emergent technologies shape preferences. This prompted the development of alternative theoretical frameworks that recognize the influence of ideational variables in shaping perception among policymakers (Kitchen, 2010; Meibauer, 2020; Rathbun, 2008; Rose, 1998). Critics, however, caution that this possibly violates the realist paradigm (Legro & Moravcsik, 1999; Vasquez, 1997). Advocates, nevertheless, continue to argue that these do not negate the importance of systemic pressures as initially theorized. Instead, ideational variables provide the necessary context as policymakers interpret structural cues (Rathbun, 2008). These interpretations, however, may deviate from reality and lead to the adoption of sub-optimal strategies. Consequently, this

[1] Moving forward, references to realism is understood as structural realism as initially proposed by Waltz (1979) unless otherwise specified.

necessitates the identification of conditions prompting this interpretative mechanism that modulates objectivity among policymakers.

Objectivity, it should be emphasized, requires the availability of information to comply with the normative expectations of rational choice. Already problematic when operating in the conventional domains of air, land, sea, and space, cyberspace introduces additional challenges such as anonymity, order of effects, complexity, and technical concepts (Brantly, 2021). Faced with these conditions, policymakers can utilize greater cognitive, and possibly material, resources to comprehend the environment or resort to cognitive shortcuts to preserve resources and achieve faster closure[2]. While the former is conceivable, temporal and resource constraints (e.g., human expertise) limit this option to a handful of actors (Hansen & Nissenbaum, 2009). The latter, however, is readily accessible and has been empirically demonstrated (Gomez, 2019a; Gomez & Villar, 2018). These findings, however, remain constrained by dependence on non-elite[3] participants and the artificiality of the scenarios. Nevertheless, there is no reason to believe that these mechanisms do not apply to elites (Kertzer, 2020) when facing complex real-world decision-making situations.

Suppose cyber conflict is an extension of strategic competition as proposed by the preceding chapter. In that case, one could argue that established preferences may function as a heuristic to overcome the uncertainty that characterizes the domain. This claim is not without basis, as the last five years saw cyber conflict scholarship acknowledging this possibility (Kaminska, 2021; Kari & Pynnöniemi, 2019; Valeriano et al., 2018). Nevertheless, a theory of national modes of cyber conflict remains absent as scholars have yet to unpack the mechanism linking techno-structural cues, established preferences, and behavior. The remainder of the chapter is organized into three different sections with these in mind.

As structural realism informs cyber conflict scholarship, the following section presents an overview of the theory and surfaces several of its shortcomings. Specifically, the discussion emphasizes the integration of ideational variables that provide insight into state preferences that appear to contradict theoretical expectations. The section concludes by identifying beliefs as a tool used by policymakers when interpreting environmental cues. This is followed by the introduction of strategic culture as a distinct form of belief employed by policymakers as a

[2] This pertains to an individual's motivated need for resolution and the avoidance of ambiguity (Kruglanski & Webster, 1996).
[3] The methodological pitfalls of using non-elite participants in experiments that aim to study elite behavior has led to substantial debates within political science and international relations scholarship (Kertzer, 2020; Mintz, Redd, & Vedlitz, 2006; Suedfeld, deVries, Bluck, Wallbaum, & Schmidt, 1996).

heuristic device when faced with uncertainty. Although the concept of strategic culture is often subjected to a myriad of critiques, the section demonstrates that establishing precise epistemological and ontological positions addresses most of these concerns. The chapter concludes by pivoting the discussion back to the question of cyber conflict. Specifically, it asks whether analysis directed by an ideational framework explains behavior-shaping preferences adopted by policymakers in the context of cyber conflict.

FROM STRUCTURAL TO IDEATIONAL FRAMEWORKS

As previously mentioned, the cyber conflict literature is influenced by the realist tradition wherein preferences develop due to structural constraints faced by states that operate within a given system. The structure of the system is characterized by the ordering of its units (i.e., states) as a function of the distribution of power and the arrangement of the linkages (i.e., alliances or partnerships) between them that generate incentives and hindrances resulting in preferences reflected in discernable patterns of behavior (Waltz, 1979). Moreover, as states are sovereign and capable of determining their actions both within and outside their borders without a centralized authority, the system is regarded as anarchic as states pursue their respective strategic interests. This results in what Glaser (1994) identifies as *competition bias* that captures the conflictual dynamics of interstate relations and typifies structural realism and its derivatives. While offering a parsimonious account of state preferences, realism is constrained by (1) its emphasis on structural attributes (Rathbun, 2008; Rose, 1998), (2) its presumption of rationality[4] (Mearsheimer, 2009), and (3) the absence of micro-level variables that explain the link between anarchy, uncertainty, and conflict (Glaser, 1994; Keohane, 1993; Lake & Powell, 1999).

The importance placed on structure reflects a desire for a parsimonious account of state behavior. However, this ignores the possibility that preferences are not derived solely from the objective interpretation of the distribution of power. Instead, these coalesce around policymakers' perceptions of the strategic environment (Jervis, 1976; Rathbun, 2008). Waltz (1959, p. 238) acknowledges the importance of looking beyond both the structure and system when he notes that *"the third image describes the framework of world politics, but without the*

[4] While Waltz did not explicitly include an assumption of realism into his theory, others such as Mearsheimer (2009) integrate the concept into their extension of structural realism. But as will be shown throughout this chapter, this assumption is challenged by other exogenous factors.

first and second image there can be no knowledge of the forces that determine policy; the first and second images describe the forces of world politics, but without the third image, it is impossible to assess their importance or predict the result."

While this may be interpreted as stressing the importance of structure, a closer reading suggests the presence of a mechanism linking sub-state, state, and the system with one another. However, structural realism fails to unpack this mechanism as it relates to preferences and observed state behavior. Furthermore, the near-exclusive focus on structural variables is cited as constraining its ability to explain divergent behavior (Schweller, 2006; Wivel, 2005). Consequently, this encouraged the development of alternative frameworks such as neoclassical realism. While critics assert that this is an ad-hoc attempt to redeem realism from its failures (Legro & Moravcsik, 1999; Vasquez, 1997), it is better understood as an effort to reframe it as a theory of foreign policy (Rose, 1998; Wivel, 2005).

The establishment of neoclassical realism provides realists with much-needed analytical leverage. Furthermore, its proponents remain firm in that the underlying structure enables and constrains state behavior. However, it parts company with structural realism in its depiction of sub-state variables as mediating the influence of structure on preferences without fundamentally challenging the nature of the international system (Kitchen, 2010; Wivel, 2005). Instead, the fundamental issue is the (non-)objective interpretation of structural cues that determines whether preferences adhere to or stray from the strategic realities faced by states (Rathbun, 2008).

Uncertainty, Rationality, and Preferences

Realism acknowledges that behavior-shaping preferences are grounded on the uncertainty surrounding intent (Greico, 1993; Mearsheimer, 1994; Waltz, 1979). However, despite its importance for realism, uncertainty often remains ill-defined, limiting its explanatory value. Rathbun (2007) tackles this and proposes two different conceptualizations. Uncertainty may manifest as the absence or shortage of information, or it may present as informational ambiguity. While this dichotomy is analytically useful, it ignores the possibility of both forms manifesting simultaneously (i.e., information is both in short supply and vague). For realism, uncertainty is resolved by interpreting the distribution of power through a priori assumptions that others would act to preserve their interests. In other words, policymakers assume that states would exploit the existing balance of power to further their objectives.

Consequently, realism appears to contain an implicit assumption of rationality. If true, then overcoming uncertainty is achieved by accumulating information regarding the intent and capabilities of others (de Mesquita & Lalman, 1992; Keohane, 1993). However, ill-suited policies still emerge despite abundant information (Bar-Joseph & Kruglanski, 2003; Fearon, 1995; Welch, 2011). As such, one could argue that manifestations of uncertainty are not mutually exclusive and that its availability does not negate the possibility of misperception (Jervis, 1976).

Chong (2013) speaks to this possibility by proposing that rationality exists in a gradient wherein individuals may appear more or less rational depending on their underlying motivations, with some seeking greater accuracy while others aim to maintain established beliefs (Lodge & Taber, 2000; Redlawsk, 2002; Taber, Cann, & Kucsova, 2009). If policymakers are treated as rational actors, then the possibility exists that the strategic environment forces them to frame their perceptions with a priori assumptions based on experience or within the temporal or resources constraints that allow for the collection of information (Kruglanski & Webster, 1996; Moravcsik, 1997). Phrased simply, policymakers need to contend with the availability and ambiguity of information along with their underlying beliefs that collectively bound their perceptions.

The degree to which perceptions are bounded determines how accurately these represent the (strategic) environment, necessitating a compromise between parsimony and reality. The more parsimonious the assessment, the more disconnected it is from reality (Todd & Gigerenzer, 2012). For critics of realism, its inability to explain paradoxical state behavior is linked with its aspirations for parsimony (Rose, 1998). This problem, however, cannot be resolved by simply adding variables to the strategic calculus of policymakers (i.e., expanding the boundaries). Brantly (2021) explains that these shortcomings are not necessarily the result of information provision errors but may indicate certain intangible factors used to interpret the information. Consequently, collecting more information alone does not resolve questions of ambiguity and meaning. To paraphrase Rose (1998), policymakers see the world through a dark glass. The question, though, is the form in which this presents itself to policymakers and the conditions in which it is used.

Proceeding with arguments based on the boundedness of rationality, it should be noted that rationality is not a prerequisite of realism. Instead, what exists is a prescription rather than an expectation of rationality (Barkin, 2003). Contemporary expressions of realism suggest that policymakers ought to act rationally to pursue their objectives – not that they will. This leaves

room for the possibility of policymakers adopting counterintuitive preferences. As Sterling-Folker (1997, p. 19) scathingly puts it, states are *"free to act as they wish"* to the extent that they are *"free to die."* Furthermore, it provides conceptual space for immaterial and intangible variables to provide analytical leverage. While some may protest that realism is fundamentally materialist and incompatible with other ontologies (Wendt, 1999b), this is not necessarily the case. Barkin (2003) proposes that this critique can be tackled if the perceived incompatibility is distilled into its fundamental attributes that include (1) realism's focus on material capabilities and (2) its identification of human nature as materialistic.

While a cursory reading of realist scholarship suggests the importance of material capabilities relative to perceptions of power and its distribution, it readily points to immaterial factors as necessary for a holistic understanding of power (Carr, 1964; Gilpin, 1981; Morgenthau, 1948; Strange, 1987; Waltz, 1979; Wolfers, 1962). Although realists often utilize tangible material capabilities as a point of reference, this does not nullify the importance of intangible artifacts (e.g., doctrine). This leads to the second point and the assumption that human nature is inherently materialistic. This refers to a priori assumptions such as insecurity and fear following perceived imbalances that are derived from the material capabilities of others. Realist logic, however, does not conclude that all individuals come to this understanding and are thus fearful, simply that only a handful of individuals can exhibit this tendency under specific conditions (Barkin, 2003). To assume that all policymakers express this sense of fear inadvertently suggests that their experience vis-à-vis others are exclusively associated with this emotion (Bleiker & Hutchison, 2008; Holmes, 2015; Marcus, 2000). Relatedly, other immaterial aspects such as identity and history inform threat perception (Garcia-Retamero, Muller, & Rousseau, 2012; Herrmann, Voss, Schooler, & Ciarrochi, 1997; Rousseau & Garcia-Retamero, 2007). If these arguments are valid, states remain subject to structural constraints within the international system. Their perception of such, however, is *"partly of their own making"* (Rose, 1998, p. 153). Consequently, the utility derived from their preferences depends on how well their perceptions align with reality.

The Role of Ideas

Ideational frameworks provide scholars the opportunity to understand better the conditions in which states, faced with comparable structural constraints, behave differently (Weingast, 1995; Wivel, 2005; Yee, 1996). Furthermore, the integration of ideational variables

considers the extent to which policymakers exercise rationality in the face of uncertainty. This, however, raises the question of determinacy; whether material or ideational attributes are the prime determinants of behavior (Kitchen, 2010; Meibauer, 2020; Rathbun, 2008). As Wendt (1999a, p. 407) asserts, ascribing to the former is indicative of the belief that *"the most fundamental fact about society is the nature and organization of material forces."* This corresponds with the core tenets of realism wherein (perceptions of) the balance of material capabilities enables and constrains state behavior. The latter, however, asserts that *"the most fundamental fact about society is the nature and structure of social consciousness."* Viewed this way, the implications of the material reality are not self-evident and are socially constructed. However, these distinctions are only matter insofar as realism disavows that analytical value of ideas.

Structural realism undoubtedly reflects materialist tendencies; however, its predecessor tacitly acknowledges the value of ideas. While emphasizing the concept of power and its pursuit thereof, classical realists accept the influence of ideas alongside material factors (Kitchen, 2010; Rose, 1998). Morgenthau (1972, p. 11) notes that ideas are a catalyst for change *"when people see things in a new light, they may act in a new way."* Similarly, Carr (1964, p. 87) posits that *"there is something which man ought to think and do, but that there is something which he can think and do, and that his thought and action are neither mechanical nor meaningless."* In these instances, both Morgenthau and Carr assert that the meaning behind structural cues is not self-evident, allowing for interpretation through priors such as ideas. Consequently, classical realists implicitly argue that the environment is not simply defined by the distribution of power but also by a plurality of ideas that demarcate *"the sphere of possible political interests"* (Morgenthau, 1938, pp. 125 - 126). This provides the necessary conceptual space for incorporating ideas that contextualize the strategic environment.

Integrating ideas without incurring paradigmatic violations is possible if the environment is treated as a *"permissive system rather than an independent causal force"* (Walt, 2002, p. 211). This suggests that material realities do not directly impact behavior-shaping preferences but whose effects are mediated. Rathbun (2008) makes this argument when observing that structural realism does not provide a mechanism linking its proposed causes and expected effects and that information is subject to policymakers' interpretation. This is crucial as it provides the rationale behind misinterpretation and misperception. If the structure functions as a *"selector"* (Waltz, 1979, p. 73), which *"rewards some types of behavior and*

punishing others" (Gilpin, 1981, p. 85)**,** perceptions determine how accurately policymakers interpret environmental cues.

The process of linking material reality and behavior through ideas offers much-needed insight. Faced with a complex and uncertain environment, ideas serve as a focal point that enables the coordination of behavior (Berman, 2013; Weingast, 1995). Relatedly, Goldstein (1993) reinforces this by asserting that ideas provide policy roadmaps in response to stimuli such as changes to the underlying structure. Consequently, it is unproductive to argue whether ideas or material reality exclusively determine state behavior; both play a crucial role.

An Ontology of Ideas

Although the concept of ideas continues to garner analytical traction, the literature remains inconsistent in its conceptualization and differentiation with other related constructs. It is not unusual, for instance, to find it used interchangeably with beliefs, ideologies, mental models, etc. This is problematic as its explanatory value depends on accurately capturing its nature and scope. Before tackling how ideas are employed to interpret material reality, an ontology of ideas is necessary. Cray and Schroeder (2015) offer four criteria with which to characterize ideas that include its (1) creation, (2) distribution, (3) causation, and (4) evolution. While broadening the concept of ideas may seem counter-productive, this serves to address the epistemological and ontological concerns surrounding its use.

