4

De-escalation Pathways and Disruptive Technology

Cyber Operations as Off-Ramps to War

Brandon Valeriano and Benjamin Jensen

1 INTRODUCTION

The cyber war long promised by pundits has yet to arrive, failing to match the dramatic predictions of destruction many have been awaiting. Despite fears that digital death is on the horizon (Clarke & Knake, 2014), the international community has seen little evidence. While cyber operations have been used in concert with conventional military strikes from Ukraine (Kostyuk & Zhukov, 2019) to operations against the Islamic State (Martelle, 2018), they have focused more on intelligence collection than shaping direct interdiction. Worst-case scenario nuclear-grade cyberattacks (Straub, 2019) are unlikely and counterintuitive to the logic of cyber action in the international system (Borghard & Lonergan, 2017) where most operations to date tend to reflect political warfare optimized for digital technology, and deniable operations below the threshold of armed conflict (Jensen, 2017; Valeriano et al., 2018).

Decades of research in the field of cybersecurity have laid bare two findings so far: (1) We have failed to witness the death and destruction (Rid, 2020; Valeriano & Maness, 2015) that early prognosticators predicted and (2) digital conflict is typically not a path toward escalation in the international system (Valeriano et al., 2018). Based on survey experiments, when respondents were put in a situation where they had to respond to a militarized crisis using a wide range of flexible response options, more often than not cyber response options were chosen to de-escalate conflicts (Jensen & Valeriano, 2019a, 2019b).

Beyond their raw potential, emergent capabilities like cyber operations are just one among many factors that shape the course of strategic bargaining (Schneider, 2019). New technologies often lead more to questions of resolve and human psychology than objective power calculations about uncertain weapons. The uncertainty introduced by new strategic options, often called exquisite capabilities and offsets, can push states toward restraint rather than war. While these capabilities can certainly lead to dangerous arms races and future risks (Craig & Valeriano, 2016), they tend to play less of an escalatory role in more immediate crisis bargaining. This finding follows work on nuclear coercion in which even nuclear weapons often fail

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

to alter calculations during crises, or have little effect on the overall probability of a crisis (Beardsley & Asal, 2009a, 2009b; Sechser & Fuhrmann, 2017).

How do cyber security scholars explain the evident restraint observed in the cyber domain since its inception (Valeriano & Maness, 2015)? Why have the most powerful states, even when confronted with conventional war, avoided cyber operations with physical consequences? Is it fear or uncertainty that drives the strategic calculus away from escalation during cyber conflicts?

In this chapter, we unpack the strategic logic of interactions during a crisis involving cyber capable actors. We outline the limits of coercion with cyber options for nation-states. After proposing a theory of cyber crisis bargaining, we explore evidence for associated propositions from survey experiments linked to crisis simulations, and a case study of the US-Iranian militarized dispute in the summer of 2019.

2 TOWARD CYBER PEACE AND STABILITY

We are now a field in search of a theory, a theory of cyber peace that explains why cyber capabilities and digital technology offer stabilizing paths in the midst of crisis interactions (Valeriano & Maness, 2015). When we refer to cyber peace, we do not mean the absence of all conflict or positive peace (Roff, 2016), what we have in mind is rather a more measured statement that, while cyber conflicts continue to proliferate, their severity and impact will remain relatively minor (Valeriano & Maness, 2015; Valeriano et al., 2018). This vision of negative peace assumes that violence will continue in the system, but we offer the perspective that during strategic bargaining, cyber options may provide a path toward de-escalation. Cyber operations have the potential to stabilize crisis interactions between rival states. This finding is especially important given that most state-based cyber antagonists are also nuclear armed states (Pytlak & Mitchell, 2016).

On the road to war a state faces many choices regarding the utilization of force and coercion (Schelling, 1960, 1966). Seeking to compel an adversary to back down, a state attempts to display credibility, capability, and resolve (Huth, 1999). To avoid outright conflict, a state can dampen the crisis by making moves that avoid conflict spirals. Much akin to the logic of tit-for-tat struggles of reciprocity (Axelrod & Hamilton, 1981), evidence suggests that actors may choose digital operations to proportionally respond to aggression.

Here we explore the role of cyber operations in producing crisis off-ramps that can stabilize interactions between rival states. That is, during a crisis a state actor is faced with response options to either escalate the conflict, deter further violence, de-escalate the situation, or do nothing. This choice is especially acute during interactions with rivals where tensions are higher. A cyber off-ramp is a strategic choice to either respond in kind, or to de-escalate during a crisis by launching a cyber operation that helps a state set favorable bargaining conditions without losing

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

a significant strategic advantage. By demonstrating weak signals and commitment to the issue at stake, crisis actors can seek to leverage information effects to forestall further escalation.

Cyber operations are not clear paths to peace, but in the context of more dramatic options digital technologies can lead us down a road away from war. During crisis situations, digital technologies can push states away from the brink of escalation by mitigating risks and revealing information to adversaries that helps to manage escalation risks.

3 WHEN DO CRISES ESCALATE?

There is well-established literature on international crises and escalation dynamics, that grew out of the Cold War, which analyzes great power competition as a bargaining process (Schelling, 1958, 2020; Fearon, 1995; Powell, 2002). Conflict as a process is the result of a strategic interactions in which participants attempt to gain an advantage short of the costly gamble of war (Fearon, 1995). During a crisis, each side attempts to signal its capabilities and resolve to the other through deploying military forces, conducting a show of force, making credible threats, and leveraging nonmilitary instruments of power like sanctions and diplomatic demarches.

In this delicate dance, most leaders look to preserve their flexibility to manage escalation risks against the probability of achieving their political objectives. Work on international crises and militarized disputes illustrates this posture through a demonstrated preference for reciprocation strategies in which states adopt a proportional response to threats as a means of maximizing their position short of escalation (Axelrod & Hamilton, 1981; Braithwaite & Lemke, 2011).

Yet, the uncertainty and pressure of a crisis, along with preexisting factors shaping strategic preferences, can pull statesmen away from prudence to the brink of war. States that are rivals are prone to arms races and place a high premium on gaining an advantage in a crisis increasing the probability of escalation (Vasquez, 1993; Sample, 1997; Valeriano, 2013). Territorial disputes tend to be particularly intractable and prone to escalation, especially when there is a recurring history of disputes (Vasquez & Henehan, 2010; Toft, 2014; Hensel & Mitchell, 2017).

Misperception looms large, causing signals to be misinterpreted (Jervis, 2017). Shifts in military capabilities can trigger different risk appetites as the offense–defense balance shifts (Jervis, 1978). There is an open debate about the extent to which espionage and subterfuge in cyberspace alters the security dilemma (Buchanan, 2016). Some work argues that cyber is the perfect weapon and will redefine warfare (Kello, 2017), while other assessments contend it creates a new stability–instability paradox (Lindsay & Gartzke, 2018). Rather than increasing the risk of escalation, cyber operations could act as a crisis management mechanism allowing decision makers to make sharp distinctions between the physical and digital worlds and build active defenses on networks (Libicki, 2012; Jensen & Valeriano, 2019a; Valeriano & Jensen, 2019).

