8 Cyber uncertainties

Observations from cross-national war games

Miguel Alberto Gomez and Christopher Whyte

Recent years have seen scholars distance themselves from the notion of the revolutionary potential of cyberspace. While the early literature asserted that actions through the domain alter the balance of power between states, evidence over the past decade suggests otherwise (e.g. Valeriano et al. 2018). Instead of serving as an independent transformative instrument, operations in cyberspace are employed alongside established instruments of foreign policy (Gartzke 2013). Consequently, the growing exercise of cyber power is less of a revolution and more of an evolution of state behavior in the 21st century. Yet despite an overall tempering of the exceptionalism attributed to cyberspace, our understanding of domain interactions remains limited with respect to the underlying decision-making processes enacted by policy elites.

Studies that approach the mechanisms of interstate interactions through cyberspace, such as that of Jensen, Valeriano, and Maness (2018), utilize observational data to explore the logic of interactions between states online. These efforts contribute to our understanding of the utility of such interactions. However, the decision-making processes leading up to the use of cyber operations remains relatively obscured. Though the argument that this is an expected limitation of observational studies – particularly in a domain characterized so centrally by covert operation and attribution challenges – is a reasonable one, it is nevertheless the case that a better grasp of the logics that drive decision-making in this domain is critical if scholars are to produce better policy-relevant knowledge about how states harness cyber power.

Despite the surge in both cyber operations and the number of state actors conducting them over the past decade, the utility afforded by actions within the domain remains at least partially unclear. Scholars have, particularly following major incidents like the 2007 digital blockade of Estonia and Stuxnet, questioned the advantages of state operation in cyberspace and have increasingly noted the un-warlike nature of cyber instrument usage.¹ One study, for instance, noted recently that less than 5.2% of publicly disclosed cyber operations resulted in concessions from their intended targets (Valeriano et al. 2018: 23). Given this, it is yet unclear why states continue to invest substantial technical, financial, and organizational resources into using the domain offensively, particularly given the existence of other promising elements of state power.

As the fervor to develop operational capabilities in cyberspace continues unabated and as system-level “logic of the domain” research continues to offer little in the way of new insight as to the utility thereof, it becomes crucial for us to pivot to focus on understanding the motivations and processes that facilitate decisions to operate in cyberspace. This chapter joins an emerging micro-foundational body of scholarship in the field of cyber security research. In the proceeding pages, we discuss the outcome of war games conducted with policy, military, and technical elites from Taiwan, the United States, and the Philippines designed to better understand the significance of decision-maker priors and situational context on key concepts such as “red lines”, attribution, and escalation.

The war games discussed in this chapter are pseudo-experimental. Thus, it is important to note that, while it surfaces certain processes, it cannot completely rule out confounding factors as effectively as might conventional experimental studies. Despite this constraint, the cross-national nature of these war games offers crucial insights concerning the commonalities and variations in response to cyber security incidents. Specifically, the war games highlight the importance of priors in the form of preexisting beliefs and policy preferences that shape operation preferences in response to cyber security incidents. Despite the consistency offered by the war games as well as the commonalities shared by the participants (i.e. respective professional backgrounds), we find that their in-game behavior appears motivated by individualized and/or socialized experiences than responding to threats. These, in turn, serve as heuristic mechanisms that guide decision-making behavior throughout gameplay.

While this is by no means a novel finding, it does confirm observations from comparable experimental studies involving non-elites. Theoretically, this demonstrates the existence of common cognitive processes between these two groups, suggesting the existence of a shared perception of cyber security threats. The possibility of this is noteworthy as it establishes the existence of uncertainty toward the domain irrespective of role that is seemingly alleviated by heuristic use. Methodologically, this challenges the criticisms aimed at experimental research that study elite behavior proxied through non-elite participants. If both populations exhibit comparable cognitive processes, then it is fair to argue that the continued use of experimental designs involving non-elites is a worthwhile endeavor.

With the core objectives and overall findings in this chapter established, the following pages are organized as follows. The next section presents an overview of developments in cyber security scholarship that highlights key questions pursued by the war games and sets the theoretical framework that guides our line of inquiry. This is then succeeded by a methodological discussion of wargaming and the design employed. In qualitatively reporting our results, we focus on the unique cross-national variations in response and cognition across different populations. Specifically, the chapter surfaces individual mechanisms resulting in preferred responses that appear to be rooted not in personal experience or strategic assessment so much as they are in shared cultural or institutional-cultural experience. Finally, the discussion concludes by highlighting the primary lessons learned

from this study and offers possible avenues of expansion for those wishing to pursue this line of inquiry further.