For something to be considered an idea requires that it be created rather than assumed to exist. Ideas emerge within a specific context that makes them historical particulars[5]. Consequently, ideas are not necessarily manifestations of the status quo. For instance, realists argue that (the idea of) fear of how others may exploit the structure to their advantage explains state behavior. As previously noted, however, realism does not claim that all policymakers subscribe to this idea. These are, instead, constructed in response to both the environment in which policymakers are embedded and individual mental states. This is reminiscent of Berman (2013) who asserts that ideas emerge through a two-step process wherein the first stage represents a demand for new ideas, often following the perceived failure of those previously established.

[5] Such that specific ideas develop in response to a particular stimulus.

However, the act of creation alone does not suffice to constitute an idea. To be considered, these need to be public rather than private; that is to say, shared by more than one individual. Although Cray and Schroeder (2015) suggest that creation remains an individuated event, sustaining an idea requires transmitting and sharing it with others. While constructivists differ in their approach as to how ideas are communicated and prolonged, a common notion exists that ideas are fundamentally a social phenomenon (Campbell, 2002; Weingast, 1995; Yee, 1996) and that these are *"intersubjectively constituted forms of social action that shape social reality"* (Bieler & Morton, 2008, p. 106).

Aside from creation and distribution, ideas need to be part of a specific causal order that affects constructs inclusive of other ideas. As with its social dimension, the exact causal role of ideas remains in dispute. Those of a neopositivist persuasion, for instance, conceptualize ideas as having a direct causal effect such that ideas are treated as discrete objects that operate apart from individuals and are thought to exist as a given (Goldstein & Keohane, 1993). This treatment is problematic as it violates the conditions of creation and distribution as previously discussed. Cray and Schroeder (2015, p. 760) assert that ideas *"can make things happen if only insofar as they are capable of inspiring agents to make things happen."* This phrasing is crucial, suggesting that ideas have an indirect causal effect that leaves agency, ultimately, in the hands of an individual(s). Jervis (2009), for instance, argues that beliefs, an ideational construct, influence and set expectations and determine whether certain propositions are seen as plausible. Similarly, identity generates notions of *us* and *the other* that, in turn, dictate how environmental cues are interpreted and responded to (Rousseau & Garcia-Retamero, 2007). Consequently, ideas manifest themselves in the causal process as mediating variables that provide context for environmental cues.

Finally, ideas must be capable of evolving and undergoing change. Berman (2001) acknowledges this possibility in the second stage of his two-step process for the emergence of ideas. He argues that change occurs when contemporary ideas are called into question (e.g., in the event of policy failure). During this step, the unsuitability of previous ideas results in a demand for new ones supplied by actors who serve as champions (Meibauer, 2020). In this case, the historical record is replete with instances in which, following military defeat, a handful of individuals espouse changes to doctrine and worldview within a given state (Katzenstein, 1996; Legro, 1995).

Ideas Expressed as Beliefs

Providing an ontology of ideas alleviates a host of analytical problems. However, several ideational constructs that correspond with the characteristics above provide a contextual lens for policymakers. To explain how ideas influence behavior-shaping preferences, it is necessary to distinguish between different manifestations. Doing so (1) helps to establish the actors relevant in its creation, expression, and maintenance, (2) demonstrates how it interacts with policymaking, and (3) determines the ease (or difficulty) of studying its effects (Berman, 2013).

Beliefs and belief systems are ideational constructs frequently used to explain how policymakers perceive their environment. Belief systems are *"the total universe of a person's belief about the physical world, the social world, and the self"* (Rokeach, 1968, pp. 123 - 124). Applied to politics, George (1969) developed an operational code belief system divided into two sub-components; beliefs regarding the nature of politics and beliefs involving the means to achieve specific goals. Consequently, beliefs are thought to exist hierarchically, with broad central beliefs connected to peripheral ones found at lower hierarchy levels (Larson, 1994).

If beliefs are treated as a manifestation of ideas, these must meet the previously established criteria. Keeping in mind that creation is an individualistic process, cognitive and social psychology informs the creation of beliefs. Take the case of enemy images, for instance. These are expectations of malicious behavior attributed to others that emerge through repeated and salient interactions (Holsti, 1962). Once established, these serve as a reference by which policymakers interpret the intent of and possible response to misbehavior (Boulding, 1959; Herrmann et al., 1997; Holsti, 1962, 1967). Furthermore, enemy images may be invoked outside the context of their creation (Dreyer, 2010), consequently defining the relationship and behavioral expectations between oneself and others. While this demonstrates the creation of a belief, it does not explain its diffusion.

As per the literature, ideas are diffused either through the bureaucratic role played by epistemic communities or by the encasement of specific beliefs within institutions themselves. For the former, beliefs spread when policymakers consult with expert communities who use the opportunity to influence the development and adoption of policies reflecting their beliefs. As such, beliefs are diffused through persuasiveness stemming from expert authority (Libel, 2016; Yee, 1996). Institutions, in contrast, *"reflect a set of dominant ideas translated through legal mechanisms into formal government organizations"* (Goldstein, 1988, pp. 181 - 182).

Consequently, institutions manifest beliefs when these provide the necessary support for their expression (Abdelal, Blyth, & Parsons, 2010; Béland & Cox, 2010; Hall & Taylor, 1996). Phrased differently, institutions advocate for policies and processes that represent these beliefs. Beliefs, moreover, function as focal points that provide the appropriate policy response given a particular stimulus (Berman, 2013; Goldstein & Keohane, 1993; Weingast, 1995). In addition, institutions also constrain the access, flow, and impact of ideas in the policymaking process. Consequently, this moderates the creation and perpetuation of certain beliefs. Nevertheless, despite the role of epistemic communities and institutions in the diffusion and perpetuation of beliefs, the causal process in which beliefs are embedded requires further analysis.

Goldstein and Keohane (1993) utilize the proposed hierarchical structure of beliefs and advance a typology that includes (1) world views, (2) principled beliefs, and (3) causal beliefs. World views exist at the top of the hierarchy and are the broadest of these constructs. These represent abstract ideas associated with the symbolism of a particular culture (e.g., religion). While these provide insight into the mindset of policymakers, their abstractness makes it challenging to identify their impact on preferences. Directly below these are principled beliefs that provide normative guidance concerning issues. These are associated with specific world views and may profoundly influence preferences. Finally, causal beliefs establish a cause-effect relationship that guides how objectives are achieved. These objectives, in turn, are influenced by either world views or principled beliefs. Amongst the three, causal beliefs demonstrate the most apparent effects on behavior-shaping preferences.

Two fundamental critiques, however, can be leveled against this typology. First is the tacit conflation between ideas and interests. It is not difficult to buy into the notion that interests reflect ideas (e.g., beliefs) or that it is in the interest of individuals to ascribe to a particular idea. There is, however, no reason to argue that individuals may hold onto ideas that are contradictory to their interests such that these remain conceptually distinct (Kitchen, 2010; Meibauer, 2020). For instance, it may be in the state's interest to signal their resolve through over displays of military capabilities as a means of deterrence, but this may come into conflict with the belief of some policymakers that doing so risks escalation. Consequently, this leads into the second critique as Kitchen (2010) finds the conflation of ideas and beliefs problematic when he notes that proponents (i.e., Goldstein and Keohane) acknowledge that ideas continue to have a causal effect even if no one believes in them. This encourages Laffey and Weldes (1997) to conclude that ideas and beliefs are distinct, leading to the assumption that for

something to be a belief, someone must believe in it. However, the separation of ideas and beliefs does not preclude the possibility that these two may interact with one another such that ideas provide the necessary roadmap to interpret reality (i.e., interests) under conditions of uncertainty and how best to pursue these (Goldstein, 1993). Cray and Schroeder's (2015) ontology renders these distinctions moot, provided that both ideas and beliefs have an observable causal effect. The issue raised by Laffey and Weldes above appears to be a matter of externalizing beliefs that others would ascribe to, as will be discussed in the succeeding paragraphs.

In his treatment of these critiques, Kitchen (2010) advances a separate typology that extends that of Goldstein and Keohane's (1993) to fit better the role of ideas in shaping policy. Grounding this hierarchy are scientific ideas that frame the relationship of entities within the international system. These establish what is (strategically) possible in the context of the environment (Jervis, 2009). Examples include the notion that democratic states are generally pacific and unlikely to come into militarized conflict. Directly following these are intentional ideas that define policy goals and are akin to principled beliefs. It should be noted that intentional ideas that run against interests can exist, although less likely to garner support. In keeping with the previous example, these could include the promotion of democratic norms. Finally, operational ideas are derived from scientific or normative ideas and provide the means to pursue objectives. These function in much the same way as causal beliefs. For instance, the promotion of democratic norms can manifest through continued efforts to support diplomatic initiatives to reduce conflict.

While these typologies demonstrate the causal effects of beliefs, these do not address how the difference between ideas and beliefs are reconciled or how beliefs evolve. Meibauer (2020) resolves this by asserting that ideas exist as externalized individual beliefs. He notes that rather than remaining as individual mental states, ideas must be externalized through a discursive process by *"individuals or groups capable of persuading others to reconsider the way they think and act."* In doing so, advocates (i.e., champions) utilize ideas such that policies *"reflect their preferred interpretation"* (Meibauer, 2020, p. 30). This treatment is in keeping with the above ontology. It reinforces the need for diffusion and raises the possibility for change and evolution through discursive contestation within a particular community. Furthermore, this overcomes the critique surrounding the distinction between ideas and beliefs such that the latter becomes an external and socialized manifestation of the former. The emphasis on introducing ideas into political discourse by advocates is established in the

literature (Campbell, 2002; Yee, 1996). Meibauer (2020, p. 31), however, provides the logic that closes the phenomenological gap between ideas and beliefs such that this *"semi-discursive conception of ideas is ontologically 'adequate': ideas can be created by particular people (based on beliefs), distributed (in communication), embedded in causal sequences (as variables), and changed (for example, they can be forgotten)."*

With these in mind, it could be argued that beliefs are the hierarchical ordering of ideas that reflect distinct perspectives of the political world that exact specific causal effects in the form of behavior-shaping preferences. Abstractly, beliefs may be conceptualized as ideas in aggregate form such that these are viewed as a collection of *"token mental states, where the token mental states that compose the aggregate are selected on the basis of their descent (by intellectual grasping) from some original token mental state that is not so descended from any other token mental state of the same type, are well defined entities that seem to have the persistence conditions required"* (Cray & Schroeder, 2015, p. 767). This reaffirms the interdependency of the beliefs and their durability. However, while this provides the nature and structure of beliefs, the issue of content remains unaddressed and is especially relevant as these account for how policy preferences are expressed.

STRATEGIC CULTURE AS BELIEFS

In acknowledging that beliefs, as an ideational variable, provide meaning to the structural realities faced by policymakers, the question of content comes to the fore. In the political science and international relations literature, references to culture shaping preferences date back to as early as the 1930s and 1940s with national character studies strongly linked with anthropological research that later evolved into strategic culture scholarship (Lantis, 2002; Sondhaus, 2006). Although scholars such as Campbell (2002) and Berman (2013) assert that culture and beliefs are distinct ideational constructs, this may simply reflect the inherent challenges in defining the former that continue to characterize strategic culture scholarship.

Given the plurality of definitions, the dissertation treats strategic culture as *"widely shared, identity-driven norms, ideas, and beliefs about the legitimate use of force by the state for the provision of security"* (Mirow, 2016, p. 34). The applicability of this definition becomes apparent throughout this section and addresses several concerns surrounding the concept. Furthermore, this corresponds to the fundamental issues that frame this dissertation; preferences surrounding the strategic use of cyber capabilities by states pursuing their

(security) goals. Gray (1981, pp. 22 - 26) asserts that strategic culture produces *"modes of thought and action with respect to force"* that result in *"dominant national beliefs"* with respect to established state behavior. This conceptualization appears to provide the causal link between beliefs (i.e., ideas) and behavior. This, however, belies the challenges associated with a concept as contentious as strategic culture.

Following in the footsteps of Snyder (1977) and his culture-centric explanation of Soviet nuclear strategy, strategic culture has since yielded four distinct generations of scholarship. The first, typified by work from Gray (1981), Snyder (1977), and Booth (1979), treats strategic culture as derived from deeply historical experiences that constitute a monolithic and undifferentiated depiction of culture, resulting in the emergence of semi-permanent preferences. The second generation adopts a different perspective. Whereas first generation scholarship asserts a deterministic correspondence between culture and strategic behavior, the second generation acknowledges the possible instrumental use of strategic culture (Johnston, 1995). Proponents (Klein, 1988; Lock, 2010) recognize the possibility of policymakers framing (strategic) interests in the context of culture as a means of gaining legitimacy that could result in a divergence between strategic discourse and operational behavior. Moving forward and tending to vary most in terms of their treatment of the concept, third generation scholarship avoids conflating strategic culture with strategic behavior in a bid to develop a falsifiable theory of state behavior grounded in culture. Developments within this tradition are often traced back to the seminal debate between Johnston (1999) and Gray (1999) in the late 1990s.

While the first three generations of strategic culture research provide an alternative to structural-materialist explanations of state preferences and behavior, significant epistemological and ontological cleavages exist between these[6]. Bracketing these challenges is the distinction between research attempting to *understand* and those seeking to *explain* phenomena (Bloomfield, 2012; Gray, 1999). Adherents to the former, primarily first and second generation scholars, assert that strategic culture does not exist as a separate reality from that of the researcher such that instances wherein it influences preferences are the result of distinct conditions that effectively negate attempts at generalization. The latter, in contrast, proposes an objective truth that can be observed and tested if causes are distinguished from the

[6] This also implies that methodological differences exist. These, however, are not the focus of this section.

relevant effects (Hollis & Smith, 1990). Three crucial questions emerge from these fundamental differences.

First is that of definition. For scholars only beginning to acquaint themselves with this concept, it soon becomes apparent that a plurality of definitions for strategic culture involves different levels and units of analysis. While it is vital to settle on an appropriate definition, this section emphasizes the epistemology and ontology of strategic culture and how it relates to ideas and beliefs. This is not to say that definitions are unimportant. Instead, ascertaining how and what we know about strategic culture allows for more flexibility in selecting definitions appropriate for the questions raised. In establishing what strategic culture is, it is necessary to ask how it is created, maintained, and transmitted. While the importance of such may seem commonsensical, this emphasis is necessary as a heated scholarly debate centers around this issue (Bloomfield, 2012; Johnston, 1995; Libel, 2020). Whereas the former (i.e., the nature of strategic culture) is often less problematic if scholars are clear on their epistemological and ontological orientation, the operationalization of the concept remains a point of contention. Specifically, the question of how and if strategic culture changes is of utmost concern. This aspect is particularly salient since culture implies permanence which leads critics to argue that strategic culture is overly deterministic (Bloomfield, 2012; Johnston, 1995).

With these in mind, it is necessary to note the emergence of the fourth generation of strategic culture scholarship (Libel, 2020). While scholarly work in this tradition has yet to achieve critical mass, these distinguish themselves through their epistemological and ontological leanings, typified in the timely article from Bloomfield (2012). Whereas previous generations were associated with either a common epistemological orientation (e.g., interpretivism in the case of first and second generation scholarship) or epistemological distinction (e.g., positivism in the case of the third generation), those that identify themselves with the fourth generation adopt analytical pluralism when approaching theoretical and methodological questions. Furthermore, scholars of this persuasion differentiate themselves by addressing the question of strategic culture and change instead of stability (Burns & Eltham, 2014; Haglund, 2014; Libel, 2016).