4 THE LOGIC OF CYBER OFF-RAMPS

This chapter helps develop a midrange theory hypothesizing that cyber operations are a possible mechanism for helping states manage crises in a connected world.

First, in crisis settings between rival states cyber operations are best thought of as a coercive capability (Borghard & Lonergan, 2017). In addition to their value in intelligence operations (Rovner, 2019), they allow states to disrupt and degrade rival networks.

As instruments of coercion, cyber operations tend to produce fleeting and limited effects, best characterized as ambiguous signals (Valeriano et al., 2018). Ambiguous signals are "covert attempts to demonstrate resolve that rely on sinking costs and raising risks to shape rival behavior" (Valeriano et al., 2018, p. 13). States engage in covert communication, probing each other during a crisis (Carson, 2020). The benefit of cyber operations is that they are a weak signal that can be denied, preserving bargaining space while still demonstrating a willingness to act. This makes cyber operations a low cost, low payoff means of responding early in a crisis.

Second, experimental studies show that the public tends to treat cyber operations different than they do other domains. There are also key threshold dynamics associated with cyber operations. In a recent study, Kreps and Schneider (2019) found that "Americans are less likely to support retaliation with force when the scenario involves a cyberattack even when they perceive the magnitude of attacks across domains to be comparable." For this reason, cyber operations offer a means of responding to a crisis less likely to incur domestic audience costs that could push leaders to escalate beyond their risk threshold.

Avoiding escalation is especially appealing since there are indications that most twenty-first century great powers maintain a public aversion to casualties. Even authoritarian regimes limit reporting and use a mix of private–military companies and proxies to hide the true cost of war from their citizens (Reynolds, 2019). Given this emerging dynamic, cyber operations offer states a means of responding to a crisis without triggering direct, immediate human costs that can often lead to an emotional, as opposed to a rational, conflict spiral. Cyber operations help states manage thresholds in crisis interactions.

Third, and less explored by the cyber security literature to date, cyber operations are defined by unique substitutability dynamics. To say cyber operations are subject to substitution effects implies that states evaluate the trade-offs inherent in using cyber instruments when signaling another state.

In economics, there is a long history of using marginal analysis (Marshall, 1890; Krugman et al., 2008) to evaluate trade-offs in production and consumption. In microeconomics, the marginal rate of substitution is the extent to which a consumer will give up one good or service in exchange for another (Krugman & Wells, 2008). The two goods or services, even courses of action, can be perfect substitutes, in which case they are interchangeable, or imperfect substitutes – in which case the

indifference curve shifts. Furthermore, there is a distinction between within-group and crosscategory substitution in economics and psychological studies of consumer choice (Huh et al., 2016). There is also a long history of work on foreign policy substitutability in international relations (Most & Starr, 1983; Starr, 2000; Most & Starr, 2015). This research maps out when similar acts, as substitutes, trigger different (Palmer & Bhandari, 2000) or similar foreign policy outcomes (Milner & Tingley, 2011).

Applied to contemporary escalation and foreign policy, contemporary leaders evaluate whether to substitute a cyber effect for a more conventional instrument of power. We propose that there are unique substitutability dynamics involved with selecting cyber operations during strategic bargaining episodes. If cyber operations are not efficient substitutes, then they require an increased number or complements. To the extent that cyber operations are an imperfect substitute, a state would have to use more cyber effects to compel an adversary than, for example, traditional diplomatic demarches or threats of military action. The central question for decision makers thus concerns the ideal typical crosselasticity of demand for cyber operations.

We theorize that cyber operations are subject to certain characteristics that make them weak substitutes, and better thought of as complements. In microeconomics, a complement implies the use of one good or service that requires the use of another complementary good or service. If you use a printer, you are going to need a constant supply of toner and paper. With respect to cyber operations, it means that, as shaping mechanisms, they will tend to be paired with at least one more instrument of power to compensate for their weak substitutability as an ambiguous signal subject to threshold effects. This logic follows earlier findings that states will tend to use cyber operations in conjunction with other instruments of power that include both positive and negative inducements (Valeriano et al., 2018).

Two additional dynamics alter the elasticity of demand for cyber effects in crisis bargaining. First, the elasticity of demand is skewed by the dual-use dynamic of cyber operations. Cyber operations tend to be a use and lose capability limiting when states will risk employing high-end capabilities (Jensen & Work, 2018). Leaders who have cyber probes spying on adversary systems worry about sacrificing their digital scouts for fleeting attack opportunities, a calculation known in US Joint doctrine as intelligence gain/loss.[1] They also worry about burning capabilities by exposing their operations. Many cyber capabilities can be both intelligence and tools of subterfuge simultaneously. A tool kit used to access a rival states computer networks and extract information can also be used to deliver malicious code.

[1] See JP 3-12 Cyber Operations: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. Of note, at the apex of national security, decision makers also weigh political gain/loss (PGL) and technical gain/loss (TGL).

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

Back to the concept of substitution, this dynamic means that states must pay information costs to burn access and deliver their payload. Once you attempt to achieve an effect beyond espionage, one increases the risk that the rival state knows you are accessing their networks. Information costs and the opportunity cost of future intelligence lost to achieve a cyber effect skew elasticity and lowers escalation risks. When a state does employ cyber capabilities to respond to a crisis scenario, they will prefer lower end capabilities to reduce information costs. There are unlikely to employ more exquisite tools to achieve a cyber fait accompli that produces an escalation spiral. More importantly, they will look for specific conditions to use cyber substitutes, such as when a rival state has less cyber capability and thus reduces information costs associated with burning a digital spy.

Second, the elasticity of demand is further skewed by a second category of information cost, the shadow of the future (Axelrod, 1984; Axelrod & Keohane, 1985). States like the United States have more than one rival, and even when a state has a single rival they expect to interact with them in the future. Therefore, burning a tool or tool kit in the present risks losing that capability relative to either another rival in the present or a target state in the future. This compounds the information costs that skew the indifference curve. As a result, cyber operations will tend to be used as complements, combined with other instruments of power to increase the expected marginal effect. They can be used as substitutes, but only under conditions where states assess a lower likelihood of paying additional information costs associated with the dual-use dimension and shadow of the future. On its own, the extent to which a cyber operation is substitutable could trigger a security dilemma (Herz, 1950; Glaser, 1997; Booth & Wheeler, 2007).[2] Yet, the substitution of cyber capabilities occurs in a larger context defined by ambiguous signals and threshold effects that dampen escalation risks. These properties help states escape the security dilemma and view cyberattacks as less escalatory than conventional military operations. In the end, cyber capabilities are weak substitutes and will be used more as complements to manage escalation outside of narrow conditions.

Taken together, the above logic of weak coercive potential, thresholds, and substitution effects produces the following three hypotheses.

H1. Cyber operations are not escalation prone.