Evolution of the field

Taking into consideration the emergent nature of cyber security as a field of study, this section provides readers with an overview of how it has evolved. Beginning with a discussion of the inherent vulnerability of the domain, it proceeds into the dominant system-level analysis of decision-making in cyberspace prevalent in the literature. By doing so, it highlights the limitations of this approach by acknowledging inconsistencies such as the emphasis on cyber capability development vis-à-vis the absence of demonstratable strategic utility and the limited prioritization of misperception among disputing parties. Consequently, this permits the discussion to flow naturally into the growing behavioral “shift” in cyber security literature as a means of rectifying these gaps in our understanding of decision-making in cyberspace. Furthermore, it emphasizes the importance of micro-level factors as an important steppingstone toward understanding system-level dynamics.

A vulnerable environment

Since its earliest conception in the writings of Arquilla and Ronfeldt (1999), the exercise of power through cyberspace has often been viewed in the context of interstate relations. Though the literature that has emerged since that time is diverse, most scholars agree that the decision to operate in cyberspace rests on three key aspects that characterized the domain: Increased dependence on cyberspace, vulnerabilities inherent to the domain, and the anonymity granted to actors within cyberspace (see, for instance, Kello 2013). Indeed, alone, these traits typify the *cyber revolution* thesis that was developed during the early 2000s.

That cyberspace sits at the heart of modern society is uncontroversial. Globally, fixed broadband subscription has grown from 0.82 to 14.81 per 100 individuals in just the past 17 years. In that same period, internet usage has ballooned from a mere 8.06% of the global population to nearly 50% (Hoffman and Novak 2001). Declining costs of infrastructure and end-user devices increased the accessibility to cyberspace across the period, permitting societies across the globe to maximize the sociopolitical and economic benefits thereof. As Kuehl (2009) notes, cyberspace is now an enabler of the traditional levers of power employed by states to meet their strategic objectives.

Economically, some states, like Singapore, maximized their potential to find positions of strength by becoming information and communications technology (ICT) service providers (Cyber security Agency of Singapore 2016). Politically, world leaders are increasingly exploiting now-pervasive social media to mobilize support (Bor 2014; Enli 2017). Socially, states like Estonia are turning to ICT to offer faster and more efficient services to their citizens (Kalvet 2012). Finally, and perhaps most relevant to this chapter, the coercive potential of cyberspace has prompted states around the world to develop or improve existing organizational

and technological capabilities (see *inter alia* Whyte 2016; Sharp 2017; Borghard and Loneragan 2017).

Juxtaposed to the enabling aspect of cyberspace are the vulnerabilities that are expected of highly complex and interconnected system. As noted by the late Charles Perrow (2014), as systems complexify, it becomes increasingly difficult to correct individual faults. Moreover, it becomes challenging to predict downstream effects of component failure on entire systems. With cyberspace, the features of its components that enable continued expansion also contributes to such pervasive vulnerabilities. Experts estimate that software will typically have between 15 and 50 errors per 1,000 lines of code. To put matters into perspective, systems on the Airbus A380 have around 120 million lines of code (Charette 2009), suggesting at least the existence of approximately 1.8 million errors. Though not all faults will lead to catastrophic failure, the interdependence of systems and their centrality in modern society makes it easy to see how exploitation of single points of failure might have dramatic consequence.

Finally, questions of identity sit at the heart of usage of this man-made domain. While digital forensics allows for the technical identification of malicious actions' origins, attribution of agency or intent remains elusive (Rid and Buchanan 2015). The anonymity offered in cyberspace emboldens malicious actors to exploit the inherent vulnerabilities and growing dependence on cyberspace to meet specific objectives.

A state-centric view of cyber conflict

How does cyberspace actually alter the strategic dynamics of interstate relations? Against the backdrop of the *cyber revolution* thesis's overarching emphasis on domain characteristics, much literature has since focused on the potential of cyber to enable coercion below the threshold of armed conflict. Enabled by expanding utilization, persistent vulnerabilities, and a sense of anonymity, frameworks that account for state activities in this domain build on the notion of the offensive advantage offered by cyberspace (Slayton 2017). Several assumptions underlie this notion, not the least of which is the attribution problem itself. Additionally, attackers rely on secrecy for effectiveness. Their tools have relatively short shelf lives given that even routine defender system updates might nullify technical abilities. And authorization for attacks often does not come from state leaders. Taken together, conflict in cyberspace is characterized by "use or lose" mentalities surrounding capability.

And yet, as convincing as the above logic might be, evidence from this past decade continues to suggest that cyber interactions are not best understood via "logic of the domain"-style arguments. Liff (2012) notes that interstate behavior is governed by the material balance of power, arguing that near-peer adversaries are likely to vigorously engage online while asymmetric relationships may involve more measured responses by the weaker party so as to avoid conventional provocation. Such arguments highlight two key focal points of contemporary cyber security scholarship: Material requirements and escalation avoidance.