The Role of Strategic Culture

In 1995, Alastair Johnston (1995) published a seminal article detailing the advances and pitfalls of strategic culture scholarship and proposed ways forward. He notes that strategic

culture scholarship overlaps in terms of two core arguments despite divergent approaches. First, states reflect contrasting strategic preferences as a function of early formative experiences. With this in mind, strategic culture is believed to be the result of a constellation of factors that include macro-environmental variables (e.g., geography, history, ethnocultural attributes), societal variables (e.g., social, economic, and political institutions), and micro-level variables (e.g., military institutions, civil-military relations) (Jones, 1990). This, however, does not preclude the possibility of anchoring strategic culture on recent experience. Second, ahistorical variables (e.g., the balance of power) are of secondary importance and only gain meaning when viewed through the lens of culture. In keeping with the underlying assumptions of ideational frameworks regarding preferences, the theorized role of strategic culture presupposes that ahistorical variables do not exert a direct causal effect. These are, instead, interpreted through strategic culture. Nevertheless, this should not be taken as an attempt to challenge the assumed rationality of policymakers.

As Johnston (1995) notes, strategic cultural frameworks are compatible with certain expressions of rationality. To start with, limited rationality is present when ideational constructs (e.g., strategic culture) simplify reality. When faced with uncertainty, policymakers may employ heuristic mechanisms to minimize cognitive load and reach closure (Hafner-Burton, Hughes, & Victor, 2013; McDermott, 2001; Norman & Delfin, 2012). These constructs also provide ranked preferences wherein alternatives are quickly dismissed in favor of those better aligned with underlying beliefs. Mintz (2004), for instance, advances his poliheuristic theory wherein policymakers first employ heuristics to limit the number of choices and then revert to more rationalist strategies when selecting their final preference; thus, expressing process rationality. Lastly, ideational constructs may be employed as a guide for what is appropriate. This may reflect policymakers' tendency to gravitate towards preferences that correspond with normative expectations, thus illustrating adaptive rationality and a logic of appropriateness (Mirow, 2016).

However, despite these similarities, Johnston remains critical of earlier scholarship, particularly the first generation. To begin with, early conceptualizations of strategic culture tended to include a legion of variables. As Johnston (1999) notes in a later article, identifying multiple variables that explain state behavior is fundamentally unproblematic given the phenomenon's complexity. However, treating strategic culture as the combined manifestation of all these variables leaves little conceptual space for non-strategic explanations. Consequently, the conceptualization of strategic culture among first generation scholars is

over-determined such that the rubric of strategic culture addresses every aspect of state behavior. Paradoxically, Johnston and others (Bloomfield, 2012; Lantis, 2002) also find the first generation's conceptualization simultaneously under-determined in that no scope conditions exist to establish the circumstances in which strategic culture is causally relevant. In effect, while strategic culture appears to explain most, if not all, aspects of state behavior, the first generation scholarship could not clarify conditions in which it could not. Moreover, Johnston (1995) continues his critique when noting that early scholarship fails to distinguish between strategic culture and strategic behavior. Gray's treatment of *"modes of thought and action"* that bring about *"dominant national beliefs"* suggests that culture and behavior are co-constitutive, resulting in a tautology. For Johnston, this precludes observing the effects of strategic culture on behavior and, consequently, preferences and prevents engaging in further theory testing.

Responding to these points, Gray (1999, p. 51) concedes that while Johnston makes fair, albeit misguided arguments, moving scholarship in this (positivist) direction will lead *"followers into an intellectual wasteland"*. Gray (1999, p. 51) emphasizes his view of strategic culture as shaping context for behavior and constituting behavior itself such that culture *"surrounds, and gives meaning to, strategic behavior, as the total warp and wood of matters strategic that are thoroughly woven together, or as both."* This stresses the first generation perspective in depicting policymakers as enculturated individuals who cannot help but act in a certain way because of their cultural embeddedness. Consequently, he does not challenge the tautology raised by Johnston in reiterating his interpretivist epistemology. In hindsight, however, scholars such as Glenn (2009) do not find competing epistemologies overly problematic, noting the presence of epiphenomenal, conventional constructivists, post-structuralist, and interpretivists approaches that have emerged since the Johnston-Gray debate. This, however, limits the possibility of research collaboration and the success (or desirability) of theory testing.

Nevertheless, Gray (1999) implicitly introduces a means to reconcile his views with Johnston's despite their differences. He does so when suggesting the value of treating culture as an idea that justifies the assumptions surrounding strategic behavior. He cites Bathurst (1993, p. 24), who notes that *"strategic culture, here, refers to those prominent patterns of (strategic) behavior which are indicative of social ways of seeing and responding to 'reality'."* Although he employs this mindset to explain the encompassing aspect of strategic culture, it recognizes (or at least does not negate) strategic culture as an interpretative lens that gives

meaning to material reality. While Gray avoids causal language, this treatment hints at its role as a mediating variable. Poore (2003) recognizes this and calls for a *context all the way down*[7] approach such that context provides the a priori justification for beliefs that undergird theoretical traditions such as structural realism. This is not lost on scholars across these two generations (Gray, 1999; Johnston, 1995; Snyder, 1977) who recognize that strategic culture functions as an ideational milieu that provides the context through which the environment is interpreted, and preferences are selected. Later scholars such as Mirow (2016) treat strategic culture as a formal conditioning cause[8] in explaining policy outcomes. He argues that strategic culture precedes agency and gives meaning to material reality; in the words of Gray, it provides the necessary context. This depicts strategic culture not as an independent cause but as a mediating variable that shapes policymakers' perspectives (Bloomfield, 2012; Mirow, 2016).

Beliefs, Schemas, and Strategic Culture

Treating strategic culture as beliefs that provide context is consistent with the perspective of anthropologists and sociologists whose research informs the use of culture in international relations. Medin, Unsworth, and Hirschfeld (2007) note that we should *"look at cultures [as] mental representations (and attendant behaviours) that are distributed across individuals in a population . . . this view focuses on the stabilizing role of cognitive structures and schemas in the production and transmission of ideas (and attendant behaviours) that achieve widespread cultural distribution."* Viewing culture as a distributed mental construct represents how sociologists and psychologists have treated culture and acknowledge its status as an ideational variable (Parsons, 1937; Weber, 1946). By the 1970s, scholars adopted definitions that link both ideas and behavior, noting that cultures were *"depositories of widespread interests and feelings"* that *"transmit meanings from person to person"* (Dittmer, 1977, pp. 557 - 569).

While these conceptualizations correspond with Cray and Schroder's (2015) ontology regarding creation, distribution, and causation, the latter is misplaced regarding its causal position if policymakers assert the contextual value of (strategic) culture. Fortunately, this position was adopted by the 1980s and 1990s when sociologists began to approach culture as mediating variable. Swidler (1986) and Tilly (1992) argue that culture serves as a catalog

[7] This overlaps with Johnston's (1999) *ideas all the way down* proposal.
[8] As per Mirow (2016, p. 30) *"condition and empower an action"*. Specifically, a formal conditioning cause functions as a source of meaning (Hagmann, 2010; Kurki, 2006).

containing interpretative strategies to navigate the material world. Within psychology, a comparable construct exists and is known as a cognitive schema.

A schema is defined as a *"cognitive structure that represents knowledge about a concept or type of stimulus, including its attributes and the relations among those attributes"* (Larson, 1994, p. 18). Although often used interchangeably with beliefs, schemas exist at a higher level of analysis and subsume the former (Larson, 1994). Furthermore, schemas are constructed around interrelated knowledge about a concept or a stimulus in much the same way as beliefs and are organized spatially, temporally, or logically (Wyer Jr & Gordon, 1984). This suggests that related schemas may be ordered in logical hierarchies much in the same way as the model proposed by Kitchen (2010). Norman (1981) reinforces this argument with his notion of action schemas wherein top-level schemas establish the underlying objectives while lower-level schemas provide the means with which these are achieved in much the same way as proposed by Goldstein and Keohane (1993) and Kitchen (2010). The context-granting feature of schemas is further strengthened by DiMaggio (1997, p. 277)**,** who advances the concept of logics of action as a set of *"representations or constraints that influence action in a given domain"* that points to the fundamental purpose of schemas.

In keeping with Gray's expectations, schemas provide the necessary context when activated by the corresponding external stimuli (Larson, 1994; Welch, 2011). For example, if an adversary purchases additional combat aircraft, the combination of both the actor's identity (i.e., an adversary) and their action can trigger schemas that serve to inform policymakers of the possible intent (i.e., context). Furthermore, if schemas constrain the range of possible actions as proposed by DiMaggio (1997), then one could argue that the schema determines the expected response (or lack thereof)[9]. In effect, this addresses the concern of Johnston and other third generation scholars who expect strategic culture to have a defined causal role. Additional benefits, however, are also achieved through this operationalization.

Contemporary scholarship recognizes that early conceptualizations of strategic culture were theoretically underspecified and unclear as to when strategic culture could (or could not) explain preferences reflected through behavior. As a heuristic device, policymakers may employ cognitive schemas when the information environment they face is uncertain (Johnson & Tierney, 2011; Lau & Redlawsk, 2001; Norman & Delfin, 2012). This statement is not meant to discount the rationality of policymakers but, instead, acknowledges the limits of human

[9] This does not suggest that the decision-maker is irrational. Instead, the meaning of the cues that are received from the environment are contingent on the schematic structure.

cognition. According to Kahneman (2011), human cognition is governed by two distinct systems identified as System 1 and System 2. The former operates subconsciously and employs heuristics to address a complex information environment efficiently. In contrast, the latter represents what we might identify as rational thought and requires greater cognitive and, in some instances, temporal resources when processing information.

While cognitive and social psychologists have long since demonstrated heuristic usage in day-to-day decision-making, political psychologists have also identified these employed in various areas of research that include electoral behavior (Lau & Redlawsk, 2001; Taber et al., 2009), foreign policy analysis (Khong, 1992; Mintz & DeRouen Jr., 2010), and intelligence studies (Bar-Joseph & Kruglanski, 2003; Yarhi-Milo, 2014). Furthermore, these processes gain prominence in the face of an uncertain environment and when the need for cognitive closure is great (Kruglanski & Webster, 1996; Norman & Delfin, 2012). Consequently, one could argue that the degree of rationality in political decision-making is a relative rather than absolute phenomenon[10] (Chong, 2013). The corresponding scope conditions become apparent if we treat strategic culture as schemas that function as heuristic devices. When faced with uncertainty, policymakers utilize strategic culture to give meaning to the structural cues they receive. These, in turn, surface contextually appropriate preferences that shape observed behavior. This logic is consistent with the expectations of rationality among strategic culture scholars, specifically Johnston (1995), who acknowledge its compatibility with strategic culture.

Creation, Transmission, and Hegemony

For observers of strategic culture scholarship, it becomes apparent that progress in the field centers on aspects of the Johnston-Gray debate. This raises important questions of what strategic culture is, what it does, and how it should be studied? While these are valid concerns, overemphasizing these comes at the costs of other equally relevant questions. Specifically, first and third generation scholarship (1) does not address the role of agency vis-à-vis strategic culture and (2) only tackles the possibility of strategic cub-cultures in passing.

The question of who or what creates strategic culture is often neglected by those who subscribe to first and third generation perspectives. Both assume that policymakers naturally possess a distinct strategic culture. This is pronounced in third generation scholarship as no

[10] This is not problematic as heuristics can serve to complement or outperform deliberate and effortful cognition in certain instances (Lau & Redlawsk, 2001).

explicit mention is made of the agency involved in its creation (Lock, 2010). The first generation, in contrast, suggests the possibility of agency (Gray, 1981; Snyder, 1977). Its significance, however, is suppressed owing to the overly deterministic depiction of strategic culture (Gray, 1999). Both remain silent on agency's value in terms of its operation and transmission. For those wishing to assign causal significance to strategic culture, its conceptualization as a cognitive process requires policymakers to subscribe to individuated mental models. This, however, ignores the reality that policymaking is a collective process (Johnston, 1995; Lantis, 2002; Lock, 2010). Furthermore, suppose we assert that strategic culture and strategic behavior remain conceptually distinct. In that case, this necessitates the assumption that policymakers are cultural "dupes" with little to no influence over culturally derived preferences. Relatedly, while first generation scholars recognize the ability of individuals to push against the influence of culture, they do not provide further explanation beyond the provision of context (Lock, 2010).

A way forward is to adopt the perspective of second generation scholarship. This requires recognizing the constructed nature of social reality such that observed practices are identified as functions of the social structures that define what is possible in terms of social and discursive interactions (Klein, 1988; Lock, 2010). This approach is unsurprising given the constructivist overtones adopted by strategic culture scholarship during the 1990s (Lantis, 2002). Consequently, this argument can be extended such that meaning derived from context is ultimately predicated on these social structures, thus assuming a degree of intersubjectivity. In doing so, strategic culture is conceptualized as *"an intersubjective system of symbols that make possible political action related to strategic affairs"* (Kratochwil, 2001, p. 19).

When adopting this conceptualization, strategic culture provides interpretative power that assigns meaning to certain practices. Furthermore, this grants legitimacy to some practices while denying others due to the intersubjectivity which emerges through a discursive process (Johnston, 1995; Lock, 2010). This is conceptually useful as it pivots effort away from tackling the origins of strategic culture and instead surfaces how distinct notions of strategic culture are expressed (i.e., externalization of the schema) and gain (or lose) favor within a community of policymakers. Furthermore, this presupposes the existence of a plurality of sub-cultures that compete for hegemony (i.e., to become the dominant strategic culture).

Multiple sub-cultures are not foreign to either first or third generation scholarship. Neither, however, provide an adequate explanation of how these gain or lose prominence resulting in what Bloomfield (2012) labels as an excessive-continuity problem, the idea of a

persistent and unchanging hegemonic strategic culture. Operationalizing strategic culture as a cognitive schema resolves this issue as nothing prohibits the presence of multiple, and possibly contradictory, schemas (Bloomfield, 2012). These individuated schemas result from distinct experiences or emerge following socialization into specific communities with unique beliefs and preferences (e.g., institutions) (Crocker, Fiske, & Taylor, 1984; Harris, 1994; Kalyuga, 2010; Lau, Kilbourne, & Woodman, 2003). Nevertheless, different schemas may still overlap because of deeper enculturation (Mirow, 2016). To paraphrase Gray, individuals from State X may hold different preferences on achieving Objective Y, but all share some cultural tendencies of State X. For these schemas to be transmitted and possibly achieve hegemony, these must be expressed externally and reinforces the importance of analyzing the communicative practices of those involved in policy deliberations.