Observations from cases and survey experiments should demonstrate that when cyber capabilities are present they are not associated with increased escalation. The null hypothesis is that cyber operations are associated with escalation spirals. The hypothesis is better evaluated through large-N methods associated with either past, observed cyber incidents or survey experiments examining escalation preferences when compared actively to the use of other instruments of power. Case studies

[2] Blue networks are home networks, gray networks are unallied network spaces, and red networks are opposition systems.

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

would show more the process and sequence associated with using cyber operations. One would expect to see cyber instruments used to check escalation as a weak, proportional alternative before crossing into higher thresholds.

H2. Cyber operations are more likely to be used as complements when states consider escalating a crisis.

Due of their weak substitutability, cyber operations will tend to complement other instruments of power. There are inherent cross-domain effects associated with modern crisis management (Gartzke & Lindsay, 2019). When examining survey experiments on crisis decision making involving selecting between cyber and noncyber response options, there should more instances of combining cyber effects with other instruments of power. The null hypothesis would be that there is no relationship between cyber escalation and using multiple instruments of power.

H3. Cyber operations are more likely to be used as substitutes for other measures of power when there are no indications of rival cyber activity.

Since cyber operations tend to be weak substitutes, due to information costs and the elasticity of demand, there should be narrow scope conditions that shape when and how they are used in place for more traditional instruments of power. The state will want to minimize the shadow of the future and avoid losing the inherent value of cyber capabilities that are unknown to the adversary. This dynamic implies that in survey experiments one would expect to see a higher percentage use of cyber tools in treatments where there are no indications the adversary is using cyber operations. This initial indication helps respondents gauge the substitutability costs and inherent trade-offs of using cyber capabilities.

5 HOPE AMONGST FEAR: INITIAL EVIDENCE

5.1 *Research Design*

Demonstrating that cyber operations can serve as crisis off-ramps and represent a common strategic choice to respond proportionally during crisis interactions can be a difficult proposition. The goal is to find evidence, under a controlled setting, when a state will have to make a choice between an option that might cause significant damage, an option that will cause little or no harm, the option of doing nothing, and the ability to wage a cyber operation against the opposition.

We propose two methods to investigate our propositions, a theory-guided case study investigation and a survey experiment using crisis simulations and wargames. Once the plausibility of our propositions is determined, we can follow-up our examinations with further support and evidence through follow on experiments. This is not a simple process and we only begin our undertaking here.

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

The case study presented here represents a theory-guided investigation according to Levy's (2008) typology. These case studies are "structured by a well-developed conceptual framework that focuses attention on some theoretically specified aspects of reality and neglects others" (Levy, 2008, p. 4). In these cases, we cannot rule out other theoretical propositions for the cause of de-escalation, but can demonstrate the process of how cyber activities provide for off-ramps on the road to conflict.

Such case studies can also serve as plausibility probes. According to Eckstein (1975, p. 108), plausibility probes "involve attempts to determine whether potential validity may reasonably be considered great enough to warrant the pains and costs of testing." We can only pinpoint the impact of a cyber operation as a choice and examine the outcome – de-escalation during a case study investigation.

Case studies are useful, but do not provide controlled situations where there are clear options and trade-offs for leadership. It might be that a cyber option was decided before the crisis was triggered, or that a cyber option in retaliation was never presented to the leader. Here, we will use a short case study to tell the story of how a cyber operation was chosen and why it represented a limited strike meant to de-escalate a conflict, but will pair this analysis with an escalation simulation.

Deeper investigations through proper controlled settings can be done through experimental studies. In this case, experimental wargames where a group of actors playing a role must make choices when presented with various options. Our other option is survey experiments to demonstrate the wider generalizability of our findings, but such undertakings are costly and time intensive.

Experiments are increasingly used in political science to evaluate decision making in terms of attitudes and preferences (Hyde, 2015; Sniderman, 2018). While there are challenges associated with external validity and ensuring that the participants reflect the elites under investigation, experiments offer a rigorous means of evaluating foreign policy decision making (Renshon, 2015; Dunning, 2016). For the experiment below, we employ a basic 2×2 factoral design.

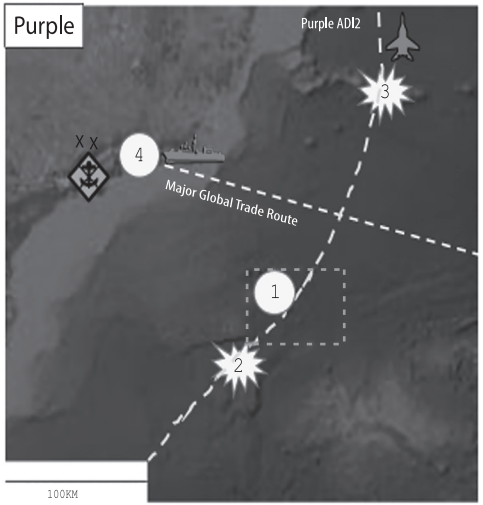
5.2 *Wargames as Experiments*

To date, research on cyber operations have focused either on crucial case studies (Lindsay, 2013; Slayton, 2017), historical overviews (Healey & Grindal, 2013; Kaplan, 2016), and quantitative analysis (Valeriano & Maness, 2014; Kostyuk & Zhukov, 2019; Kreps & Schneider, 2019). Recently, researchers have expanded these techniques to include wargames and simulations analyzed as experiments.

There is a burgeoning literature on the utility of wargames and simulations for academic research. Core perspectives generally define the purpose and utility of wargames, failing to include the wider social science implications of new methodologies defaulting toward the perspective that war-gaming is an art (Perla, 1990; Van Creveld, 2013). More recently, there has been an increasing amount of research offering

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

(ES//NF) Green J2: Corcyra Crisis



Military Balance 20XX		Purple	Green
	Attack Submarines:	40 (20 nuclear)	25 (all nuclear)
	Ballistic Missile Submarines:	8	10
	Carrier Strike Groups:	7	9
	Surface Combatant	100	85
	Fighters	1,800	2,000
	Bombers	300	500
	Nuclear Arsenal (f of Warheads)	1,500	1,250
	Active Army\Marine Personnel	500,000	450,000
	Active Special Forces Personnel	75,000	125,000

Event	Description
1	14OCT20XX. Corcyra LLC, a major international shipping firm headquartered in Green hit by ransomware attacks linked to Purple. Analysts suspect it is linked to territorial dispute between Purple and a Green ally.
2	15OCT20XX. Naval standoff between a Purple Surface Action Group and a Green Expeditionary Strike Group transiting the area. No shots fired, but both sides claim the other locked on fire control radar.
3	15OCT20XX. Aggressive, close proximity maneuver by Purple fighters flying near Green maritime patrol craft resulting in Green emergency landing.
4.	16OCT20XX. Cyber intrusions identified targeting Purple commercial and military port facilities. Purple media demands retaliation.

FIGURE 4.1 *Diagram from Wargame Simulation.*

a social science perspective on war-gaming as a research methodology (Schneider, 2017; Pauly, 2018; Jensen and Valeriano, 2019a, 2019b). The perspective that wargames can add to our knowledge about crisis bargaining under novel technological settings is one we follow herein (Reddie et al., 2018; Lin-Greenberg et al., 2020).