In studies of both, it has become apparent that a significant amount of economic, technical, and organizational resources is necessary to effectively employ cyber operations as a coercive instrument (Slayton 2017). In her seminal article, Slayton (2017) argues that substantial organizational capabilities, and corresponding technical skills, are required to successfully infiltrate and threaten secure systems. Furthermore, she challenges the notion that attackers are advantaged in cyberspace by arguing that adversarial success requires knowledge of preexisting defensive mechanisms already in place. Defenders often have the upper hand in shaping the environment such that costs incurred by an adversary are disproportionate to gains (Gartzke 2013). Furthermore, the types of cyber operations popularized by the media and Hollywood are unlikely upon closer inspection. Punishment and risk manipulation strategies are infeasible because of the significant technical and organizational resources required (Valeriano et al. 2018). In these instances, it may be cheaper to rely on conventional means (e.g. a missile).

Recently, scholars such as Lindsay and Gartzke (2016) suggested that in-domain interactions reflect the stability–instability paradox observed during the Cold War. Adversaries interact and exploit one other’s vulnerabilities online without necessarily engaging in actions that are likely to trigger escalation. In addition, the covert nature of cyber operations means that digital action can constitute signaling via which adversaries might actively communicate their interests in both long-standing and emergent issues while controlling for domestic pressure that may provoke a less measured response. Similarly, Maness and Valeriano (2015) observe that adversaries limit their interactions within the pre-defined range of the existing adversarial relationship. That is to say, while offensive operations in cyberspace are to be expected, these only occur within the normalized bounds of the existing rivalry.

Although cyber security scholarship continues to prosper as an emergent field of study, the majority of scholars that pursue a structural account of state interactions within cyberspace generally agree on the mechanisms established in the preceding paragraphs. *First, resources constrain the overall utility expected from cyber operations. Second, cyber operations serve as an instrument that signals resolve while minimizing escalation.*

During the third quarter of 2018 the United States issued a new cyber strategy signaling a shift away from a deterrence approach to cyber conflict management. Noting the high tempo of operations and growing capabilities of adversaries online, the new strategy surfaces the concept of persistent engagement and forward defense. In sum, the two concepts argue that cyber security may only be achieved by continually engaging and degrading adversarial capabilities and operations wherever they are found (Department of Defense 2018). These concepts, derived from the work of Harknett and Fischerkeller (2017), align both with the strategic realities faced by the United States and the general trend of cyber security scholarship.

That said, they also ignore the potential unintended escalation. Though it would be correct to note – as many have – that escalation has not taken place in response to cyber operations, the prospect cannot be ruled out entirely. In particular, in

debates about the prospective value of persistent engagement, little has been said concerning the possibility of in-domain misperception. Specifically, if the strategy calls for the United States to operate freely in cyberspace, regardless of territorial considerations, what might allies and adversaries interpret from such actions? Although Harknett and Fischerkeller are sanguine about the prospect of continued stability, their dismissal of the possibility for miscommunication is worrisome. Moreover, the limited interest expressed by the field in misperception and other manifestations of cognitive and affective components are problematic given the tendency of decision-makers to rely on these structures given the unique characteristics of the domain.

The behavioral turn in cyber conflict

A groundswell is taking shape with respect to scholarship focusing on the micro-foundational aspects of cyber security. Both Dean and McDermott (2017) support the idea that a growth in the analysis of individual (and organizational) level aspects of cyber security is likely to contribute positively to our understanding of decision-making and state behavior in cyberspace. And while not as consistent as the established structural accounts of behavior in cyberspace, available studies continue to complement existing frameworks as those highlighted in the preceding subsection. Specifically, current research within this level of analysis focuses on the effects of uncertainty on judgment.

For the purpose of this chapter, we treat uncertainty as a function of ambiguity. That is to say, cyberspace is characterized by a significant amount of ambiguity that introduces cognitive constraints on individual decision-makers resulting in sub-optimal outcomes (Rathbun 2007). This is not a novel claim and was proposed by other scholars as a potential source of exceptionalism and hyperbole with respect to cyberspace (Hansen and Nissenbaum 2009; Godman and Arquilla 2014). Ambiguity, in this context, pertains to the uncertainty of meaning given the occurrence of a cyber security incident. That is to say, decision-makers, and the wider polity to the extent that they are aware, are uncertain as to how to interpret malicious actions. In terms of on-going research, interest is centered on how uncertainty impacts judgments concerning intent and consequences (e.g. escalation).

Intent is difficult to gauge when the only evidence available is malicious code. Compared to conventional military instruments, the appearance of tanks at the border sends a clearer signal than the discovery of malware on sensitive systems. Buchanan (2016) argues that this uncertainty of intent may trigger a dilemma between parties. Malicious code used for tolerated espionage activities may also be employed to degrade or disrupt critical infrastructure. Without a clear admission of intent, victims are unable to discern the function of these unwanted discoveries. A similar concern is echoed by Gartzke and Lindsay (2015) who further emphasize that despite discovery and neutralization, victims may feel the need to escalate in order to deter future attempts by potential adversaries.