As noted by Risse (2000, p. 5), *"the human agent does not exist independently from the social environment and its collectively shared system of meanings."* Consequently, it could be argued that the success of a particular schema in becoming the hegemonic strategic culture is predicated on its resonance among other policymakers. This view is shared by Meibauer (2020), who notes that individual beliefs only gain interpersonal relevance and exert influence over policymaking (e.g., by establishing commonly held preferences) when they are introduced by individuals that champion it. In turn, schemas only matter once an individual introduces and champions these during policy deliberation. As per Berman (2001, p. 235), *"individuals or groups are capable of persuading others to reconsider the way they think or act."* Schemas, in this sense, are employed as deliberative devices to communicate and convince others to grant a preferred context to a situation or issue.

The emphasis placed on discourse is a recent development in the literature. Libel (2020) approaches strategic culture from the point of view of discursive institutionalists. By doing so, discourse is seen to *"encompass not only the substantive content of ideas but also the interactive processes by which ideas are conveyed. Discourse is not just ideas or 'text' (what is said) but also context (where, when, how, and why it was said). The term refers not only to structure (what is said, or where and how) but also to agency (who said what to whom)"* (Schmidt, 2008, p. 313). Examining strategic culture in this light is instructive as both perpetuation and change are not treated as the sole effect of external shocks (Lantis, 2002;

Legro, 1995; Thompson, Ellis, & Wildavsky, 1990). But instead, it takes into consideration discourse involving an actors' ideas at critical junctures[11].

Building on this rationale, the persistence of the hegemonic strategic culture is attributed to its advocates' cognitive state and exogenous circumstances. Schemas are subject to change under certain conditions (Larson, 1994). Foremost amongst this is the extent that these provoke cognitive dissonance. Cognitive dissonance emerges along two different axes. On the one hand, the employed schema may not represent the information environment and is not ecologically rational[12] (Gigerenzer, 2008). As such, attempts to interpret (i.e., provide context) results in inappropriate choices leading to policy failure that could be treated as external shocks. Faced with this divergence between reality and existing mental models, policymakers may be prompted to abandon a schema or restructure it (Welch, 2011).

On the other hand, underlying motivations may similarly bring about cognitive dissonance. Motivational goals regulate how schemas are employed to interpret available information. These manifest themselves in two distinct forms, accuracy goals that encourage the objective assessment of information and direction goals focused on maintaining prior beliefs (Ford & Kruglanski, 1995; Taber, Lodge, & Glathar, 2001). Although uncertainty often leads to the spontaneous emergence of directional goals given the limitations of human cognition, accuracy goals may still appear when individuals are motivated to engage in more deliberate and effortful analysis of the available information (Kruglanski & Webster, 1996; Taber et al., 2001). The latter may occur when policymakers desire to either avoid negative consequences of poor or inappropriate policy choices (Kruglanski & Webster, 1996) or experience significant dissonance to cause a change in their underlying beliefs (Welch, 2011).

The extent to which policymakers adopt directional or accuracy goals during critical junctions partially determines the persistence of a hegemonic strategic culture. If the former prevails, policymakers may maintain the existing schema representing the hegemonic sub-culture. However, alternative schemas may enjoy enough support resulting in challenges if the latter proves more pronounced. These arguments are built on Bloomfield's (2012) approach by identifying the conditions in which individuals are likely to abandon a schema, thus providing

[11] As per Capoccia and Kelemen (2007, p. 343), these are situations "*in which the structural (that is, economic, cultural, ideological, organizational) influences on political action are significantly relaxed for a relatively short period, with two main consequences: the range of plausible choices open to powerful political actors expands substantially and the consequences of their decisions for the outcome of interest are potentially much more momentous.*"

[12] Pertains to the situation in which schemas or other cognitive devices are constructed in such a way that these accurately depict aspects of the real world (Gigerenzer, 2008).

the opportunity for another to gain hegemony. Furthermore, adopting a new schema necessitates a discursive process to externalize a new mental state in keeping with Libel's (2020) discursive institutionalist approach to changes in strategic culture and the process by which Meibauer (2020) conceives that ideas are transformed into externalized beliefs.

Completing the Causal Chain

The discussion surfaces the challenges of utilizing strategic culture as an ideational variable to link environmental cues, preferences, and behavior. However, integrating perspectives across four generations of strategic culture scholarship with an eye towards analytical pluralism yields a falsifiable framework to test the strengths and weaknesses of other theories such as structural realism. In doing so, the fundamental critiques against strategic culture need to be revisited in consolidating the arguments. First, (1) early conceptualizations are prone to being both over- and under-determined. Tangential to this, (2) the debates involving first and third generation scholarship ignored the concept of agency. To an extent, both camps assumed their existence as a given. Lastly, (3) the mechanism and variables responsible for changes in strategic culture were all but ignored until recently.

As shown in the debate between Johnston and Gray and further emphasized by positivists scholars in this field, the question of over-determination is routinely addressed by narrowing the definition of what constitutes strategic culture. While definitions tend to broaden or narrow depending on the subject under scrutiny, these are characterized by the distinct separation of strategic preferences and behavior. This clarifies what strategic culture is and avoids the tautology that plagues earlier conceptualizations. Furthermore, this establishes the necessary framework for theoretical comparison to test the relationship between causes (i.e., structural variables), mediators (i.e., strategic culture), and effects (i.e., strategic preferences). Epistemological differences aside, however, the literature treats strategic culture as providing context and meaning to material reality. Whether termed as *context all the way down* (Poore, 2003) or *ideas all the way down* (Johnston, 1999), it serves as a lens through which policymakers view the world and formulate behavior-shaping preferences.

Conceptualized as such and borrowing from cognitive and social psychology, strategic culture is operationalized as a cognitive schema that provides a structured and simplified understanding of the strategic environment. Initially residing within an individual, schemas develop either through first-hand experience or through socialization within a community

(Crocker et al., 1984; Harris, 1994; Kalyuga, 2010; Lau et al., 2003). This schema, however, is not the sole means with which policymakers interpret the environment. Given informationally optimal conditions or accuracy goals, policymakers are expected to objectively evaluate available information in keeping with the normative expectations of rational choice. When faced with uncertainty, however, heuristic devices (e.g., schemas) are employed to minimize cognitive load and to reach closure faster. These cognitive processes determine the utilization of strategic culture as a schematic device and establish the necessary scope conditions that address the issue of under-determination.

Policymaking, however, is not an individuated process, even within the most autocratic of regimes. Consequently, these internal mindsets are expressed externally through a discursive process. The degree of intersubjectivity among policymakers and institutions determines which schema becomes the hegemonic strategic culture. This emphasizes the agency necessary to create and maintain strategic culture beyond the individual policymaker(s).

Lastly, the hegemonic strategic culture changes following exogenous external shocks (e.g., policy failure) or an endogenous discursive process. The former is shared across the different generations of scholarship thus far. These events provoke cognitive dissonance amongst policymakers that, if severe enough, result in the abandonment of a schema. Relatedly, other policymakers who possess divergent schemas may view this situation as an opportunity to advocate for their beliefs, bringing about contestation (Bloomfield, 2012; Libel, 2020). Either way, these ideas would again need to be externalized through discourse, resulting in either the continuity or replacement of the hegemonic strategic culture.

IDEATIONAL FRAMEWORKS AND CYBER CONFLICT

The chapter began with a discussion of whether the cyber conflict literature recognizes that strategic preferences towards this domain are an objective response to the structural and technological pressures faced by policymakers. A brief overview of the empirical evidence, however, suggests otherwise. As with conflict in the conventional space, preferences that manifest as observable behavior do not consistently align with the realities faced by states. Consequently, the chapter discusses the variables that appear to mediate the influence of material reality. In surfacing the role of ideational variables in this causal process, the chapter identifies strategic culture as a lens through which policymakers interpret their environment. Despite drawing from various disciplines, ideational approaches are not foreign to political

science or international relations scholarship. Keeping this in mind, it is necessary to inquire whether the cyber conflict literature utilizes ideational variables to explain preferences and behavior in cyberspace.

The State of the Field

Contemporary cyber conflict scholarship is best described as being constructed around *logics of the domain* such that preferences appear to be determined by conceptualizations of what is (and is not) possible through cyberspace. While scholars note the importance of the strategic environment that feeds into the calculus of policymakers (Liff, 2012; Maness & Valeriano, 2016), there is little said regarding the mechanism linking cause and effect; drawing parallels with the limitations of structural realism as noted by Rathbun (2008). To explain this situation, some invoke strategic competition to rationalize the choices made by policymakers concerning the exercise of power in and through cyberspace (Fischerkeller & Harknett, 2020; Harknett & Smeets, 2020; Warner, 2020).

Framing cyber conflict as an extension of strategic competition in the real-world necessitates the assumption that preferences in this domain are governed by the structural and technological realities faced by states (Forsyth & Pope, 2014; Maness & Valeriano, 2016). Proponents assert that cyberspace, as an enabler of conventional levers of power (Kuehl, 2009), offers the opportunity to shift the balance of power in their favor (Liff, 2012; Saltzman, 2013). Depicted this way, cyber conflict as a manifestation of strategic competition draws heavily from structural realism such that states ought to adopt preferences (i.e., strategies) that ensure their security in this environment. To use the phrase advanced by Fischerkeller and Harknett (2020), this leads to a *cyber fait accompli.* A superficial reading would lead one to believe that this reaffirms earlier narratives of unrestricted cyber conflict (Forsyth & Pope, 2014; Saltzman, 2013). However, advocates explain that stability ensues due to tacit bargaining and agreed competition. To quote Fischerkeller and Harknett (2019, p. 273), *"U.S. adversaries have, through their behaviors, tacitly established an agreed competition in cyberspace, bounded by the operational space inclusive of and above operational restraint (i.e., inactivity) and exclusive of and below operations generating armed-attack equivalent effects."* Phrased succinctly, frequent adversarial interactions establish the limits of acceptable behavior that minimize the risk of escalation. This perspective is not unique as others (Gomez, 2018; Lindsay

& Gartzke, 2014) argue that these interactions encourage the emergence of tacit behavioral norms in cyberspace. However, gaps in the causal logic appear upon closer inspection.

To begin with, no explanation is offered as to why states ought to fear other states that operate in cyberspace aside from the perceived risk of exploitation (Fischerkeller & Harknett, 2020; Forsyth & Pope, 2014; Schneider, 2019). This point is crucial given the limited number of states involved in cyber conflict (Valeriano & Maness, 2014). Granted that there tends to be renewed interest in cyber capabilities following major incidents (Dunn Cavelty, 2012), not all states adopt a distinctly offensive approach in terms of their strategies (UNIDIR, 2013). While this is partly explained by resource constraints (Pytlak & Mitchell, 2016; Slayton, 2017), capable states that opt for a more pacific strategy need to be accounted for. Besides assumptions of (malicious) strategic intent, this perspective takes other liberties concerning the communicative clarity of cyber operations.

The above quote suggests that agreed competition is contingent on the fluency of actors in interpreting the meaning behind a particular operation or campaign. This is tantamount to a leap of faith given the difficulty of discerning intent from malicious behavior in cyberspace (Buchanan, 2017; Gartzke & Lindsay, 2017). Furthermore, there is little said regarding the importance of experience (Brantly, 2021) in moderating the interpretability of intent. As Healey (2019) suggests, inexperienced state actors may be unable to distinguish between actions that perpetuate the status quo or are genuine attempts to escalate.

Finally, depicting cyber conflict as strategic competition is derived from the US experience in cyberspace. While advocates do not necessarily stress this fact, neither do they temper their theoretical expectations around this constraint. Consequently, this raises questions of whether a similar phenomenon exists in other interstate configurations. Although the empirical evidence demonstrates that the balance of incidents often involves the United States (Valeriano & Maness, 2014), trends in capability development such as the militarization of cyberspace (Blessing, 2021; UNIDIR, 2013) merits consideration. Stepping back from these critiques, it becomes apparent that this framework rests on an assumption of rationality among policymakers when perceiving threats to and from cyberspace. Furthermore, there is a latent belief in the generalizability of these arguments without added efforts to determine whether the enabling conditions are present in other cases (i.e., non-US).

The Limits of Rationalist Frameworks

A handful of cyber conflict scholars adopt a rationalist approach when studying this phenomenon (Smeets & Work, 2020). While this provides a parsimonious account of cyber conflict, it runs the risk of deviating too far from reality such that it is of limited value when analyzing real-world interactions. Despite this constraint, rationalist models provide initial insight that directs later research efforts.

Building on the argument that cyber conflict reflects strategic competition; a rationalist perspective should first address the conditions in which an aggressor would choose to act. Axelrod and Iliev (2014) are first to tackle this question when they propose that the timing of cyber conflict is a function of the (1) stakes involved, (2) the characteristics (i.e., persistence and stealth) of cyber capabilities, and the (3) value of these capabilities. The authors note that the distribution of stakes varies based on the context in which cyber operations are employed. The stakes for criminal endeavors, for instance, remain constant such that the optimum decision is to use these when and where available. In contrast, stakes in international affairs are heavily skewed towards rarer events. Consequently, the optimum condition necessitates exercising capabilities during high-stakes situations when these are less stealthy but persistent. While the argument is sound, this is predicated on a few conditions.

To start with, recognizing the optimum condition is contingent on the ability of policymakers to interpret the strategic environment to determine the stakes involved accurately. Although this assumption is necessary for simplicity, there is no shortage of research pointing to the risk of misperception (Gomez, 2019b; Jervis, 1976; Schneider, 2017). Failing to consider this, policymakers may choose to engage in conflict at a sub-optimal point in time. The second condition revolves around assumptions surrounding cyber capabilities. The authors are not alone in emphasizing the importance of technical characteristics. Brantly (2016) asserts that the initiation of cyber conflict is inversely correlated with the attributability of the operation, such that the ability to avoid attribution encourages risk acceptant behavior.

While there is an argument to be made regarding the tactical benefits derived from the characteristics of cyber operations, their strategic value remains in doubt. Contrary to earlier assertions of the utility afforded by a single large-scale operation, Harknett and Smeets (2020) posit that ostentatious displays of capability may be less relevant than sustained cyber campaigns. Consequently, repeated contact over time through less complex operations may meet the desired objectives. This, however, runs the risk of nullifying the technical advantages

afforded by cyber operations. Repeated interactions establish patterns of behavior that reduce uncertainty through the accumulation of tactical, operational, and strategic evidence (Rid & Buchanan, 2015). Consequently, this allows defenders to identify both intent and capabilities of potential adversaries. While the former decreases the likelihood of misperception, the latter could prompt greater circumspection among aggressors when choosing to engage in an operation. Although this may lead to greater stability, it may also prompt the use of specific capabilities sparingly such that, to other observers, these appear more advanced and may be misperceived as an attempt to shift the status quo (Buchanan, 2017; Gartzke & Lindsay, 2017). While this may result in agreed competition and stability, this is contingent on the ability of both parties (i.e., attacker and target) to interpret each other's actions and intent accurately.

Edwards et al. (2017) attempt to address these concerns when they propose a two-player model to determine the conditions in which an aggressor initiates conflict and when targets respond. Briefly, an aggressor is not expected to initiate hostilities if it knows itself to be vulnerable and if the (potential) costs outweigh gains. Vulnerability pertains to the situation(s) in which an (1) aggressor is subject to a retaliatory cyber operation or (2) that the aggressor is in a tenuous geopolitical position wherein attribution can have significant strategic consequences. This conceptualization of vulnerability also considers the defender's knowledge. Consequently, aggressors are further restrained if they are concerned that the target is aware of their vulnerability. However, even when vulnerable, aggressors may initiate conflict if the (potential) gains outweigh costs or when they believe that the target is incapable or unwilling to respond. Although this model better captures the dynamics of cyber conflict, it fails to address the perceptual constraints faced by both the aggressor and target. Specifically, it complicates the situation by assuming the ability of both aggressors and targets to accurately evaluate the other's vulnerability and the corresponding effects of cyber operations (Dunn Cavelty, 2013; Hansen & Nissenbaum, 2009; Kaminska, 2021; Perrow, 1984).