To evaluate the utility of cyber operations in a crisis, the researchers used a conjoint experiment linked to a tabletop exercise recreating national security decision making. Small teams were given packets that resembled briefing materials from US National Security Council (NSC) level deliberations based on guidance from NSC staffers from multiple prior administrations. The packets outlined an emerging crisis between two nuclear-armed states: Green and Purple. The graphics and descriptions tried to obscure the crisis from current states, such as China and the United States. The respondents were asked to nominate a response to the crisis, selecting from a range of choices capturing different response options using diplomatic, information, military, and economic instruments of power. Each instrument of power had a scalable threshold of options, from de-escalatory to escalatory. This range acted as a forced Likert scale. Figure 4.1 shows a sample page from the respondent packets outlining the road to crisis and balance of military capabilities.

The packets were distributed to a diverse, international sample of 400 respondents in live session interactions. In the terms of the types of respondents who participated, 213 were students in advanced IR/political science classes, indicative of individuals likely to pursue a career in foreign policy, 100 were members of the military with the most common rank being major (midcareer), 40 were members of a government involved with foreign policy decision-making positions, 19 were involved with major international businesses, and 13 opted not to disclose their occupation, while 15 left it blank. Of these respondents there were 267 male respondents, 110 female respondents, and 4 who preferred not to say, while 19 opted to leave it blank.[3] With respect to citizenship, 295 respondents were US citizens, 87 were non-US citizens, and 4 preferred not to say, while 14 left their response blank.[4]

These participants were randomly assigned to one of four treatment groups:

Scenario 1. A state with cyber response options (cyber resp) that thinks the crisis involves rival state cyber effects (cyber trig);
Scenario 2. A state with no cyber response options (no cyber resp) that thinks the crisis involves rival state cyber effects (cyber trig);
Scenario 3. A state with cyber response options (cyber resp) that thinks the crisis does not involve rival state cyber effects (no cyber trig); and
Scenario 4. A state with no cyber response options (no cyber resp) that thinks the crisis does not involve rival state cyber effects.

[3] Participants were encouraged to identify gender based on preference and leave it blank if they were gender fluid in most settings to create a safe, inclusive environment.
[4] Participants were encouraged to fill out this option only if they felt comfortable to preserve maximum anonymity and create a safe, inclusive space.

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

TABLE 4.1 *Treatment groups*

Treatment			Number
1.	Cyber Response Options (Yes)	Assumed Rival Cyber Activity (Yes)	100
2.	Cyber Response Options (No)	Assumed Rival Cyber Activity (Yes)	100
3.	Cyber Response Options (Yes)	Assumed Rival Cyber Activity (No)	100
4.	Cyber Response Options (No)	Assumed Rival Cyber Activity (No)	100

N = 400.

These treatments allowed the researchers to isolate cyber response options and assumptions about the role of rival state cyber effects in the crisis. These treatment groups are listed in Table 4.1.

To measure escalation effects associated with cyber capabilities (H1), the survey experiment examined participant response preferences using the respondent initial preference (RESP) variable. This variable asked the survey respondents to indicate their initial reaction and preferred response to the crisis as de-escalate (1), adopt a proportional response (2), escalate (3), or unknown at this time (4). Coding along these lines allowed the researchers to factor in uncertainty and capture if there were any differences between what the survey respondents wanted to do initially, and what they selected to do after reviewing approved response options across multiple instruments of power. Furthermore, as a 2 × 2 experiment focused on attitudes and preferences, the RESP variable helped the team determine if the four different treatments altered the decision to escalate as a cognitive process, and how each participate viewed their options given limited information in a rivalry context. The results are shown in the contingency table (Table 4.2 and Figure 4.2).

Escalation was generally low with only twenty respondents preferring escalation. When they did opt to escalate, neither the presence of cyber response options nor the adversary use of cyber seemed to affect their response preference. Alternatively, when states had cyber response options and there were no signs of rival state cyber effects, participants opted to de-escalate (57) more than expected (47.5). The results were inverse when states were in a crisis that lacked cyber options and adversary cyber effects (treatment 4). Here there were less observed preferences to de-escalate (28) than expected (42.5) and more instances of proportional responses (67) than expected (49.8). The results also lend themselves to categorical variable tests for association using the phi coefficient (Sheskin, 2020). The phi coefficient is 0 when there is no association and 1 when there is perfect association. The value is .286 indicating a weak but significant relationship between the treatment group and escalation preferences consistent with the hypothesis. Cyber options were not associated with escalation and were, in fact, linked to preferences for de-escalation.

TABLE 4.2 *Contingency results by treatment*

			Treatments				
			Cyber Trig Cyber Resp	Cyber Trig No Cyber Resp	No Cyber Trig Cyber Resp	No Cyber Trig No Cyber Resp	Total
RESP	De-escalate	Count	41	44	57	28	170
		Expected Count	42.5	42.5	42.5	42.5	170.0
		% within RESP	24.1	25.9	33.5	16.5	100.0
		% within SCENARIO	41.0	44.0	57.0	28.0	42.5
		% of Total	10.3	11.0	14.2	7.0	42.5
		Standardized Residual	−.2	.2	**2.2	**−2.2	
	Proportional	Count	51	46	35	67	199
		Expected Count	49.8	49.8	49.8	49.8	199.0
		% within RESP	25.6	23.1	17.6	33.7	100.0
		% within SCENARIO	51.0	46.0	35.0	67.0	49.8
		% of Total	12.8	11.5	8.8	16.8	49.8
		Standardized Residual	.2	−.5	**−2.1	**2.4	
	Escalate	Count	5	3	7	5	20
		Expected Count	5.0	5.0	5.0	5.0	20.0
		% within RESP	25.0	15.0	35.0	25.0	100.0
		% within SCENARIO	5.0	3.0	7.0	5.0	5.0
		% of Total	1.3	0.8	1.8	1.3	5.0
		Standardized Residual	.0	−.9	.9	.0	

(continued)

TABLE 4.2 *(continued)*

			Treatments				
			Cyber Trig Cyber Resp	Cyber Trig No Cyber Resp	No Cyber Trig Cyber Resp	No Cyber Trig No Cyber Resp	Total
	Uncertain	Count	3	7	1	0	11
		Expected Count	2.8	2.8	2.8	2.8	11.0
		% within RESP	27.3	63.6	9.1	0.0	100.0
		% within SCENARIO	3.0	7.0	1.0	0.0	2.8
		% of Total	0.8	1.8	0.3	0.0	2.8
		Standardized Residual	.2	**2.6	−1.1	−1.7	
Total		Count	100	100	100	100	400
		Expected Count	100.0	100.0	100.0	100.0	400.0
		% within RESP	25.0	25.0	25.0	25.0	100.0
		% within SCENARIO	100.0	100.0	100.0	100.0	100.0
		% of Total	25.0	25.0	25.0	25.0	100.0

$X^2 = 32.723$, $p < .000$ (two-sided), ** = standardized residual is ±1.96.