The lack of certainty with respect to intent provokes a host of heuristic mechanisms to assist in reaching cognitive closure. For their part, both Gartzke and Lindsay (2015) posit that previous behavior may serve as an anchor on which to evaluate the overall intent. This is also shared by Maness and Valeriano (2015) who posit that escalation is minimized in rivalry relationships due to pre-expectations. Both sets of authors indirectly reference the concept of *enemy images* in their arguments. *Enemy images* are cognitive constructs through which other actors are believed to behave in bad faith. These constructs are often formed over time and are molded by another actor's behavior during separate, and possibly unrelated, interactions. As cyber operations are increasingly appearing during emergent or existing disputes, it is likely that these images are formed even before the occurrence of a cyber security incident and lends explanatory weight to the assumptions of the above authors.

Empirically, the influence of *enemy images* on judgments of intent was demonstrated by Gomez (2019) in two separate survey experiments. For the first, the presence of an *enemy image* dissuaded participants from maximizing the available information in order to accurately assess the probability that a suspected adversary was responsible for a given cyber security incident. This implies that behavioral expectations take priority over a rigorous and deliberative assessment of a given situation despite the availability of information. For the second, *enemy images* resulted in participants gravitating toward evidence confirming their pre-existing beliefs regarding the behavior of a potential adversary and a refusal to adjust their judgments in the face of evidence.

The reliance of decision-makers on priors, specifically a dependence on preexisting beliefs, is crucial in understanding interstate behavior in cyberspace. While systemic explanations expect restraint as a means of managing escalation, expectations based on past experience may provoke a more forceful response between adversaries. Moreover, these beliefs may also provoke a degree of overconfidence that is unsubstantiated by material realities and may encourage a more hawkish response to an incident (Bar-Joseph and Kruglanski 2003). As such, *the utilization of enemy images as a heuristic mechanism to reduce uncertainty may result in a deviation from expected rational behavior on the part of decision-makers.*

Apart from intent, uncertainty with respect to the consequences of cyber operations may prompt a host of heuristic mechanisms that may prove detrimental to the maintenance of stability in cyberspace. In this case, questions concerning consequences have been approached from the perspective of the general public and that of political elites. And while the results appear to diverge in some areas, these findings add nuance to existing frameworks that explain interstate relations in cyberspace.

With respect to the influence of uncertain consequences on the general public, Gross, Canetti, and Vashdi (2016, 2017) experimentally demonstrate that the physiological and psychological impact of these incidents are comparable to that of conventional terrorist attacks and that the (potential) loss of life provokes a hawkish attitude among participants in the study. This finding is crucial. Despite the lack of ample evidence, the media still continues to promote the idea of cyber

operations as an existential threat (Lawson and Middleton 2019). Without the necessary expertise, the public may anchor their beliefs on these narratives that increases pressure on policy elites to act decisively. Elites themselves, however, are not immune to the effects of unknown consequences.

Kreps and Schneider (2019) find that elites participating in a series of war games resort to analogical reasoning to make sense of the uncertain consequences of cyber operations. Over a six-year period, elites participating in a war game sponsored by the US Department of Defense (DoD) drew parallels between cyber operations and nuclear weapons. That is, the use of the former is likely to generate a significant destabilizing effect – even after the militarization of a conflict. The use of analogies as a salve for uncertainty is not unheard of. Political psychologists have long argued that analogies are employed as a heuristic mechanism to simplify complex situations by drawing parallels with previous, though not necessarily similar, cases (Khong 1992). For instance, references to Hitler when certain world leaders are acting in a belligerent manner permit leaders to better communicate their message without having to invest significant cognitive resource to the task. Although this may be an efficient simplifying mechanism, it is not without its issues.

The successful use of analogies depends on the degree to which similarities exist. Suffice to say, applying an analogy to a completely unrelated issue may result in a wholly inappropriate outcome (Khong 1992; Bar-Joseph and Kruglanski 2003). For example, references to cyber operations and the 9/11 attacks find little in common with each other. While the United States is vulnerable through cyberspace owing to the state of its infrastructure, there is no evidence to show that terrorists are capable of launching a similar attack. Moreover, there is no proof that a cyber operation has resulted in the loss of life as a first-order effect. Analogies may also prime the use of stereotypes that further aggravates the situation. Building on the example above, references to 9/11 may provoke anger that, in turn, inhibits further search for information thus resulting in abrupt and rash decision-making (Carver and Harmon-Jones 2009; Weeks 2015).

In the case of the war games conducted by Schneider, participants either refused to exercise or severely curtailed their ability to operate within the domain. This appears to contradict one key aspect of state cyber operations mentioned previously: That these are a function of existing material capabilities. The result of the war games appears to temper this claim. Because of their belief in the destabilizing potential of cyber operations by drawing analogies with nuclear weapons, the participants hesitate to use their capabilities to better influence the situation in their favor. Furthermore, Schneider suspects that apprehension (rather than fear) also served to modulate the exercise of cyber power (2019).

Unlike fear that results in an inhibition of deliberative and thoughtful cognition, apprehension promotes risk-averse behavior among individuals. In this case, apprehension due to uncertainty of effects and how the opposing party would perceive cyber operations resulted in cautious behavior. As with analogies, this limits the ability of participants to maximize their capabilities despite having the balance of power in their favor.