Complexity, a pronounced challenge for conventional interstate relations, is compounded further by the unique attributes of cyberspace (Brantly, 2021). Keeping in mind the latent uncertainty of cyberspace and the shortage of (cyber) expertise within the policymaking community (Hansen & Nissenbaum, 2009), the parametric expectations of these models are unlikely to be met. This reinforces Brantly's (2021) argument that, at best, interpretations of the strategic environment (including cyberspace) are bounded by either a priori assumptions derived from experience or the temporal or resource constraints that moderate the search for new information. Consequently, one can expect rationality vis-à-vis

cyber conflict to exist in varying degrees across policymakers. Moreover, and relevant to the framework adopted by this dissertation, the boundaries that frame decisions leave interpretative space for policymakers to discern the meaning behind these cybersecurity incidents (Morgenstern & von Neumann, 1953).

Nascent Ideational Cyber Conflict Research

Having established the limits of rational thought during periods of cyber conflict, it would not be unjustified to claim that the environment's uncertainty encourages the use of ideational variables as contextual aids. Over the last decade, cyber conflict scholars have shown a growing interest in ideational frameworks as a means of explaining preferences and behavior. These efforts, however, remain disjointed in terms of the relevant actors involved (i.e., elite versus non-elites) and the ideational constructs presumed to be at work (e.g., beliefs, enemy images, culture, etc.).

Given the dissertation's explicit interest in security policy, elite preferences towards cyberspace are an ideal starting point. Unsurprisingly, this area of research is challenging given the difficulties associated with access to the relevant subjects and artifacts (Lin-Greenberg, Pauly, & Schneider, 2021; McDermott, 2002). Consequently, contemporary research in this area may be categorized based on the source of empirical evidence. On the one hand, observational studies are constructed using publicly available policy documents and observed state behavior that demonstrate the theorized link between causes (e.g., techno-structural constraints) and effects (e.g., specific policy preferences). On the other hand, experimental or pseudo-experimental studies employ elites or appropriate proxies to study the underlying causal mechanisms. Readers should note that neither one should be seen as objectively better than the other.

An ideal representative of observational studies is work done by Valeriano, Jensen, and Maness (2018). In their book, *Cyber Strategy: The Evolving Character of Power and Coercion*, the authors utilize a dataset of publicly disclosed cybersecurity incidents from 2000 to 2017 involving rival states. When analyzing the behavior of actors such as the United States, China, and Russia, the authors note that the preferences adopted in response to cyber conflict correspond with those established prior to the advent of cyberspace. The current Russian orientation towards influence operations corresponds with preferences during the Soviet era, if not earlier. Relatedly, cyber espionage operations that have typified Chinese cyber operations

appear to be associated with the desire to exploit information asymmetries and reflect classical Chinese strategic thought. While the authors do not explicitly attribute these observations to a single ideational variable, their discussions implicitly suggest the role of strategic culture in defining national modes of cyber conflict.

To an extent, this gap is addressed by scholarship from Kari and Pynnöniemi (2019) and Kaminska (2021). The former explicitly references the role of strategic culture concerning Russian threat perception towards cyberspace. Utilizing Russian policy documents, the authors (2019, p. 24) identify narratives that represent Russian strategic culture, such as *"a sense of vulnerability, the narrative of Russia as a besieged fortress, the mythology of permanent war, and technological inferiority."* Employing document analysis, Kari and Pynnöniemi (2019) demonstrate how Russian policymakers contextualize the strategic environment using these narratives. However, the study is limited, focusing on a single case[13] (i.e., limited generalizability). Furthermore, it does not consider whether references to these narratives are employed instrumentally such that policymakers obtain the necessary legitimacy that allows them to pursue actions that may not reflect the underlying strategic culture. Moreover, there is no mention of the conditions that may lead to changes in preferences.

While Kaminska (2021) does not explicitly cite strategic culture as influencing the observed restraint of US cyber operations, she links the uncertainty associated with cyberspace to the risk-avoidant tendencies of US society. Specifically, she argues that the characterization of cyberspace as a complex adaptive system[14] and the ease with which cyber capabilities proliferate increases uncertainty. Responding to this, policymakers adopt the *dominant risk management paradigm* that provides the necessary context for their cybersecurity preferences. Moreover, she bases her argument on the notion that risk is influenced by the politics and culture within a given state (Beck, Giddens, & Lash, 1994), implicitly referencing established beliefs as the foundation for interpreting the environment. Unfortunately, this study also suffers from issues of generalizability and does not address changes in preferences.

Although limitations that stem from single case studies may be a necessary compromise for achieving analytical depth, the issue of excessive continuity (i.e., unchanging preferences) expressed in these studies may be easier to address. While Brantly (2021) does not explicitly

[13] Not unusual for research involving strategic culture.
[14] This characterizes cyberspace as a system that creates new knowledge with innate causal properties that result in the adaptive behavior of the system. Consequently, the system is deemed chaotic as it can behave in a manner that was not intended or expected by its designers (Kaminska, 2021).

tackle culturally rooted preferences, he notes the possibility of states adapting their preferences to correspond with lessons from previous interactions. This process finds parallels with third generation strategic culture scholarship that investigates how recent military developments and setbacks encourage a pronounced shift in world view and preferences (Johnston, 1995; Katzenstein, 1996; Legro, 1995).

Moving forward, these examples of observational research demonstrate the influence of ideational variables such as culture on contextualizing the environmental cues received by policymakers. These studies, however, are limited in their ability to unpack the underlying causal mechanism. While the analysis conducted by Kari and Pynnöniemi (2019) comes closest to achieving this, it is difficult to investigate the cognitive processes at work without access to the policymakers themselves or relevant decision-making artifacts. Consequently, cyber conflict scholars are turning to experimental and pseudo-experimental methods as this allows for isolating variables relevant to the phenomenon while minimizing the impact of confounders (McDermott, 2002; Schechter et al., 2021).

This form of scholarship is best represented in wargaming work done by Jacquelyn Schneider and her colleagues (Schechter et al., 2021; Schneider, 2017). Specifically, her analysis of wargames conducted over six years at the United States Naval War College surfaces the tendency of policy and military elites to utilize established beliefs when evaluating risks. Furthermore, these beliefs are projected onto adversaries as a means of coping with uncertainty. This process, and most importantly its discursive aspect, is surfaced when in-game behavior, debriefing responses, and non-participatory observations are analyzed in conjunction with one another. Unfortunately, while the methodology provides the opportunity to unpack the causal mechanism at work, demographic limitations (i.e., only US nationals) do not permit comparative analysis and limits generalizability.

In response, recent work by Gomez and Whyte (2020b) overcomes this limitation by conducting a series of cross-national wargames involving participants from the United States, Europe, and Asia. Conceived as a means of studying escalatory risk in the wake of a cybered conflict[15], participants play the role of policymakers in a fictitious state facing conflict with its near-peer neighbor. Despite attempts to control external influences, the study consistently finds participants resorting to beliefs and preferences associated with their respective states (i.e., strategic culture). During debriefing, participants note that their tendency to turn towards

[15] The scenario presented involves events and issues across multiple domains – one of which is cyberspace.

established beliefs and preferences is encouraged by the pronounced uncertainty within the scenario. Consequently, the ongoing study highlights the heuristic value of these ideational variables.

The preceding examples demonstrate interest among cyber conflict scholars to utilize ideational variables to explain state policy and behavior. Specifically, the emergence of distinct national modes of cyber conflict points to the possible instrumentalization of strategic culture as a lens through which structural and technical realities are interpreted and acted upon. However, the cyber conflict literature still lacks a clear theoretical framework to establish the conditions in which these ideational variables manifest causal effects. Relatedly, methodological constraints need to be considered further to account for the challenges involved when studying the influence of immaterial constructs such as strategic culture.

OVERCOMING UNCERTAINTY IN CYBERSPACE

Miguel Alberto Gomez

University of Hildesheim
Center for Security Studies, ETH

ABSTRACT

An understanding of strategic behavior in cyberspace is often premised on the uncertainty inherent in the domain. However, little is said regarding the exact nature of this uncertainty and the underlying motivations that direct attempts at overcoming it. In response, this article advances a cognitive-cultural explanation of strategic behavior in cyberspace and argues that behavioral preferences arise from the schematic use of strategic culture as a remedy for uncertainty. However, the suitability of these preferences is moderated by the presence of accuracy goals. These accuracy goals must, in turn, dictate the extent to which these are deemed suitable. While two decades of cybersecurity research hints at the presence and significance of these mechanisms, little effort has gone into advancing this line of inquiry. Consequently, the article consolidates these findings into a robust analytical framework to explain strategic behavior in cyberspace.

UNPACKING STRATEGIC BEHAVIOR IN CYBERSPACE

Miguel Alberto Gomez

University of Hildesheim
Center for Security Studies, ETH

Christopher Whyte
Virginia Commonwealth University

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.

TRACING STRATEGIC PREFERENCES IN CYBERSPACE

Miguel Alberto Gomez

University of Hildesheim
Center for Security Studies, ETH

ABSTRACT

Our understanding of strategic preferences in cyberspace rests on the material and strategic factors that shape state behavior. This, however, is derived from the actions of established cyber powers. Given the material resources required to effectively operate in this environment and repeated interactions that form the boundaries of accepted behavior, the literature does not adequately explain the emergence of strategic preferences among novice actors. The article posits that these are not exclusively the function of either the material or strategic factors. Instead, strategic culture features prominently in the selection of strategic preferences that shape state behavior in cyberspace.

CONCLUSION

REEVALUATING STRATEGIC PREFERENCES

Are strategic preferences towards cyber conflict a response to techno-structural realities faced by states? While the literature continues to distance itself from technologically deterministic accounts of policymaking, most recently by associating cyber conflict with strategic competition (Fischerkeller & Harknett, 2020), the reality is more nuanced. In acknowledging the pervasive uncertainty characterizing cyberspace, the dissertation observes the tendency for the *"systemic slippage between policy-guiding mental representations of reality and reality itself"* (Goldgeier & Tetlock, 2001, p. 72) among policymakers. While not suggesting the irrationality of these individuals, this emphasizes the boundedness of human cognition that, for better or for worse, shapes preferences.

The dissertation proposes that preferences stem from contextualizing structural and technological cues through the lens of strategic culture. Faced with an uncertain environment further compounded by the continued shortage of expertise, strategic culture is employed as a cognitive schema externalized through a discursive process, as demonstrated by the cross-national wargames and the case study respectively. The former emphasizes the ambiguity surrounding issues of attribution and intent and its resolution through the heuristic use of established preferences. Relatedly, the latter notes that policies surrounding the employment of emergent technologies vis-à-vis national security are informed by the dynamics between domestic and regional strategic culture.

While these observations reveal the analytical utility of strategic culture, its operationalization as a cognitive schema serves to address persistent critiques of it being simultaneously over- and under-determined. As a schematic device, strategic culture is employed in instances wherein objectivity (i.e., strict adherence to the expectations of the rational choice model) is either impossible or undesirable[1]. Consequently, rationality is bounded by *"a priori assumptions based on experience"* (Brantly, 2021, p. 2). For instance, Singaporean participants in the wargame asserted the need to demonstrate resolve while maintaining diplomatic options. Relatedly, Philippine-based participants note the importance of projecting strength notwithstanding material imbalances to discourage aggression resulting from persistent vulnerability. For both sets of participants, adversarial identity and intent were ambiguous and led to the adoption of cultural preferences that proved successful in the past.

[1] There is either not enough information or time to do so.

This was not a given, however, and schematic thinking was tempered if the motivation to do so existed. Specifically, participants exhibited more objectivity if policy failure risked significant national, organizational, or personal costs. These observations establish the scope conditions that determine the schematic use of strategic culture and addresses the persistent critiques leveled against it.

Relatedly, the dissertation tackles the issue of sub-cultures and excessive continuity, the assumption of a single dominant and enduring strategic culture. Although contemporary strategic culture scholarship addresses these concerns, these efforts are aimed at policies applied to conventional domains (i.e., land, sea, air, and space). However, if cyber conflict is an extension of strategic competition in these areas, would existing preferences perpetuate into this domain? This is a salient point given the unique characteristics of cyberspace and the plurality of actors and perspectives (Burton & Claire, 2020; Hansen & Nissenbaum, 2009). Nevertheless, the evidence presented in the empirical chapters tackle these concerns.

While rarely explicit, respondents in the case study recognized the presence of established and possibly competing preferences amongst organizations responsible for overseeing Philippine cybersecurity with respect to national security. The unique dynamic at the domestic level where contestation involving the military and civilian sectors that carry distinct preferences results in the emergence of policies that are further shaped by regional preferences. As exhibited in the wargame, this contestation is even more pronounced when Philippine-based participants express distinct perspectives associated with their assigned roles (i.e., as the secretary of defense, foreign affairs, or information technology). Furthermore, the wargame also surfaced beliefs exogenous to the participants' assigned role that informed their preferences during gameplay. Collectively, this finds that structural and technological cues are interpreted through different sub-cultural lenses, reflecting the plurality of competing sub-cultures.

These observations confirm the propositions that constitute the proposed ideational framework. First, *policymakers employ strategic culture as a meaning-making tool from which preferences are derived in pursuit of security*. Echoing Gray's (1999) argument, strategic culture provides the necessary context that makes certain actions possible. Strategic culture, however, is not assumed to be a given, nor is it monolithic. While *policymakers exhibit shared preferences when socialized into a common strategic culture*, this presupposes that *policymakers belonging to different epistemic communities may hold distinct preferences, though the possibility of shared preferences exist.* This emphasizes the possibility of sub-

cultures competing for hegemony and further underscores the evolution of strategic culture in response to external shocks or discursive contestation. Finally, dependence on this contextual lens is not a foregone conclusion, and objective interpretation of the environment remains possible. This occurs when *accuracy goals limit the range of preferences derived from strategic culture by encouraging the objective evaluation of technological and structural cues*. Consequently, the dissertation contributes to cyber conflict scholarship by demonstrating the value of employing strategic culture as an analytical device in explaining preferences towards cyber conflict.

IMPLICATIONS FOR THEORY

The dissertation finds itself part of the growing behavioral turn in cyber conflict scholarship that emerged over the last five years. Acknowledging that earlier scholarship recognizes the influence of technological and structural variables over preferences, behavioralists complement this by stressing the importance of individual-level variables in policy construction and adoption. While not dismissing the value of factors such as cyber capabilities and the balance of power, these scholars assert that cyber conflict cannot be understood independently of the individual and communities that exist within and through it. To that end, behavioralist scholarship applied to cyber conflict is categorized into two groups based on the mechanism that links perception, preferences, and behavior in cyberspace.