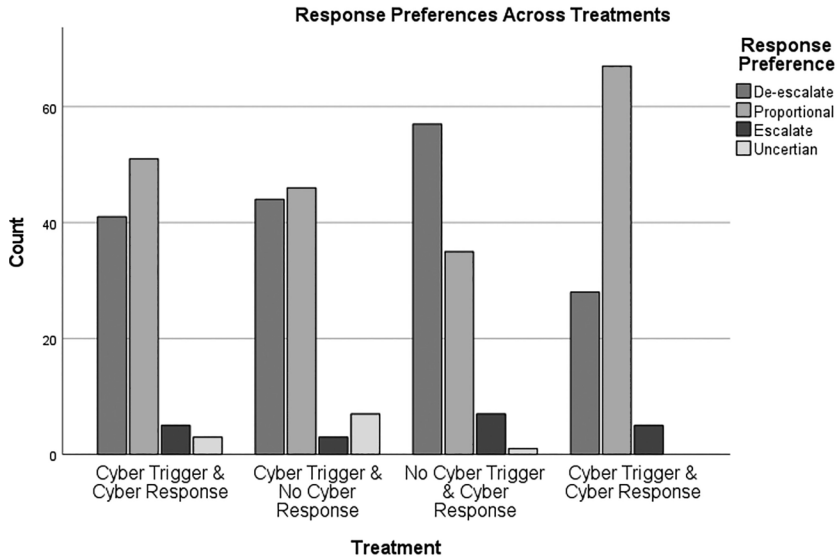


FIGURE 4.2 *Response preferences from wargame simulation.*

A second measure of escalation allows the team to differentiate between the RESP and the overall degree of potential escalation based on the instruments of power selected. This measure is less effective since it does not capture the attitude and preference as a cognitive process in line with best practices in experiments, but does allow the researchers to further triangulate their findings. The researchers created a variable odds of escalation (OES) and average odds of escalation (OESAAVG). OES is a summation and adds the escalation scores from across the actual response options selected. OESAAVG is a binary variable coded 1 if the OES score is over the average and 0 if it is under the average (Table 4.3). OESAAVG allows the researchers to look across the treatments and see if there are differences when cyber response options are present and absent.

The results cast further doubt on cyber operations as being escalatory. Both treatments 1 and 3 had less combined instruments of power above the average coercive potential (29, 30) than expected (37, 37). Of particular interest, when states had cyber response options and escalated, the magnitude tended to be less with treatment 1 seeing 29 instances of above average coercive potential versus 37 expected (–1.3 standardized residual) and treatment 3 seeing 30 instances versus 37 expected (–1.2 standardized residuals). These contrast with treatment 2 where there is a cyber trigger and no cyber response options available. Here there were 48 instances of above average coercive potential versus 37 expected (1.8 standardized residual). Cyber appears to have a moderating influence on how participants responded to the crisis.

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

TABLE 4.3 *Expected count of escalation events*

			SCENARIO				
			1	2	3	4	Total
OESAAVG	0	Count	71	52	70	59	252
		Expected Count	63.0	63.0	63.0	63.0	252.0
		Standardized Residual	1.0	−1.4	.9	−.5	
	1	Count	29	48	30	41	148
		Expected Count	37.0	37.0	37.0	37.0	148.0
		Standardized Residual	−1.3	1.8	−1.2	.7	
Total		Count	100	100	100	100	400
		Expected Count	100.0	100.0	100.0	100.0	400.0

$X^2 = 10.725$, $p < .013$ (two-sided), ** = standardized residual is ±1.96.

Turning to the second hypothesis, to measure complementary effects associated with the survey experiment, the researchers examined how participants combined instruments of power. Participants were allowed to recommend three response options to the crisis. These response options were organized by instruments of power on the aforementioned Likert scale. Each instrument had six options. In treatments where participants had cyber response options, six additional options were added each with an equivalent level of escalation. This gave participants a total of twelve responses in cyber treatments. Since the packets involved four instruments of power (diplomatic, information, military, economic), participants had a total of 24 response options in noncyber treatments (treatments 2, 4) and 48 in cyber response treatments (1, 3). Participants could choose three response options all in one instrument of power, or spread them across multiple instruments of power. Table 4.4 shows the number of response options selected for each instrument of power across the treatments below. There were no statistically significant differences across the treatments with respect to the distribution of the responses.

In each survey experiment, the researchers used this information to create a variable called COMB (combined) that measured the number of instruments of power a respondent used. This number ranged from one to three. Since the survey experiments asked participants to select three options, they could either select three options from any one instrument of power or employ up to three combined instruments of power. To confirm the second hypothesis, one would need to see a higher than expected instances of combining instruments of power comparing conventional versus cyber escalation preferences.

TABLE 4.4 *Treatment groups and instrument of power response preferences*

Treatment	Diplomatic	Information	Military	Economic
1	80	88	57	53
2	81	84	54	67
3	70	85	77	50
4	71	86	60	62

$X^2 = 12$, $p < .213$ (two-sided).

TABLE 4.5 *Conventional versus cyber escalation*

	Conventional Escalation		Cyber Escalation	
Inst Power	No Escalation	Escalation	No Escalation	Cyber Escalation
1	+0(.5)	+1(.5)	6(6.4)	+1(.6)
2	18(16.8)	15(16.2)	19(23.8)	**7(2.2)
3	84(84.7)	82(81.7)	158(152.8)	9(14.2)
	$X^2 = 1.217$, $p < .544$ (two-sided) $N = 200$ (Treatments 2, 4)		$X^2 = 13.726$, $p < .005$ (two-sided) $N = 200$ (Treatments 1, 3)	

** = standardized residual > 1.96.

+ = count is less than 5 (cannot evaluate).

To evaluate hypothesis two along these lines, the researcher separated treatments 2 and 4 and 1 and 3 to compare escalation preferences and combined instruments of power. In Table 4.5, the conventional escalation column shows how many times respondents used 1, 2, or 3 instruments of power, differentiating between treatments that saw escalation and no escalation.[5]

Third, to evaluate substitution, the researchers compare percentages. There should be a higher rate of substitution, measured as using a cyber option, in treatment 3 than in treatment 1. In treatment 3, participants have no evidence the rival state is using cyber capabilities thus making them more likely to substitute cyber effects due to the lower, implied information costs. A respondent would look at the situation and see more utility in using cyber because no adversary cyber effects are present. Alternatively, when adversary cyber effects are present, participants will assess higher information costs. They will be more

[5] For this test, the escalation measure was the coercive potential and whether any instrument selected was greater than 3 on the previously discussed Likert scale for each instrument of power.

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

TABLE 4.6 *Coercive potential*

Treatment	Escalation	Escalation Involved Cyber
1	35	6 (17.14%)
2	50	NA
3	21	11 (52.38%)
4	48	NA

$N = 400$.