With respect to the uncertainty of consequences, its influence over decision-making and, in turn, state behavior, is twofold. *On the one hand, parallels between real-world violence and cyber operations increases hawkishness among non-elites. On the other, the use of analogical reasoning and a sense of apprehension may temper elite response despite having the capabilities to act more decisively.*

Uncertainty with respect to both intent and consequences has serious implications for our understanding of state behavior in cyberspace. While structural explanations expect adherence to the normative requirements of rational choice, the inclusion of micro-foundational concepts raises questions as to the extent to which one could expect decision-makers to act rationally.

War gaming and cross-national comparisons

A methodological shift

With a growing interest in the micro-foundational components of cyber security, scholars are implementing wargaming as a tool to better understand the phenomenon of decision-making in response to cyber operations (for instance, Lin-Greenberg 2018). Although observational studies provide the means with which to investigate real-world incidents, simulations such as war games offer their own set of advantages.

Unlike observational studies, war games provide researchers with the opportunity to observe the intricacies of decision-making in analogous situations (Kreps and Schneider 2019). While approaches such as archival research may afford scholars the opportunity to dissect these processes after the fact, the nature of cyber security suggests that these artifacts are likely to remain classified in the near future. War games, in contrast, enables scholars to observe (in-game) and probe (post-game) participants on the nuances of their actions. Moreover, the fact that fictitious scenarios are used reduces the reticence of participants to share their opinions.

War games also provide scholars a degree of control. While not as extensive as those afforded to experiments, researchers are able to immerse participants in scenarios that best represent their research objectives. This aspect speaks to the question of controlling for confounding variables that may obscure the mechanisms under investigation. This degree of control also extends to the actual participants of the said game. Scholars are able to select participants based on fundamental attributes (e.g. elites versus non-elites) so as to permit a comparison between groups. For instance, running a simulation between specialists and laymen permits an analysis of the importance of domain expertise.

Finally, war games offer a predictable and plausible environment to conduct research. Cyber security scholars interested in studying novel events are at the mercy of the unpredictability of cyber security incidents. With that in mind, war games permit the immersion of participants into relevant scenarios in order to gauge their respective reactions. And while critics may argue the degree to which observed behavior is aligned with that of real-world cases, it should be noted that

absolute realism is not a requirement for participant engagement. Psychological studies note that the suspension of disbelief, or the mere plausibility of the scenario, is enough to encourage realistic behavior from participants (Perla and McGrady 2011). Consequently, the mundane realism of these activities need not be taken to the extreme in order to reap benefits.

War games, however, are not without their disadvantages. Despite the degree of control afforded, these are not comparable with experimental designs that test the internal validity of processes under investigation. Furthermore, experiments are much easier to replicate and thus provide other scholars the opportunity to validate findings. These require other methodologies to complement this particular constraint. War games are also susceptible to developing extreme or unrealistic scenarios. Although nothing prohibits designers from testing behavior at the boundaries of reality, these are less likely to provide useful observations. War games are also best suited to tackling questions concerned with behavior rather than employing it as a means to tease out operations specifics. Phrased differently, a different method is necessary if scholars are after a specific value (e.g. how many tanks will tip the balance of power). Finally, war games are not immune to the problem of accessibility. An accurate assessment of elite behavior still requires the participation of these said elites. The participation of these individuals limits the utility gained from this methodological choice.

Cyber Rubicon wargame

Building on the behavioral turn in cyber security research, a series of cyber security war games were conducted from January to August 2019 involving participants from Taiwan, the Philippines, and the United States.² The objective of the war game is to determine the means with which prior beliefs and analogical reasoning are employed to discern intent and consequences. Readers should note that these war games are part of a larger research project which involves a cross-national survey experiment which is not discussed in this chapter.

The war game consists of a scenario involving the fictitious states, Idemore and Vadare (see Figure 8.1). Both are depicted as having comparable military and economic capabilities and share a common border with each other. At the start of the war game, a growing dispute involving natural resources is taking shape between the two states. Overshadowing this issue are disruptive cyber operations that appear to have originated from Vadare. As the game progresses, Vadare appears to be bringing its diplomatic and military instruments to bear in support of its interests. All the while, cyber operations continue to affect Idemore.

Participants, acting in teams of three, play the role of Idemorean policy elites tasked with addressing the growing crisis. Each participant adopts the role of either the Secretary of Foreign Affairs, Secretary of Defense, or the Secretary of Information Technology and Security. The decision to segregate participants into these roles is twofold. First, these represent state organs that are most likely to be involved in an interstate cyber security incident. Second, by assigning participants to leadership roles in different organizations the simulation aims to mimic

Figure 8.1 Visualization of Vadare and Idemore given to war game participants.

organizational dynamics that may take effect in a real-world setting. It should also be noted that, ideally, participants are recruited from elites that already enact these fictitious roles in one form or another (i.e. military officers are recruited to be the Secretary of Defense). This, however, is constrained by their availability.