Some scholars adopt a cognitive approach. Recognizing that cyberspace is an inherently uncertain domain, scholarship in this group points to the use of heuristics as a perceptual device that informs policy choices. For example, research from Gomez (2019a, 2019c), Brantly (2021), and Kostyuk and Wayne (2021) note the use of the availability and representativeness heuristics to complement limited domain expertise. Relatedly, Schneider (2017) observes mirror imaging among policy and military elites when evaluating adversarial responses to cyber operations against them. Finally, scholars (Kari & Pynnöniemi, 2019; Valeriano et al., 2018) point to beliefs that pre-date cyberspace as shaping threat perception and strategic preferences.

Complementing these findings, others note the influence of affect (i.e., emotions) on the formation of preferences. Starting with the seminal work conducted by Gross, Canetti, and Vashdi (2017), cybersecurity incidents appear to elicit affective responses comparable to conventional threats. Consequently, individuals, and the public specifically, are found to

manifest feelings of anger and dread that modulate support for specific policy options such as retaliation. For instance, Shandler et al. (2021) find that pronounced levels of anger lead to calls for retaliation following a severe cybersecurity incident. Although subsequent (Shandler, Gross, & Canetti, 2021) and related (Kreps & Schneider, 2019) research observe that domain expertise generates a moderating effect, the consequences for policy remain substantial. Furthermore, noting that emotions precede cognition (Gray, 1990), the relevance of both cognitive and affective perspectives becomes apparent.

Nevertheless, despite these contributions, scholarship focused on cognitive and affective mechanisms independent of each other is limited owing to their focus on individual perceptions and preferences. While providing crucial insight, these have yet to explain how individuated processes feed into social phenomena such as policy construction in the context of cyber conflict. About this gap, the dissertation offers some initial inroads.

While the framework recognizes the utility of employing strategic culture as a cognitive schema, it asserts that this individuated construct needs to be manifested externally to exert an observable effect on policy. Specifically, it notes that policymakers belonging to different communities may reflect schemas distinct from one another. When advocating for specific preferences during policy deliberation, this may result in discursive contestation wherein a particular viewpoint increases in prominence and becomes the hegemonic strategic culture – at least until it is challenged. The dissertation proposes and tests a mechanism with which a cognitive construct, possibly unique to a subset of individuals, is externalized such that it exerts a causal effect on policy preferences.

However, this is not to say that other studies assume that policymaking is attributable to a single policymaker. Instead, the cyber conflict literature does not explicitly tackle how individual cognitive and affective states feed into policy construction. For instance, in the case of research done by Shandler et al. (2021), the mechanism linking a preference for retaliation and individual affective states (i.e., audience cost) is apparent but left unexplored. In contrast, the dissertation recognizes the social dimension of this process when acknowledging the possible competition between different groups advocating for their respective preferences. However, readers should note that this leaves several theoretical aspects of preference formation unresolved.

To start with, the dissertation does not explicitly tackle the origins of individual sub-cultures. While addressing this question necessitates expanding its scope at the cost of reduced rigor and consistency[2], future research endeavors should consider moving in this direction. There exists the possibility that individuals belonging to communities not traditionally associated with issues of national security may hold divergent preferences from those of their counterparts in established institutions (e.g., foreign and defense ministries) (Burton & Claire, 2020; Dunn Cavelty, 2013; Tanczer, Brass, & Carr, 2018). This is not unlikely for smaller states with the establishment of cybersecurity organizations independent of existing government agencies (Oppenheimer, 2021). With the plurality of individuals and organizations involved in the construction of cybersecurity policy, the effect that this may have on the discursive processes that result in the adoption of policies needs to be considered.

Apart from the inclusion of voices outside the established policy community, the role of affect needs to be considered further in the context of policymakers. The framework employed by the dissertation does not provide the necessary analytical leverage to determine the influence of affect on preferences. As such, it could not be convincingly argued that policymakers adopt preferences sans an affective mechanism. Scholars (Gray, 1990; Taber & Lodge, 2006), however, demonstrate that affect cannot be divorced from cognitive processes. Given the emotional salience of cyber conflict amongst the public (Gross et al., 2017; Kreps & Schneider, 2019), it is inappropriate to argue that policymakers are not subject to comparable processes (Kertzer, 2020). Consequently, this raises the question of whether emotions serve to further moderate the range of preferences deemed appropriate by policymakers. Interviews involving both wargame participants and policy elites suggest the presence of both anger and anxiety when responding to a cybersecurity incident or developing a cybersecurity policy. While the current methodology prevents further unpacking the role of these emotions, their presence viewed in the context of the available literature suggests a possible interaction with existing schemas in making certain preferences more or less palatable for policymakers.

IMPLICATIONS FOR METHODOLOGY

Apart from its theoretical orientation, the dissertation also reflects the growing adoption of experimental and pseudo-experimental methodologies in cyber conflict research. Despite

[2] Investigating the development of strategic culture in a particular state necessitates further sociological and historical research which is outside the scope of this dissertation.

divergent views among cyber conflict scholars on how best to approach the phenomenon, there is common ground regarding the scarcity of data and its impact on theory development and testing. The opaque nature of cyber conflict and the bias in reporting incidents constrains observational studies. Although large-N observational studies allow for the generalization of findings, the potential for selection bias in these datasets needs to be acknowledged. In response, cyber conflict scholars are turning to other methodologies to overcome issues of quantity and quality of data.

Seen as the gold standard for scientific research, experiments enable the isolation of suspected causes to test for their presumed effects while limiting the influence of confounding variables (Aldrich & Lupia, 2011; Falk & Heckman, 2009). Coupled with innovative designs such as including open-ended questions (Roberts et al., 2014), researchers can employ experiments to surface mechanisms that link both cause and effect. Consequently, it is increasingly common to find cyber conflict research that utilizes fictitious scenarios to mirror real-world incidents and readily accessible Internet-based participants to study preferences vis-à-vis cyber conflict. This, however, is not without its pitfalls and is limited by the artificiality of scenarios and an overreliance on non-elite samples to study elite behavior.

Experimental designs need to balance experimental and mundane realism when considering their intended purpose. The former pertains to aspects of the experimental treatment meant to evoke the outcome under investigation. The latter, in contrast, refers to the degree to which the experiment and its treatment(s) correspond with the real world. Experimental cyber conflict research often errs on the side of the former (Gomez, 2019a, 2019c; Kostyuk & Wayne, 2021). This, unfortunately, comes at the cost of oversimplifying a complex phenomenon**,** leading to questions of external validity (McDermott, 2004).

Tangential to this issue is the appropriateness of employing non-elite participants (e.g., crowdsourced Internet participants or undergraduate students) as proxies when studying elite behavior. The focal point of this criticism is that these participants may lack the requisite knowledge and experience possessed by policymakers. While this may indeed be the case, the suitability of using non-elites remains the function of the underlying research goals. If the objective is the study of variables and processes that are fundamental human tendencies (e.g., reliance on heuristics), then the sample used is less of an issue. However, suppose the phenomenon in question is predicated on traits endogenous to a given role or experience. In that case, using non-elites may raise internal and external validity questions (Mintz et al., 2006).

Responding to these challenges, Schneider and others (Lin-Greenberg et al., 2021; Schechter et al., 2021; Valeriano & Jensen, 2021) proposed the adoption of strategic simulations (e.g., wargames) to address the limitations of conventional experimental designs. Utilizing complex and (possibly) multi-round scenarios, a balance between experimental and mundane realism is struck. Additionally, triangulation across multiple data sources (e.g., in-game response, non-participatory observations, debriefing) allows researchers to analyze relevant mechanisms and identify possible confounding variables. However, the use of simulations does not eliminate concerns surrounding participant identity such that research oriented around elite behavior still requires these individuals or suitable proxies. Furthermore, a distinction is necessary between experimental and observational variants of this approach. Studies oriented towards the former are expected to subscribe to the requirements of conventional experimental research and aim for achieving internal validity. The latter, in contrast, is employed in instances wherein research is oriented towards surfacing process of a distinct subset of individuals. This allows scholars to work with a much smaller sample size while generating a more nuanced analysis than conventional large-N experiments. Nevertheless, Lin-Greenberg, Pauly, and Schneider (2021) caution that this comes at the cost of theoretical generalization. Consequently, scholars need to be more mindful of the goals that drive research.

In terms of its methodology, the dissertation finds itself in the company of scholars such as Schneider (2017) and Valeriano and Jensen (2021), that utilize simulations when studying cyber conflict. However, it distinguishes itself from these on two fundamental points. While Schneider conducted research involving elites over an extended period, these are demographically restricted, such that participation is limited to military and policy elites within the United States. Consequently, it is unclear whether the processes observed exist apart from US policymakers. While Valeriano and Jensen recruited participants across various nationalities, their analysis is limited to in-game responses. While this more closely resembles the experimental variant, the absence of additional data points makes it challenging to trace the causal mechanism that links cause and effect.

Recognizing these limitations, the dissertation adopts the middle route by conducting a cross-national study for comparison while simultaneously integrating multiple observation points. While this addresses the limitations mentioned above, modifications to the design are encouraged. One of which is to allow for free play between two teams. While having multiple rounds enables greater realism during gameplay, limiting interactions to the input of a single

team choosing from a fixed set of options constraints the possible dynamism one might expect to see in real-world crises. Although this limits control over confounders, there is enough analytical leverage given the availability of multiple data points to address this concern.

Besides in-game dynamics, the context in which teams operate can also be made to vary. As it stands, the fictitious scenario depicts the interactions between near-peer states. The balance of (conventional) power is kept constant to permit a more straightforward analysis. However, a stricter test to ascertain whether structural cues are interpreted through the lens of strategic culture necessitates introducing variance. Coupled with its proposed transformation into a two-team game, this would further its realism but at the cost of analytical parsimony. However, as mentioned previously and keeping in mind the objectives of this scholarly endeavor, this is a necessary compromise in the future.

IMPLICATIONS FOR POLICY

A cursory review of public declarations involving cyber conflict over the past twenty years reveals the continuing exceptionalism that typifies events in cyberspace. Given references to its potential to transform interstate relations by policymakers (Bumiller & Shanker, 2012; Clarke & Knake, 2014) and further reinforced by persistent media narratives (Jarvis et al., 2017), one cannot help but conclude that cyber capabilities are a distinct aspect of national power. To an extent, this is a valid point as cyberspace enables actions that would otherwise be difficult or impossible (Saltzman, 2013). However, while its unique characteristics allow for a degree of tactical freedom not seen before (Healey, 2016; Liff, 2012), it remains constrained by the strategic environment and perceptions that shape its interpretation.

As tersely summarized by Gray (2013, p. 52) when talking about cyber conflict, *"the sky is not falling."* His counsel to avoid alarmism given the rising tide of cyber conflict echoes the suspicion of several scholars (Iasiello, 2013; Lindsay & Gartzke, 2014; Maness & Valeriano, 2016; Rid, 2012) concerning the threat posed by state-associated cyber operations. Furthermore, while time may have proven the assumption that cyber operations are a limited means to alter the distribution of power between states, this does not imply that these are devoid of strategic value. In a recent article published in Foreign Affairs, Jacquelyn Schneider (2022, p. 31) proposes the analogy of a termite infestation that is *"hidden in the recesses of foundations, that gradually eat away at the very structures designed to support people's lives"*

to describe cyber conflict. While this depiction divorces itself from narratives involving the catastrophic effects of cyber operations, the tangible outcome of exercising power in and through cyberspace is no less troubling. Furthermore, depicting cyber conflict as a long-term process geared towards a particular goal indicates strategic considerations among policymakers (Harknett & Smeets, 2020).

Although early cyber conflict scholarship implies that the advent of cyberspace requires a new analytical framework, developments over the last decade see interstate interaction in cyberspace governed by established strategic expectations (Maness & Valeriano, 2016). Instead of introducing a revolution in interstate affairs, cyber operations and conflict are treated as another expression of established state preferences (Kaminska, 2021; Kari & Pynnöniemi, 2019; Valeriano et al., 2018). However, there continues to be a dearth of scholarly work focused on investigating the processes linking structural and technological cues with behavior-shaping preferences. Although there is no shortage of research focused on testing causal effects, unpacking the underlying mechanism is necessary not only for academic rigor but also for designing policy interventions as a means of correcting maladaptive practices.

Concerning the dissertation's findings, the schematic use of strategic culture to contextualize the strategic environment functions as a double-edged sword. This socio-cognitive mechanism reduces the time necessary to identify preferences that inform policy choices as a matter of expediency. This could be beneficial under periods of crisis as it allows policymakers to act efficiently. However, the suitability of heuristics-derived preferences is a function of their correspondence with the real world (Todd & Gigerenzer, 2012). Given that these preferences may have developed prior to the advent of cyberspace, the possibility of a perceptual mismatch exists, resulting in strategic failure (Meibauer, 2020).

Consequently, the dissertation surfaces the need for policymakers to carefully consider how they approach their interpretation of the strategic environment. Although the uncertainty that typifies interstate relations increases the likelihood of heuristic usage, this is not a foregone conclusion. Whether they be established or emergent state actors, processes should be introduced that encourage the accurate assessment of available information. While this statement should not be interrupted as a call for penalizing individuals, policymakers should be made aware of the possibility of bias. One means of doing so is introducing a review process following instances of policy failure (e.g., escalation of conflict). Individuals external to but familiar with the policymaking community should lead this review. Their role outside the policymaking community reduces the likelihood of possessing the same priors that may have

resulted in bias. This increases the chances of identifying the sources of bias and suggesting corrective measures.

Similarly, the use of ill-suited schemas may also be a function of limited domain expertise. This is an enduring problem even amongst established state actors (Legg, 2021). Furthermore, the empirical evidence presented throughout the dissertation cites this as a fundamental issue that challenges policymakers. Consequently, addressing this overdependence on heuristics may be achieved by developing domain expertise among policymakers or providing ready access to experts. While this may be easier said than done given the difficulty of recruiting and maintaining talent (Kollars & Moore, 2019), the available evidence suggests that familiarity with the capabilities and limitations of cyberspace encourages greater objectivity among those observing it. This emphasis on educating policymakers highlights the unique attributes of cyberspace and cyber conflict as a field of study.

ADVANCING CYBER CONFLICT SCHOLARSHIP

While there continues to be substantial scholarly interest in unpacking the phenomena of cyber conflict, its embeddedness in modern society ensures its sustained policy relevance and necessitates the continued cooperation between academia and the world of policy. This is especially pronounced in instances wherein expectations noticeably deviate from observed reality as in the case of the limited use of Russian cyber capabilities in the ongoing Ukraine – Russia war. Despite predictions among certain policy specialists and political leaders, the conflict between Ukraine and Russia does not appear to feature significant cyber components that can shift the dynamics of the conflict. While scholars (Lonergan, Lonergan, & Valeriano, 2022) note factors that range from the inherent limits of cyber operations to costs (e.g., material) necessary for inflicting significant physical effects; a handful of policymakers and specialists continue to hold on to the notion of the revolutionary potential of this human-made space (Menn & Timberg, 2022). Consequently, the risk of misperception leading to inappropriate policy choices remains a reality despite greater understanding within the academic community over the last two decades of the impact of cyber capabilities and conflict.