TABLE 4.7 *Coercive potential and cyber substitution*

Treatment	Diplomatic	Information	Military	Economic
1	20(3)	10(4)	12(1)	7(1)
3	10(5)	7(5)	14(7)	4(2)

$N = 2{,}000$.

concerned about adversaries being able to mitigate the expected benefit of any cyber response (Table 4.6).

As predicted, there was more observed substitution in treatment 3, as opposed to treatment 1. In treatment 3, 52.38% of the response options selected (i.e., coercive potential) involved cyber equivalents compared with 17.14% for treatment 1. Because there were no indications of adversary cyber capabilities in this treatment, participants likely perceived a cross-domain advantage, hence less information costs. This alters the hypothetical elasticity of demand making cyber a more perfect substitute. Table 4.7 breaks out the substitution further.

In treatment 1, cyber responses were substituted at a higher rate for information effects (40%) than other instruments of power. Three of the four substitutions involved the option to "burn older exploits in adversary systems disrupting their network operations in order to signal escalation risks."

In treatment 3, cyber responses were heavily used to substitute for conventional responses over 50% of the time. The most common military substitution (4/7) involved opting to "compromise data of individual members of the military to include identify theft, fraud, or direct social media messaging." This option substituted for the conventional response: "Conduct a public show of force with air and naval assets challenging known defense zones and testing adversary response." Participates opted for information warfare, or more conventional displays of military force. The most common information substitution remained burning "older exploits in adversary systems disrupting their network operations in order to signal escalation risks." The most common diplomatic substitution in the packet was "use spear phishing, waterholing,

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

and other methods to expose sensitive political information." Again, information warfare was a substitute for more conventional forms of coercion when the adversary posture suggests a low probability of response to information operations.

Another factor stands out when looking at the descriptive statistics associated with differentiating conventional and cyber escalation, measured as coercive potential. As seen in Table 4.6, there is a higher observed rate of coercive potential in noncyber response treatments. The available of cyber response options appears to reduce the coercive potential by substituting information warfare for more traditional approaches to coercion.

Overall, we have evidenced that cyber response options can moderate a conflict between rival powers. Respondents generally used cyber options to either respond proportionally or seek to de-escalate the situation until more information can be gathered. What we cannot explain is whether or not the results were influenced by the presence of nuclear weapons on both sides, different regime types, and other possible confounding variables because our sample was not large enough to enable additional treatments.

6 CASE STUDY PROBE: THE UNITED STATES AND IRAN

To further examine the concept of cyber off ramps and contemporary escalation dynamics, we turn to a theory-guided case study examination (Levy, 2008). Since survey experiments are prone to external validity challenges (Renshon, 2015), a case analysis helps triangulate the findings from the three hypotheses. To this end, interactions between the United States and Iran in the summer of 2019 offer a viable case for examination (Valeriano & Jensen, 2019). Referring to the prior hypotheses, we argue that cyber operations are not escalation prone (H1). We also note that cyber operations are more likely to be used as complements when states do consider escalating (H2), and that cyber operations are more likely to be used as substitutes when there are no indications of rival cyber activity (H3). We now examine our developing theory's plausibility in the context of this case.

6.1 *Origins*

The full picture of what happened between Iran and the United States in the summer of 2019 will continue to develop as classified information is released, but what we do know suggests there was a significant confrontation with cyber operations playing a role as a coercive instrument alongside diplomatic, economic, and military inducements in the dispute. Given that Iran and the United States maintain an enduring rivalry and have a history of using force, even if through proxies, this case was particularly escalation prone. Yet, instead of going to war, Tehran and Washington pulled back from the brink. The key question is why?

https://doi.org/10.1017/9781108954341.004 Published online by Cambridge University Press

As long-term rivals, the United States and Iran have been at loggerheads over the control of the Middle East and resource access for decades (Thompson & Dreyer, 2011). The origins of the contemporary rivalry between Iran and the United States started, from an Iranian perspective, in 1953 when the CIA helped their UK counterparts stage a coup (Kinzer, 2008). From the US perspective, the rivalry dates to the Iranian Revolution and the overthrow of the Shah in 1979, installed in the 1953 coup (Nasri, 1983). The new regime, led by Ayatollah Ruhollah Khomeini, launched a revisionist series of direct and proxy challenges against US interests in the region (Ramazani, 1989) that culminated in a protracted conflict with Iraq. During the Iran–Iraq War, the United States backed Iran's rivals, including Iraq and the larger Gulf Cooperation Council. Iran in turn backed Shiite groups across the Middle East implicated in attacking US forces in the Lebanon.

In the aftermath of the Iranian Revolution and during the subsequent Iran–Iraq War, the United States engaged in limited but direct military engagements with Iran, including the failed Desert One raid to rescue American hostages (1980), and during Operation Earnest Will (1987–1988) in which the US Navy escorted Gulf State oil tankers in a convoy to protect them from Iranian military forces (Wise, 2013). This period included multiple naval skirmishes such as Operational Praying Mantis (1988) and Operational Nimble Archer (1988) in which US forces attacked Iranian oil rigs and military forces in retaliation for Iranian mining in the Strait of Hormuz and repeated attacks. Contemporary US perspectives on Iranian motives and likely foreign policy preferences emerged during this period, with the Washington foreign policy establishment seeing Iran as a revisionist, revolutionary state.[6] Similarly, Iranian attitudes toward the United States hardened even further as Washington labeled the country part of an Axis of Evil (Shay, 2017) and invaded its neighbor, Iraq. Iran opted to counter by funding proxy Shiite groups in Iraq and undermining the transitional Iraqi government.[7]

Parallel to its proxy struggle with the United States in Iraq, Tehran sponsored terror groups that attacked US interests across the region and accelerated its nuclear weapons program.[8] Starting in 2003, the International Atomic Energy Agency started pressuring Iran to declare its enrichment activities, which led to multilateral diplomatic efforts starting in 2004. These efforts culminated in UN Security Council resolutions expanding sanctions on Iran over the subsequent years, and the US joining the multilateral effort (P5+1) in April 2008 following a formal Iranian policy review. Backed by the larger range of diplomatic and economic sanctions that had been in place since the Iranian Revolution, the pressure resulted in the 2015 Joint Comprehensive Plan of Action (JCPOA). This agreement limited Iran's ability to develop nuclear

[6] For an overview of US intelligence estimates during this period, see a 1985 declassified CIA study: www.cia.gov/library/readingroom/docs/CIA-RDP86T00587R000200190004-4.pdf.

[7] This analysis focuses on the context of the dyadic rivalry and does not address the role of Israel and other US security partners in the Middle East, such as Saudi Arabia.

[8] For a timeline of Iranian nuclear efforts and related diplomacy, see the Arms Control Association Timeline (updated September 2020): www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

weapons and included European allies as treaty members distributing the burden of enforcement internationally (Mousavian & Toossi, 2017).