The war game is divided into three (3) distinct rounds that simulate growing severity and uncertainty with the situation. At the start of each round, participants are presented with general and role-specific information pertaining to the ongoing crisis. No specific instruction is given whether or not to share or conceal the latter to determine whether or not information-seeking behavior will occur. Other than current developments, participants are also given a list of possible policy responses; one of which needs to be selected by the end of the round. This choice determines the underlying conditions that teams will face in the succeeding round.

It should also be pointed out that this war game is distinct in that it employs a pseudo-experimental component during gameplay. Teams during the second round are either informed that a cyber operation has affected the national health-care system or the national tax system. Teams are randomly assigned to either

condition. This design choice was made to determine the extent to which target salience affects decision-making behavior among the teams.

The entire war game takes approximately 1.5–2 hours to accomplish. After gameplay, teams are debriefed in order to better understand the decision-making processes employed throughout gameplay. The feedback obtained from these sessions are also compared to a pre-game survey meant to measure individual characteristics such as risk aversion, policy preference, and domain expertise to assess whether and how these characteristics influence in-game behavior.

The role of distinct cross-national perspectives

Over the course of three war games involving dozens of participants across three countries, we find distinct evidence in support of the notion that decision-makers, when faced with issues of digital insecurity and the use of cyber instruments, attempt to make their task simpler by looking to parallel non-cyber situations. As is well-observed in the literatures on foreign and domestic policymaking, decision-makers invariably seek to streamline their approach to prospective crises by referring to heuristic shortcuts. Doing so allows stakeholders the cognitive tools necessary to make quick inference about the meaning and significance of events presented to them. In the course of our games, we see, perhaps not unexpectedly, participants frequently look to real-world geostrategic situations, historical episodes, or concepts borrowed from other domains of interstate engagement in their attempt to rapidly assess and respond to evolving cyber-enabled circumstances. Consistent with other findings from preceding survey experimentation, however, the degree to which these efforts affect information processing, confidence in actions proposed and more is variably dependent on preexisting know-how. Simply put, the more individuals know about cyber conflict, the nature of their worldview vis-à-vis international engagement and their educational background – among other things – impacts the manner in which looking for non-cyber parallels is sufficiently grounded in the reality of the scenario being presented.

For the purposes of this chapter, perhaps the most interesting findings from the war games pertain to the clear role of distinct cross-national perspectives in explaining variation in outcomes across participants. Even given the broad similarities in the populations under study as being foreign policy professionals (of one kind or another) in a democratic state, it is clear that cultural, procedural, and political expectations unique to each national context shape decision-maker actions. This is not unique to elites as a similar observation is made with non-elites (Gomez 2019a, 2019b), but it is significant as it confirms the existence of a comparable process among elites.

Perhaps most visibly, there was clear variation across war game participants on numerous instances in how process and procedure made their way into an individual's perception of their assumed role. Across the board, participants communicated clear motivation for their actions based on an operational understanding of the roles given to them. This manifested in two ways – in (1) their understanding of the relationship between roles within their assigned teams and (2) within their

understanding of the norms of foreign policy process. On the former point, for instance, one team noted that a unanimous decision was not easy initially because each team member was only willing to accept responsibility for reporting their portfolio. On the latter point, for instance, a US team consistently articulated their logic of approach to cyber intrusions as a potential function of foreign policy gambits being prosecuted in other domains.

Relatedly, this finding that role perception dictated divergent – occasionally dramatically so – decision-making outcomes among participants was clear not only in how procedure made its way into the process of scenario response. Likewise, there was clear variation in how individuals assessed their responsibilities as either policy, military, or cyber experts within a democratic government – i.e. they focused on the normative implications of their potential responses. For several teams, responsibilities assessed toward the civilian side of government or toward the polity at large led to the determination of thresholds for engagement that varied starkly from those whose response emerged more simply – at least as was represented in debriefing – from analysis of the facts being presented. Moreover, such assessments differed across national cases, which we discuss below.

With regard to the details of the foreign policy crisis being experienced, our findings also highlight the fashion in which attribution and blame manifest with some interesting variation across national professional settings. In particular, we found that war game participants diverged around the question of whether or not a foreign country is complicit in aggressive cyber activity *regardless of whether or not that country's government is actually involved*. As one US team noted,

[s]o, I see that as a little different then Afghanistan harboring Al Qaida forces because they are terrorists, although they are not necessarily linked. Because they are harboring those forces. Because the servers, in this case, were coming from Vadare. The state has some sort of responsibility to react.

This differs from what was generally seen in other country populations (e.g. Taiwan and the Philippines) under study, a team within which, for instance, articulated the consensus position that technical attributes *must* drive calculations above and beyond geographical descriptors. As one officer suggested,

the fact that there was no traffic, you know, there was no botnet traffic indicating that this was actually fired or, you know, triggered from within the enemy state [...] that's probably the key piece of information that attributes the uncertainty into the equation.