As such, scholarship focused on unpacking the decision-making processes involving not only cyberspace, but other emergent technologies that introduce a surplus of uncertainty is crucial. Specifically, it is important to determine whether these developments necessitate a

change in how we approach interstate relations and the degree to which these technologies are truly revolutionary or simply complement existing capabilities. If it is the former, then partnership between academia and the policy world stand to offer crucial insights that allows for the maximization of potential benefits. If the latter should be the case instead, careful study of how policymakers approach these developments offer the opportunity to avoid possible misperceptions and its unintended consequences.

Keeping this in mind, the dissertation advances useful theoretical and methodological tools to help understand policy construction with respect to emergent technologies such as cyberspace. Moreover, it contributes to the continuing maturity of cyber conflict scholarship by advancing an ideational framework to complement contemporary materialist explanations. And while it is by no means perfect, it provides scholars with a feasible roadmap for future inquiry by incorporating and emphasizing the importance of individuals in the decision-making process which, thus far, has been limited owing to the challenges of utilizing intangible constructs such as ideas as an analytical tool.

REFERENCES

Abdelal, R., Blyth, M., & Parsons, C. (Eds.). (2010). *Constructing the International Political Economy*. Ithaca: Cornell University Press.

Aldrich, J., & Lupia, A. (2011). Experiments and Game Theory's Value to Political Science. In J. Druckman, D. Green, J. Kuklinski, & A. Lupia (Eds.), *Cambridge Handbook of Experimental Political Science* (pp. 89-101). New York: Cambridge University Press.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141-165.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences, 111*(4), 1298-1303.

Bar-Joseph, U., & Kruglanski, A. (2003). Intelligence failure and need for cognitive closure: On the psychology of the Yom Kippur surprise. *Political Psychology, 24*(1), 75-99.

Barkin, J. (2003). Realist Constructivism. *International Studies Review, 5*(3), 325 - 342.

Bathurst, R. (1993). *Intelligence and The Mirror: On Creating an Enemy*. London: SAGE.

Beck, U., Giddens, A., & Lash, S. (1994). *Reflexive modernization: Politics, tradition and aesthetics in the modern social order*. Stanford: Stanford University Press.

Berman, S. (2001). Review: Ideas, Norms, and Culture in Political Analysis. *Comparative Politics, 33*(2), 231 - 250.

Berman, S. (2013). Ideational Theorizing in the Social Sciences since "Policy Paradigms, Social Learning, and the State". *Governance: An International Journal of Policy, Administration, and Institutions, 26*(2), 217-237.

Bieler, A., & Morton, A. (2008). The Deficits of Discourse in IPE: Turning Base Metal into Gold? *International Studies Quarterly, 52*(1), 103 - 128.

Bleiker, R., & Hutchison, E. (2008). Fear no more: emotions and world politics. *Review of International Studies, 34*, 115-135.

Blessing, J. (2021). *The Global Spread of Cyber Forces, 2000–2018*. Paper presented at the 13th International Conference on Cyber Conflict (CyCon).

Bloomfield, A. (2012). Time to Move On: Reconceptualizing the Strategic Culture Debate. *Contemporary Security Policy, 33*(3), 437-461.

Booth, K. (1979). *Strategy and Ethnocentrism*. New York: Holmes and Meier.

Borghard, E. (2019, 22.03.2019). What a U.S. Operation Against Russian Trolls Predicts About Escalation in Cyberspace. Retrieved from https://warontherocks.com/2019/03/what-a-u-s-operation-against-russian-trolls-predicts-about-escalation-in-cyberspace/

Borghard, E., & Lonergan, S. (2017). The Logic of Coercion in Cyberspace. *Security Studies, 26*(3), 452-481.

Boulding, K. (1959). National images and international systems. *Journal of Conflict Resolution, 3*(2), 120-131.

Brantly, A. (2016). *The decision to attack: military and intelligence cyber decision-making*. Athens, GA: The University of Georgia Press.

Brantly, A. (2020). Entanglement in Cyberspace: Minding the Deterrence Gap. *Democracy and Security*, 1 - 24.

Brantly, A. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity, 7*(1).

Brown, J., & Fazal, T. (2021). #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security*, 1-17.

Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. London: Hurst & Company.

Buchanan, B. (2020). *The Hacker and the State*. Cambridge: Harvard University Press.

Bumiller, E., & Shanker, T. (2012, 05.04.2022). Panetta Warns of Dire Threat of Cyberattack on U.S. Retrieved from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Burns, A., & Eltham, B. (2014). Australia's Strategic Culture: Constraints and Opportunities in Security Policymaking. *Contemporary Security Policy, 35*(2), 187 - 210.

Burton, J., & Claire, L. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy, 5*(3), 449-470.

Béland, D., & Cox, R. (Eds.). (2010). *Ideas and Politics in Social Science Research*. New York: Oxford University Press.

Campbell, J. (2002). Ideas, Politics, and Public Policy. *Annual Review of Sociology, 28*(1), 21 - 38.

Capoccia, G., & Kelemen, R. (2007). The study of critical junctures: Theory, narrative, and counterfactuals in historical institutionalism. *World Politics, 59*(3), 341 - 369.

Carr, E. (1964). *The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations*. New York: Harper and Row.

Carson, A. (2018). *Secret Wars: Covert Conflict in International Politics*. Princeton: Princeton University Press.

CCDCOE. (2017, 05.04.2022). Cyber Security Strategy Documents. Retrieved from https://ccdcoe.org/library/strategy-and-governance/

Chong, D. (2013). Degrees of rationality in politics. In L. Huddy, D. Sears, & J. Levy (Eds.), *The Oxford handbook of political psychology* (pp. 96 - 129). Oxford: Oxford Univeristy Press.

Clarke, R., & Knake, R. (2014). *Cyber war*: Tantor Media, Incorporated.

Cray, W., & Schroeder, T. (2015). An Ontology of Ideas. *Journal of the American Philosophical Association, 1*(4), 757 - 775.

Crocker, J., Fiske, S., & Taylor, S. (1984). Schematic bases of belief change. In *Attitudinal judgment* (pp. 197-226): Springer.

Denning, P., & Denning, D. (2016). Cybersecurity is harder than building bridges. *American Scientist, 104*(3), 154-157.

DiMaggio, P. (1997). Culture and Cognition. *Annual Review of Sociology, 23*(1), 263 - 287.

Dittmer, L. (1977). Political Culture and Political Symbolism. *World Politics, 29*(4), 552 - 583.

Dreyer, D. (2010). Issue conflict accumulation and the dynamics of strategic rivalry. *International Studies Quarterly, 54*(3), 779-795.

Dunn Cavelty, M. (2012). The Militarisation of Cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict* (pp. 1-13). Tallinn: IEEE.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105-122.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences, 114*(11), 2825-2830.

Egloff, F. (2020). Public Attribution of Cyber Intrusion. *Journal of Cybersecurity, 6*(1).

Falk, A., & Heckman, J. (2009). Lab Experiments Are a Major Source of Knowledge in the Social Sciences. *Science, 5952*(326), 535-538.

Fearon, J. (1995). Rationalist Explanations for War. *International Organization, 49*(3), 379-414.

Fischerkeller, M., & Harknett, R. (2018, 09.11.2018). Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace. Retrieved from https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace

Fischerkeller, M., & Harknett, R. (2019). Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *The Cyber Defense Review*, 267-287.

Fischerkeller, M., & Harknett, R. (2020). Cyber Persistence, Intelligence Contests, and Strategic Competition. *Texas National Security Review*.

Ford, T, & Kruglanski, A. (1995). Effects of epistemic motivations on the use of accessible constructs in social judgment. *Personality and Social Psychology Bulletin, 21*(9), 950 - 962.

Forsyth, J., & Pope, M. (2014). Structural Causes and Cyber Effects Why International Order is Inevitable in Cyberspace. *Strategic Studies Quarterly, 8*(4), 112-128.

Garcia-Retamero, R., Muller, S., & Rousseau, D. (2012). The Impact of Value Similarity and Power on the Perception of Threat. *Political Psychology, 33*(2), 179-193.

Gartzke, E., & Lindsay, J. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies, 24*(2), 316-348.

Gartzke, E., & Lindsay, J. (2017). Thermonuclear cyberwar. *Journal of Cybersecurity, 3*(1), 37-48.

George, A. (1969). The" operational code": A neglected approach to the study of political leaders and decision-making. *International studies quarterly, 13*(2), 190-222.

Gigerenzer, G. (2008). Why Heuristics Work. *Perspectives on Psychological Science, 3*(1), 20-29.

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security, 43*(3), 141-189.

Gilpin, R. (1981). *War and Change in World Politics*. Cambridge: Cambridge University Press.

Glaser, C. (1994). Realists as Optimists: Cooperation and Self-Help. *International Security, 19*(3), 50 - 90.

Glenn, J. (2009). Realism versus Strategic Culture: Competition and Collaboration? *International Studies Review, 11*(3), 523-551.

Goldgeier, J., & Tetlock, P. (2001). Psychology and International Relations Theory. *Annual Review of Political Science, 4*, 67 - 92.

Goldstein, J. (1988). Ideas, institutions, and American trade policy. In G. Ikenberry, John, D. Lake, & M. Mastanduno (Eds.), *The state and American foreign economic policy*. New York: Cornell University Press.

Goldstein, J. (1993). *Ideas, interests, and American trade policy*. New York: Cornell University Press.

Goldstein, J., & Keohane, R. (Eds.). (1993). *Ideas and Foreign Policy*. New York: Cornell University Press.

Gomez, M. (2018, 06.11.2018). In Cyberwar, There Are Some (Unspoken) Rules. Retrieved from https://foreignpolicy.com/2018/11/06/in-cyberwar-there-are-some-unspoken-rules-international-law-norms-north-korea-russia-iran-stuxnet/

Gomez, M. (2019a). Past behavior and future judgements: seizing and freezing in response to cyber operations. *Journal of Cybersecurity, 5*(1), tyz012.

Gomez, M. (2019b). Sound the alarm! Updating beliefs and degradative cyber operations. *European Journal of International Security, 4*(2), 190-208.

Gomez, M., & Tran Dai, C. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy, 3*(2), 217 - 235.

Gomez, M., & Villar, E. (2018). Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats. *Politics and Governance, 6*(2), 61-72.

Gomez, M., & Whyte, C. (2021). Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly*, *65*(4), 1137-1150.

Gray, C. (1981). National style in strategy: The American example. *International security, 6*(2), 21-47.

Gray, C. (1999). Strategic culture as context: the first generation of theory strikes back. *Review of International Studies*, 49 - 69.

Gray, C. (2005). The American Way of War: Critique and Implications. *Rethinking the Principles of War*, 27-33.

Gray, J. (1990). Brain systems that mediate both emotion and cognition. *Cognition & emotion, 4*(3), 269-288.

Greico, J. (1993). Understanding the Problem of International Cooperation: The Limits of Neoliberal Institutionalism and the Future of Realist Theory. In D. Baldwin (Ed.), *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(1), 49-58.

Hafner-Burton, E., Hughes, A., & Victor, D. (2013). The Cognitive Revolution and the Political Psychology of Elite Decision Making. *Perspectives on Politics, 11*(2), 368-386.

Haglund, D. (2014). What Can Strategic Culture Contribute to Our Understanding of Security Policies in the Asia-Pacific Region? *Contemporary Security Policy, 35*(2), 310 - 328.

Hagmann, J. (2010). *Insecurity Communities: Contested Constructions of Security and Foreign Politics in Contemporary France, Germany and Switzerland*. Geneva: Graduate Institute of International and Development Studies.

Hall, P., & Taylor, R. (1996). Political Science and the Three New Institutionalisms. *Political Studies, 44*(5), 936 - 957.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Harknett, R., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*.

Harris, S. (1994). Organizational culture and individual sensemaking: A schema-based perspective. *Organization Science, 5*(3), 309 - 321.

Healey, J. (2016). Winning and losing in cyberspace. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), *2016 8th International Conference on Cyber Conflict* (pp. 37-49). Tallinn: IEEE.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity, 5*(1), tyz008.

Herrmann, R., Voss, J. F., Schooler, T., & Ciarrochi, J. (1997). Images in international relations: An experimental test of cognitive schemata. *International Studies Quarterly, 41*(3), 403-433.

Hollis, M., & Smith, S. (1990). *Explaining and Understanding International Relations*. Oxford: Clarendon Press.

Holmes, M. (2015). Believing This and Alieving That: Theorizing Affect and Intuitions in International Politics. *International Studies Quarterly, 59*(4), 706-720.

Holsti, O. (1962). The belief system and national images: A case study. *Journal of Conflict Resolution, 6*(3), 244-252.

Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *2013 5th International Conference on Cyber Conflict* (pp. 451-470). Tallinn: IEEE.

ITU. (2016, 05.04.2022). *ICT Development Index*. Retrieved from http://www.itu.int/net4/ITU-D/idi/2016/

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security, 2*(1), 64-87.

Jensen, B., Maness, R., & Valeriano, B. (2016). *Cyber Victory: The Efficacy of Cyber Coercion.* Paper presented at the Annual Meeting of the International Studies Association.

Jensen, B., & Valeriano, B. (2019). *What Do We Know About Cyber Escalation? Observations from Simulations and Surveys*. Retrieved from

Jervis, R. (1976). *Perception and misperception in international politics* (New edition. ed.). Princeton: Princeton University Press.

Jervis, R. (2009). Understanding beliefs and threat inflation. *American Foreign Policy and the Politics of Fear: Threat Inflation since, 9*(11), 16-39.

Johnson, D., & Tierney, D. (2011). The Rubicon theory of war: how the path to conflict reaches the point of no return. *International Security, 36*(1), 7 - 40.

Johnston, A. (1995). Thinking About Strategic Culture. *International Security, 19*(4), 32-64.

Johnston, A. (1998). *Strategic culture and grand strategy in Chinese history*. Princeton: Princeton University Press.

Johnston, A. (1999). Strategic cultures revisited: reply to Colin Gray. *Review of International Studies, 25*(3), 519 - 523.

Jones, D. (1990). Soviet strategic culture. In C. Jacobsen (Ed.), *Strategic Power: United States of America and the U.S.S.R.* (pp. 35 - 49). London: Palgrave Macmillan.

Kahneman, D. (2011). *Thinking, fast and slow* (1st ed.). New York: Farrar, Straus and Giroux.

Kalyuga, S. (2010). Schema Acquisition and Sources of Cognitive Load. In J. Plass, R. Moreno, & R. Brünken (Eds.), *Cognitive Load Theory* (pp. 48-64): Cambridge University Press.

Kaminska, M. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity, 7*(1).

Kari, M., & Pynnöniemi, K. (2019). Theory of strategic culture: An analytical framework for Russian cyber threat perception. *Journal of Strategic Studies*, 1 - 29.

Katzenstein, P. (1996). *Cultural Norms and National Security: Police and Military in Postwar Japan*. Ithaca: Cornell University Press.

Keohane, R. (1993). Institutionalist Theory and the Realist Challenge After the Cold War. In D. Baldwin (Ed.), *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press.

Kertzer, J. (2020). Re-Assessing Elite-Public Gaps in Political Behavior. *American Journal of Political Science*.

Khong, Y. (1992). *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965*: Princeton University Press.