In 2018, the Trump administration withdrew from the agreement, arguing that Iran was still building nuclear weapons and directing proxy warfare against US allies (Fitzpatrick, 2017). The Trump administration wanted to move past the JCPOA agreement, which had reduced tensions in the region. Instead, the Trump administration ramped up sanctions and designated the Islamic Revolutionary Guard Corps, with the Quds force (Tabatabai, 2020), a terrorist organization in 2019 (Wong & Schmitt, 2019). The leader of the organization, QasemSoleimani, became a prime target (Lerner, 2020).

6.2 *Cyber and Covert Operations*

Given Iran's use of proxies, covert operations generally color the relationship between Iran and United States. These activities included the use of cyber capabilities. The United States and Iran were deep in a cyber rivalry, with twenty cyber conflicts between 2000 and 2016 (Valeriano et al., 2018). Data on cyber interactions only begin in 2000, making it difficult to catalog the full range of covert and clandestine activity between 1979 and 2000.

With respect to cyber operations, the United States likely initiated seven cyber operations while Iran launched thirteen (Maness et al., 2019). The most significant event was when the United States and Israel launched the Stuxnet attack, which disabled centrifuges in the Natanz nuclear power plant (Lindsay, 2013). The overall impact of the attack on the Natanz plant is intensely debated, but assessment at the time suggested a limited overall impact on Iran's ability to produce nuclear materials (Barzashka, 2013). It is still unknown what effect the Stuxnet attack had on Iranian internal calculations and assessment of US capabilities.

The pattern between the United States and Iran has often been for the United States to rely on cyber espionage and degrade operations to harm Iranian interests and activities, while Iran generally seeks to avoid direct confrontation in cyberspace (Valeriano & Maness, 2015). Saudi Arabia is a frequent proxy cyber target of Iran, given that the United States is seen as its protector and ally. Iran's actions against the United States mostly entail basic espionage, economic warfare, and the typical probes and feints in cyberspace (Eisenstadt, 2016).

Another key aspect of the covert competition, and the prime threat that Iran offered to the United States, was the use and control of proxy forces in the region. The Iranian Quds force controlled proxy actors in the region (Eisenstadt, 2017), with Houthi forces seeking to attack forces in the region with Scud missiles (Johnston et al., 2020). The awareness that Hezbollah was taking clear direction from Iran altered the dynamics of the dispute between Israel and its regional rivals (Al-Aloosy, 2020). Entering the summer of 2019, Iran's use of proxy forces dominated the concerns of the Trump administration (Simon, 2018; Trump, 2018).

Origins

1979	Rivalry starts with deposition of the Shah of Iran
1980	United States sides with Iraq during with Iran
1993	Persian Gulf War between United States and Iraq
2002	Iran labeled as part of the Axis of Evil
2003	War between Iraq and the United States
2015	Joint Comprehensive Plan of Action
2016	Iranian proxies attack USS Mason off coast of Yemen, missiles fail to hit target
2018	Trump administration withdraws from JCPOA

Focus Summer 2019

April 2019	Islamic Revolutionary Guard Corps designed as a terrorist organization
May 2019	Iran caught attacking tankers; United States increases military presence in the Gulf
June 20, 2019	Downing of US Global Hawk UAV
June 20, 2019	Aborted US strike on Iran
June 22, 2019	Cyber incidents directed against Iran
Dec 27, 2019	Iran attack kills a US contractor on a US base in Iraq
Jan 3, 2020	General Solemani assassinated by the United States

FIGURE 4.3 *Iran–United States Case Timeline* (Source) [no date].

6.3 *The Summer 2019 Crisis*

As the summer began in 2019, tensions accelerated due to concerns about Iranian proxy warfare, the use of cyber actions in the region, and the pursuit of nuclear weapons after the end of the JCPOA (see Figure 4.3 for the timeline of events). In addition to increased hacking activities, Iran attacked tankers in the Persian Gulf, with two incidents occurring in May of 2019. At one point, Iranian operatives were seen placing unidentified objects on the hull of a tanker before it was disabled. Iran "called the accusations part of a campaign of American disinformation and 'warmongering'" (Kirkpatrick et al., 2019).

Following intelligence reports that Iran was plotting an attack on US interests in the Middle East on May 5, 2019, National Security Adviser, John Bolton, announced (Bolton, 2019) the deployment of a carrier strike group and bomber task force to the Middle East to "send a clear and unmistakable message to the Iranian regime that any attack on the United States interests or those of our allies will be met with unrelenting force." In response, on May 12 the crisis escalated with four commercial vessels, including two Saudi Aramco ships, targeted by sabotage attacks attributed to Iran in the Gulf of Aden (Yee, 2019). By May 13, the Pentagon announced plans to deploy as many as 120,000 troops in the region in additional fighter squadrons and naval task forces already headed to the region (Schmitt & Barnes, 2019). In response, on May 14 Iranian proxies in Yemen launched a massive attack against Saudi oil infrastructure using a mix of drones and cruise missiles (Hubbard et al., 2019). By the

end of May, the United States implicated Iran proxies in firing rockets at US interests in Iraq and responded with additional troop deployments and weapon sales to Saudi Arabia. These measures added to the range of economic sanctions the Trump administration initiated following its departure from the JCPOA (News, 2018).

The increasingly militarized crisis continued into June. On June 6, 2019, Iranian-backed rebels in Yemen shot down a MQ-9 Reaper, leading the US Central Command (CENTCOM) Commander to warn that US forces faced an imminent threat throughout the region (Kube, 2019). On June 13, magnetic mines, likely delivered by Iranian unmanned subsurface vehicles, damaged two additional commercial vessels, leading the United States to announce additional troop deployments.

The downing of a US RQ-4A Global Hawk UAV on June 20, 2019, served notice that conflict was likely to escalate. The United States deemed it an unprovoked attack of an aircraft in international waters. President Trump ordered a military strike on June 20, but halted the operation over fears of mass casualties on the Iranian side, or fears of the impact of a war with Iran on reelection. He stated on Twitter, "We were cocked & loaded to retaliate last night on 3 different sights when I asked, how many will die. 150 people, sir, was the answer from a General. 10 minutes before the strike I stopped it, not proportionate to shooting down an unmanned drone." (Olorunnipa et al., 2019).

Instead of escalating the conflict, on June 22 the United States leveraged a series of cyber operations to respond proportionally to Iranian provocations. There seems to have been a few distinct operations; it is unclear how many separate teams or tasks were directed against Iran. One operation disabled Iran's ability to monitor and track ships in the region by attacking their shipping databases (Barnes, 2019b). Another operation by US Cyber Command was said to have disabled Iranian missile sites, making them vulnerable to air attacks (Nakashima, 2019). In addition, the United States was also likely dumping Iranian code on the site VirusTotal (Vavra, 2019), potentially impairing Iranian's ability to retaliate by spilling their tools so other defenders were prepared.