Perhaps unsurprisingly, this particular result fits with a broader observation made in post-war game analysis of results and of debriefing materials, that certain specific national narratives dominated the reach for parallels to inform decision-making processes. With respondents in both Philippines and Taiwan, clear reference was made by participants to the overarching threat of Chinese military

modernization and perceived assertiveness in regional affairs. Such references occurred both directly and as a lens through which assessments of intent and capabilities were conducted. As one officer in Taiwan noted, “there’s an occasion to serve in the military in Taiwan, we know, we are actively prepared for a war, right?” By contrast, respondents in the United States were less willing to cast the scenario being presented as representative of a particular real-world situation and instead resorted on numerous instances to simple categorization of the event (i.e. a contest between “middle powers” such as “Iran and Iraq” or “Pakistan and India”) as a means to introduce prospectively useful concepts or precedents. Interestingly, the only two exceptions to this approach with the US population were exchange officers from Australia and the Philippines, both of whom consistently referenced the People’s Republic of China in attempting to contextualize in-game cyber actions.

Finally, the debriefing sessions held in conjunction with our war games across three countries demonstrated some variation in the role that death might play in dictating more or less severe response to cyber incidents. In Taiwan, participants generally felt that loss of life throws the question of retaliation to cyber incidents into more assured territory, with one team asserting strongly that the death of a Taiwanese citizen dictates a democratic mandate for the government to affect justice in its chosen foreign policy response. As one official put it, “[c]yber attack against our infrastructure that leads to loss of human life [...] [t]hat would cause astonishing domestic pressure”. By contrast, military officers surveyed in the United States again reached for categorical characterizations of the scenario to debate the prospect of death in cyber-enabled incidents versus historical or situational ones. Faced with the question of what level of injury to the American people would require a reasonably severe initial response, American participants variously suggested that low numbers of indirect deaths would, particularly given the relative opacity of cyberattacks, perhaps be seen more as an unfortunate result of infrastructure failure or interference. As one officer put it, problems of foreign source “attribution protects us too with no firm return address”. As another noted, “[t]hese things can be slow moving and I don’t believe we’d be forced into military force”. The severity of initial response would, as they saw it, depend directly on the nature of media coverage and public opinion. In other words, where Taiwanese respondents were quick to assert the principle of severe response to death from cyber incidents, American counterparts suggested that the principle applied in greater or lesser degrees depending on either the fact or scope of negative response by the population. “But sure, it might [...]”, one US team described, “[...]become something the president can’t ignore”.

Conclusion

This chapter supports the premise of the recent behavioral turn in cyber security research that much variation across cyber conflict dynamics and outcomes are best explained at the level of the individual and the institution. Specifically, we suggest that war games are useful tools of research that, particularly when

pseudo-experimental designs are employed in support of experiments, can validate findings that often offer greater statistical power and are yet necessarily simple in their construction. Moreover, war games provide the opportunity to better clarify research questions that emerge from such experimental findings.

In our cyber conflict escalation war games, we see evidence that decision-making in this domain works similarly to foreign policy decision-making more broadly insofar as stakeholders reach for shortcuts in past experiences that help them see meaning as quickly as possible. The degree to which such shortcuts interfere with objectivity emerges from a series of factors that constitute individuals' worldview.

Beyond such broad confirmation of well-known decision-making dynamics at work where cyber is involved, however, we also see distinct evidence of cross-national cultural variations influencing response decisions among elite stakeholders. For future research, it seems particularly clear that the socio-institutional correlates of civilian-military relations in a given democracy stand to have a unique impact on decision-making processes, both in terms of the value calculations that individuals bring into their roles and in terms of the strategic cultures that form around unique national circumstance. In our simulations, we see evidence of such context even affecting assessments of the significance of indirect civilian deaths in crisis situations, which suggests that such correlates might ultimately have some effect on the strategic calculations states make around signaling and adversary behavior. As such, scholars and practitioners alike would do well to both encourage and undertake behavioral research that can be scaled to useful inference for the development of doctrine and practical training.

Notes

- 1 Early examples of which include, among others, Liff (2012), Rid (2013), Lindsay (2013), Gartzke (2013), and Valeriano and Maness (2014).
- 2 Additional war games are being planned with Singapore, Switzerland, and Israel.

References

All Links checked on August 20 2021.

- Arquilla, J., and Ronfeldt, D. (1999). The Advent of Netwar: Analytic Background. *Studies in Conflict and Terrorism*, 22(3): 193–206.
- Bar-Joseph, U., and Kruglanski, A. W. (2003). Intelligence Failure and Need for Cognitive Closure: On the Psychology of the Yom Kippur Surprise. *Political Psychology*, 24(1): 75–99.
- Bor, S. E. (2014). Using Social Network Sites to Improve Communication between Political Campaigns and Citizens in the 2012E. *American Behavioral Scientist*, 58(9): 1195–1213.
- Borghard, E. D., and Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. *Security Studies*, 26(3): 452–481.