Kitchen, N. (2010). Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation. *Review of International Studies, 36*(1), 117-143.

Klein, B. (1988). Hegemony and strategic culture: American power projection and alliance defence politics. *Review of international studies, 14*(2), 133-148.

Kollars, N., & Moore, E. (2019, 05.04.2022). Every Marine a Blue-Haired Quasi-Rifleperson. Retrieved from https://warontherocks.com/2019/08/every-marine-a-blue-haired-quasi-rifleperson/

Kratochwil, F. (2001). Constructivism as an Approach to Interdisciplinary Study. In K. Fierke & K. Jorgensen (Eds.), *Constructing International Relations: The Next Generation*. New York: M. E. Sharpe.

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *Journal of Cybersecurity, 5*(1).

Kruglanski, A., & Webster, D. (1996). Motivated closing of the mind:" Seizing" and" freezing.". *Psychological review, 103*(2), 263.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. Kramer, Stuart H.; Wentz, Larry (Ed.), *Cyberpower and National Security* (pp. 24-42). Dulles: Potomac Books.

Kurki, M. (2006). Causes of a Divided Discipline: Rethinking the Concept of Cause in International Relations Theory. *Review of International Studies, 32*(2), 189 - 216.

Laffey, M., & Weldes, J. (1997). Beyond belief: ideas and symbolic technologies in the study of international relations. *European Journal of International Relations, 3*(2), 193 - 237.

Lake, D., & Powell, R. (1999). *Strategic Choice and International Relations*. Princeton: Princeton University Press.

Lantis, J. (2002). Strategic Culture and National Security Policy. *International Studies Review, 4*(3), 87-113.

Larson, D. (1994). The role of belief systems and schemas in foreign policy decision-making. *Political Psychology*, 17-33.

Lau, C-M., Kilbourne, L., & Woodman, R. (2003). A shared schema approach to understanding organizational culture change. *Research in Organizational Change and Development, 14*.

Lau, R., & Redlawsk, D. (2001). Advantages and disadvantages of cognitive heuristics in political decision making. *American Journal of Political Science, 45*(4), 951-971.

Legg, J. (2021, 05.04.2022). Confronting The Shortage Of Cybersecurity Professionals. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/21/confronting-the-shortage-of-cybersecurity-professionals/?sh=153f1bf78b9b

Legro, J. (1995). *Cooperation Under Fire: Anglo-German Restraint During World War II*: Cornell University Press.

Legro, J., & Moravcsik, A. (1999). Is anybody still a realist? *International Security, 24*(2), 5 - 55.

Libel, T. (2016). Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy. *Defence Studies, 16*(2), 137 - 156.

Libel, T. (2020). Strategic culture as a (discursive) institution: a proposal for falsifiable theoretical model with computational operationalization. *Defence Studies, 20*(4), 353 - 372.

Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Santa Monica: Rand Corporation.

Liff, A. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401-428.

Lin, H. (2016). Attribution of malicious cyber incidents: From soup to nuts. *Journal of International Affairs*, *70*(1), 75-137.

Lin-Greenberg, E., Pauly, R., & Schneider, J. (2021). Wargaming for International Relations Research. *European Journal of International Relations*.

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404.

Lindsay, J., & Gartzke, E. (2014). Coercion through Cyberspace: The Stability-Instability Paradox Revisited. In K. Greenhill & P. Krause (Eds.), *The Power to Hurt: Coercion in the Modern World*.

Lindsay, J. (2017). Restrained by design: the political economy of cybersecurity. *Digital Policy, Regulation and Governance*.

Lock, E. (2010). Refining strategic culture: return of the second generation. *Review of International Studies, 36*(3), 685 - 708.

Lodge, M., & Taber, C. (2000). Three steps toward a theory of motivated political reasoning. In A. Lupia, M. McCubbins, & S. Popkin, L. (Eds.), *Elements of reason: Cognition, choice, and the bounds of rationality* (Vol. 183, pp. 183 - 213). Cambridge: Cambridge University Press.

Lonergan, E., Lonergan, S., & Valeriano, B. (2022, 05.04.2022). Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why. Retrieved from https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/

Maness, R., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society, 42*(2), 301-323.

Marcus, G. (2000). Emotions in politics. *Annual Review of Political Science, 3*, 221-250.

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security, 46*(2), 51-90.

Mayer, D. (2012, 11.11.2012). Ratio of Bugs Per Line of Code. Retrieved from https://www.mayerdan.com/ruby/2012/11/11/bugs-per-line-of-code-ratio

McDermott, R. (2001). The psychological ideas of Amos Tversky and their relevance for political science. *Journal of Theoretical Politics, 13*(1), 5-33.

McDermott, R. (2002). Experimental methodology in political science. *Political Analysis*, 325-342.

McDermott, R. (2004). *Political psychology in international relations*: University of Michigan Press.

Mearsheimer, J. (1994). The False Promise of International Institutions. *International Security, 19*(3), 5 - 49.

Mearsheimer, J. (2009). Reckless States and Realism. *International Relations, 23*(2), 241 - 256.

Medin, D., Unsworth, S., & Hirschfeld, L. (2007). Culture, Categorization and Reasoning. In S. Kitayama & D. Cohen (Eds.), *Handbook of Cultural Psychology* (pp. 615 - 644). New York: Guildford Press.

Meibauer, G. (2020). Interests, ideas, and the study of state behaviour in neoclassical realism. *Review of International Studies*, *46*(1), 20-36.

Menn, J., & Timberg, C. (2022, 05.04.2022). The dire predictions about a Russian cyber onslaught haven't come true in Ukraine. At least not yet. Retrieved from https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/

Mintz, A. (2004). How do leaders make decisions? A poliheuristic perspective. *Journal of Conflict Resolution, 48*(1), 3-13.

Mintz, A., & DeRouen Jr., K. (2010). Psychological Factors Affecting Foreign Policy Decisions. In *Understanding Foreign Policy Decision Making* (pp. 114-118). New York: Cambridge University Press.

Mintz, A., Redd, S., & Vedlitz, A. (2006). Can we generalize from student experiments to the real world in political science, military affairs, and international relations? *Journal of Conflict Resolution, 50*(5), 757-776.

Mirow, W. (2016). *Strategic Culture, Securitisation and the Use of Force*. New York: Routledge.

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization, 51*(4), 513 - 553.

Morgenstern, O., & von Neumann, J. (1953). *Theory of games and economic behavior*: Princeton University Press.

Morgenthau, H. (1938). The problem of neutrality. *University of Kansas City Law Review, 7*.

Morgenthau, H. (1948). *Politics among Nations: The Struggle for Power and Peace*. New York: Knopf.

Morgenthau, H. (1972). *Science: Servant or Master?, Perspectives in Humanism*. New York: New American Library.

NATO. (2019). Strategy and Governance. Retrieved from https://ccdcoe.org/library/strategy-and-governance/

Newman, L. (2020, 29.10.2020). Ransomware Hits Dozens of Hospitals in an Unprecedented Wave. Retrieved from https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/

Norman, D. (1981). Categorization of action slips. *Psychological Review, 88*(1).

Norman, E., & Delfin, R. (2012). Wizards under uncertainty: Cognitive biases, threat assessment, and misjudgments in policy making. *Politics & Policy, 40*(3), 369-402.

Oppenheimer, H. (2021). *Developing Digital Capacity: How and Why Foreign Assistance Shapes Institutions*.

Parsons, T. (1937). *The Structure of Action* (Vol. Free Press): New York.

Perrow, C. (1984). *Normal accidents : living with high-risk technologies*. Princeton, N.J.: Princeton University Press.

Poore, S. (2003). What is the context? A reply to the Gray-Johnston debate on strategic culture. *Review of International Studies, 29*(2), 279 - 284.

Poznansky, M., & Perkoski, E. (2018). Rethinking secrecy in cyberspace: The politics of voluntary attribution. *Journal of Global Security Studies, 3*(4), 402-416.

Pytlak, A., & Mitchell, G. (2016). Power, rivalry, and cyber conflict: an empirical analysis. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space : theoretical, strategic and legal perspectives* (pp. 65-82). London: Routledge.

Rathbun, B. (2007). Uncertain about uncertainty: Understanding the multiple meanings of a crucial concept in international relations theory. *International Studies Quarterly, 51*(3), 533-557.

Rathbun, B. (2008). A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. *Security Studies, 17*(2), 294-321.

Redlawsk, D. (2002). Hot cognition or cool consideration? Testing the effects of motivated reasoning on political decision making. *Journal of Politics, 64*(4), 1021-1044.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5-32.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Profile Books Ltd.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

Risse, T. (2000). Let's Argue!: Communicative Action in World Politics. *International Organization, 54*(1), 1 - 39.

Roberts, M., Stewart, B., Tingley, D., Lucas, C., Leder-Luis, J., Gadarian, S., . . . Rand, D. (2014). Structural Topic Models for Open-Ended Survey Responses. *American Journal of Political Science, 58*(4), 1064-1082.

Rokeach, M. (1968). *Beliefs, attitudes, and values*. San Francisco: Jossey-Bass.

Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics, 51*(1), 144 - 172.

Rousseau, D., & Garcia-Retamero, R. (2007). Identity, power, and threat perception - A cross-national experimental study. *Journal of Conflict Resolution, 51*(5), 744-771.

Rovner, J. (2019, 16.09.2019). Cyber War as an Intelligence Contest. Retrieved from https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/

Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy, 34*(1), 40-63.

Schechter, B., Schneider, J., & Shaffer, R. (2021). Wargaming as a methodology: the international crisis wargame and experimental wargaming. *Simulation & Gaming*, *52*(4), 513-526.

Schelling, T. (1958). The strategy of conflict. Prospectus for a reorientation of game theory. *Journal of Conflict Resolution, 2*(3), 203-264.

Schmidt, V. (2008). Discursive institutionalism: The explanatory power of ideas and discourse. *Annual Review of Political Science, 11*, 303 - 326.

Schneider, J. (2017, March). Cyber and crisis escalation: insights from wargaming. In *USASOC Futures Forum*.

Schneider, J. (2019). The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War. *Journal of Strategic Studies, 42*(6), 841-863.

Schneider, J. (2022). A World Without Trust: The Insiduous Cyber Threat. *Foreign Affairs, 101*(1), 32 - 43.

Schweller, R. (2006). *Unanswered threats: Political constraints on the balance of power*. New Jersey: Princeton University Press.

Shandler, R., Gross, M., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Support for Retaliation - A Multi-Country Survey Experiment. *British Journal of Political Science*, 1-19.

Shandler, R., Gross, M., & Canetti, D. (2021). A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemporary Security Policy*, *42*(2), 135-162.

Slayton, R. (2017). What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security, 41*(3), 72-109.

Smeets, M. (2020). U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and National Security, 35*(3), 444-453.

Smeets, M., & Work, J. (2020). Operational Decision-Making for Cyber Operations: In Search of a Model. *The Cyber Defense Review, 5*(1), 95-112.

Snyder, J. L. (1977). *The Soviet Strategic Culture. Implications for Limited Nuclear Operations*. RAND CORP SANTA MONICA CALIF.

Sondhaus, L. (2006). *Strategic Culture and Ways of War*. London: Routledge.

Sterling-Folker, J. (1997). Realist environment, liberal process, and domestic-level variables. *International Studies Quarterly, 41*(1), 1 - 25.

Strange, S. (1987). The persistent myth of lost hegemony. *International Organization, 41*(4), 551 - 574.

Suedfeld, P., deVries, B., Bluck, S., Wallbaum, A., & Schmidt, P. (1996). Intuitive perceptions of decision-making strategy: Naive assessors' concepts of integrative complexity. *International Journal of Psychology, 31*(5), 177-190.

Swidler, A. (1986). Culture in Action: Symbols and Strategies. *American Sociological Review, 57*(2), 273 - 286.

Taber, C., Cann, D., & Kucsova, S. (2009). The motivated processing of political arguments. *Political Behavior, 31*(2), 137-155.

Taber, C., & Lodge, M. (2006). Motivated skepticism in the evaluation of political beliefs. *American Journal of Political Science, 50*(3), 755-769.

Taber, C. , Lodge, M., & Glathar, J. (2001). The motivated construction of political judgments. In J. H. Kuklinski (Ed.), *Citizens and politics: Perspectives from political psychology* (pp. 198-226). Cambridge: Cambridge University Press.

Tanczer, L., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy, 9*(3), 60-66.

Thompson, M., Ellis, R., & Wildavsky, A. (1990). *Cultural Theory*. Boulder: Westview Press.

Tilly, C. (1992). How to detect, describe, and explain repertoires of contention. *Center for Studies of Social Change Working Paper Series, 150*(6).

Todd, P., & Gigerenzer, G. (2012). *Ecological rationality: Intelligence in the world*. New York: Oxford University Press.

UNIDIR. (2013). *The Cyber Index: International Security Trends and Realities*. Geneva: United Nations Institute for Disarmament Research

Valeriano, B., & Jensen, B. (2021, 05.04.2022). *Wargaming for Social Science*. Retrieved from https://ssrn.com/abstract=3888395

Valeriano, B., Jensen, B., & Maness, R. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

Valeriano, B., & Maness, R. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research, 51*(3), 347-360.

Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities : cyber conflict in the international system*. Oxford ; New York: Oxford University Press.

Van Evera, S. (1998). Offense, defense, and the causes of war. *International Security, 22*(4), 5-43.

Vasquez, J. (1997). The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition. *American Political Science Review, 91*(4), 899 - 912.

Walt, S. (2002). The Enduring Relevance of the Realist Tradition. In I. Katznelson & H. Milder (Eds.), *Political Science:The State of the Discipline* (pp. 197–230). New York: W.W. Norton.

Waltz, K. (1959). *Man, the state, and war*. New York: Columbia University Press.

Waltz, K. (1979). *Theory of international politics*. New York: Random House.

Weber, M. (1946). The Social Psychology of the World Religions. In H. Gerth & C. Mills (Eds.), *From Max Weber*. Oxford: Ofxord University Press.

Weingast, B. (1995). A rational choice perspective on the role of ideas: Shared belief systems and state sovereignty in international cooperation. *Politics & Society, 23*(4), 449 - 464.

Welch, D. (2011). *Painful choices: a theory of foreign policy change*. New Jersey: Princeton University Press.

Wendt, A. (1999a). Four sociologies of international politics. In R. Little & M. Smith (Eds.), *Perspectives on World Politics* (pp. 446 - 456). New York: Routledge.

Wendt, A. (1999b). *Social theory of international politics*: Cambridge University Press.

Wivel, A. (2005). Explaining why state X made a certain move last Tuesday: the promise and limitations of realist foreign policy analysis. *Journal of International Relations and Development, 8*(4), 355-380.

Wolfers, A. (1962). *Discord and Collaboration: Essays on International Politics*. Baltimore: Johns Hopkins University Press.

Wyer Jr, R., & Gordon, S. (1984). The cognitive representation of social information. In R. Wyer Jr & T. Srull (Eds.), *Handbook of social cognition* (Vol. 2). New Jersey: Lawrence Erlbaum.

Yarhi-Milo, K. (2014). *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. New Jersey: Princeton University Press.

Yee, A. (1996). The causal effects of ideas on policies. *International organization*, *50*(1), 69-108.