- Buchanan, B. (2016). *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press.
- Carver, C. S., and Harmon-Jones, E. (2009). Anger is an Approach-Related Affect: Evidence and Implications. *Psychological Bulletin*, 135(2): 183–294.
- Charette, R. N. (2009). This Car Runs on Code. *IEEE Spectrum*. Retrieved from: <https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>.
- Cyber Security Agency of Singapore. (2016). *Singapore Cybersecurity Strategy*. Retrieved from: <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>
- Dean, B., and McDermott, R. (2017). A Research Agenda to Improve Decision Making in Cyber Security Policy. *Penn State Journal of Law & International Affairs*, 5(1): 29–71.
- Enli, G. (2017). Twitter as Arena for the Authentic Outsider: Exploring the Social Media Campaigns of Trump and Clinton in the 2016 US Presidential Election. *European Journal of Communication*, 32(1): 50–61.
- Gartzke, E. (2013). The Mth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2): 41–73.
- Gartzke, E., and Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 24(2): 316–348.
- Goldman, E. O., and Arquilla, J. (2014). *Cyber Analogies (No. NPS-DA-14-001)*. Monterey, CA: Naval Postgraduate School.
- Gomez, M. A. (2019a). Past Behavior and Future Judgements: Seizing and Freezing in Response to Cyber Operations. *Journal of Cyber Security*, 5(1): tyz012.
- Gomez, M. A. (2019b). Sound the Alarm! Updating Beliefs and Degradative Cyber Operations. *European Journal of International Security*, 4(2): 190–208.
- Gross, M. L., Canetti, D., and Vashdi, D. R. (2016). The Psychological Effects of Cyber Terrorism. *Bulletin of the Atomic Scientists*, 72(5): 284–291.
- Gross, M. L., Canetti, D., and Vashdi, D. R. (2017). Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes. *Journal of Cyber Security*, 3(1): 49–58.
- Fischerkeller, M. P., and Harknett, R. J. (2017). Deterrence is not a Credible Strategy for Cyberspace. *Orbis*, 61(3): 381–393.
- Hansen, L., and Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4): 1155–1175.
- Hoffman, D. L., Novak, T. P., and Schlosser, A. E. (2001). The Evolution of the Digital Divide: Examining the Relationship of Race to Internet Access and Usage Over Time. In B. M. Compaine (ed.), *The Digital Divide: Facing a Crisis or Creating a Myth*. Cambridge: MIT Press, pp. 47–97.
- Kalvet, T. (2012). Innovation: A Factor Explaining e-Government Success in Estonia. *Electronic Government: An International Journal*, 9(2): 142–157.
- Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2): 7–40.
- Khong, Y. F. (1992). *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965*. Princeton, NJ: Princeton University Press.
- Kreps, S., and Schneider, J. (2019). Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics. *Journal of Cyber Security*, 5(1): tyz007.
- Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and National Security*, 30. Dulles: Potomac Books.

- Lawson, S., and Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday*, 24(3). <https://doi.org/10.5210/fm.v24i3.9623>.
- Liff, A. P. (2012). Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3): 401–428.
- Lin-Greenberg, E. (2018). Game of Drones: The Effect of Remote Warfighting Technology on Conflict Escalation (Evidence from Wargames). SSRN. Retrieved from: <https://dx.doi.org/10.2139/ssrn.3288988>.
- Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3): 365–404.
- Lindsay, J. R., and Gartzke, E. (2016). Coercion through Cyberspace: The Stability-Instability Paradox Revisited. In K. M. Greenhill and P. J. P. Krause (eds), *The Power to Hurt: Coercion in Theory and in Practice*. New York: Oxford University Press, pp. 179–203.
- Perla, P. P., and McGrady, E. D. (2011). Why Wargaming Works. *Naval War College Review*, 64(3): 111–130.
- Perrow, C. (2014). *Complex Organizations: A Critical Essay*. Brattleboro: Echo Point Books & Media.
- Rathbun, B. C. (2007). Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in International Relations Theory. *International Studies Quarterly*, 51(3): 533–557.
- Rid, T. (2013). *Cyber War Will not Take Place*. Oxford: Oxford University Press.
- Rid, T., and Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2): 4–37.
- Slayton, R. (2017). What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, 41(3): 72–109.
- Sharp, T. (2017). Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *Journal of Strategic Studies*, 40(7): 898–926.
- US Department of Defense. (2018). *National Cyber Strategy of the United States of America*. Washington: US Department of Defense.
- Valeriano, B., and Maness, R. C. (2014). The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. *Journal of Peace Research*, 51(3): 347–360.
- Valeriano, B., and Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.
- Valeriano, B., Jensen, B. M., and Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.
- Weeks, B. E. (2015). Emotions, Partisanship, and Misperceptions: How Anger and Anxiety Moderate the Effect of Partisan Bias on Susceptibility to Political Misinformation. *Journal of Communication*, 65(4): 699–719.
- Whyte, C. (2016). Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea. *Comparative Strategy*, 35(2): 93–102.