The cyber operations served to signal risk to the Iranians and preserve further options to manage the crisis if it was to continue. The proportional response to Iran's activities possibly allowed for the conflict to stabilize and helped push the two states away from the brink of war. On the road to war, cyber options provide a critical path away from confrontation while still managing to service domestic audience concern

On June 24, cyber security scholar, Bobby Chesney, observed, "Indeed, reading the tea leaves from the past weekend, it appears the cyber option helped ensure there was an off-ramp from a kinetic response that might have led to further escalation." (Pomerleau & Eversden, 2019). On June 25, Valeriano and Jensen (2019) wrote a column in *The Washington Post* that stated, "contrary to conventional wisdom, cyber options preserve flexibility and provide leaders an off-ramp to war."

Following a tense summer, the conflict moved into a new phase in late 2019 and 2020 with the killing of an American contractor after a rocket attack on the US base in Iraq on December 27, 2019 (Barnes, 2019a). The United States retaliated with strikes against Iranian proxies, the Hezbollah, in Iraq and Syria. Hezbollah then attacked the American embassy in Iraq, leading to the US president authorizing the assassination of IRGC Commander, Qasem Solemani, on January 3, 2020 (Zraick, 2020). The United States moved to deploy 4,000 addition troops in the region and Iran retaliated by launching missile strikes on US bases in Iraq, wounding over a hundred soldiers (Zaveri, 2020). The conflict was finally de-escalated, with the United States choosing to not respond to the Iranian attack by claiming that no one had been killed. Since there was six months between the summer and winter 2019/2020 incidents, they are treated as two distinct, albeit linked, crisis cases.

6.4 *Assessing the Case*

Assessment of the events suggests that the crisis with Iran could have escalated in June 2019 after the downing of the Global Hawk UAV, seen as a significant piece of military hardware costing around $220 million (Newman, 2019). Demands for retaliation and escalation were rife in the foreign policy community and within the Trump Administration (Trevithick, 2019).

Instead of escalation, the United States took a different path, consistent with Hypothesis 1. By responding through cyber actions, the United States did two things. First, it demonstrated commitment and credibility to counter Iranian operations by signaling intent for future operations that could have dramatic consequences on Iranian power in the region. Second, these cyber operations also served as Phase 0 operations meant to shape the environment and set the conditions should the United States want to use additional military options in the future. With Iranian defensive systems compromised, Iran was vulnerable to an American attack that never came, and simultaneously subject to a cyber substitute consistent with Hypothesis 3. Cyber operations served to de-escalate the conflict by vividly illustrating the shadow of the future for continued Iranian harassment in the region.

President Trump also increased targeted sanctions directed at Iran's leadership and threated further strikes, stating that he did not need Congressional approval due to the existing authorization for military forces in the region to respond to terrorist threats (Crowley, 2020).[9] These moves are consistent with Hypothesis 2, which suggests that cyber operations are used to complement other forms of power if there is a consideration for escalation.

[9] A list of all US sanctions can be found at a US State Department resource (www.state.gov/iran-sanctions/). Sanctions were already fairly extensive in the summer of 2019 and the United States only added targeted sanctions against industries and various actors after the downing of the US Global Hawk.

When challenged by a strike on an American asset in the region, the United States had two options, respond in kind or escalate the conflict. Doing nothing would incur significant audience costs among President Trump's base of support because it would demonstrate weakness. Escalation would likely provoke retaliation by proxy forces all over the Middle East leading to significant US casualties. War would also harm the President's reelection chances after promising a reduction in tensions and an end to the wars in the region (Tesler, 2020).

Choosing the option of cyber operations and increased sanctions fits clearly with an off-ramp perspective on crisis bargaining. As Hypothesis 3 argued, cyber operations are likely to be used as substitutes when there are no indications of adversary cyber activity. Here cyber options substituted military options because Iran did not escalate in the cyber domain in response to US cyber moves, and Washington likely judged it had a domain advantage.

Cyber options offered a path out of the conflict through responding in ways that target Iran's command and control functions directly, demonstrating decreased capacity for Iran to control their battlespace. Of particular interest, some of the cyber operations specifically limited Iran's ability to retaliate in cyberspace by leaking the malicious code Tehran was likely to use. No other military response options were utilized, although they were considered, after cyber operations were leveraged. Cyber options can serve as off-ramps from the path to war.

7 CONCLUSION: THE PROMISE AND LIMIT OF CYBER OFF-RAMPS

Based on the observations from experiments and a case study of a US-Iranian crisis in the summer of 2019, we conclude that cyber response options limit the danger of escalation. If used correctly to signal to the opposition to moderate behavior, or as demonstrations of resolve, cyber operations allow states to check the behavior of the opposition with minimal danger of escalation. Cyber options allow a state to express discontent and reshape the balance of information between two opposing parties.

To date, states appear to use cyber options to decrease tensions. This is a counterintuitive finding when many in the discipline suggest that either cyber is inherently escalatory or the nature of conflict has changed. It might be true that conflict has changed, but information operations and cyber operations are generally less escalatory and therefore less dangerous than confronting the opposition with conventional weapons. In other words, the logic of substitution and complements appears to apply to the digital domain. The nature of research suggests that there is less danger in using cyber operations as off-ramps to initial confrontations. We must be clear that we are not suggesting cyber operations as a first strike option. To the contrary, cyber operations likely risk sparking a security dilemma when the target is less capable. Yet, as reactions to initial hostility, cyber options provide a path away from war.

Despite a demonstrated case, as well empirical and experimental evidence suggesting cyber operations are not associated with crisis escalation, there are still limits to these findings. Inequality and the inability of a state to respond to a cyber action with cyber response options increases the dangers of escalation. The behavior and strategic posture of the target can be a critical part of the equation. A history of disputes that create overall tension in a dyad can lead to escalation if the issue is salient enough, even if there are cyber response options (Vasquez, 1993). Our simulation was constricted to one interaction, meaning that we did not test the conditions for escalation across a series of disputes.

The policy advice that emerges from this research is to integrate cyber options into a "whole of government" response tailored to each contingency. In an extended bargaining situation, cyber responses to initial moves can reveal information and decrease tensions, countering much of the hype and hysteria about digital technology exacerbating conflict. That said, cyber operations must be evaluated in terms of the extent to which they act as a complement or substitute, as well as how they might lead to misperception or undermine global connectivity, given the fact that the networks cyber operations target and rely on are largely owned by the private sector. Misperception is still a risk in the digital domain.

The policy goal should be to adopt moderate cyber operations that seek to shape the environment to avoid escalation risks, even if those risks are generally low. By revealing and gathering information in a bargaining situation, cyber options can help decrease tensions by giving states the space they need to maneuver and seek to end a conflict. Using cyber operations, especially cyber operations meant to critically wound command and control facilities or cause death in an offensive manner early during the precrisis period, would likely lead to escalation.

REFERENCES

Al-Aloosy, M. (2020). *The changing ideology of Hezbollah*. Springer.

Axelrod, R. (1984). *The evolution of cooperation*. Basic Books.

Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. *Science*, 211(4489), 1390–1396.

Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World Politics*, 38(1), 226–254.

Barnes, J. E. (2019a, December 27). American contractor killed in rocket attack in Iraq. *New York Times*. www.nytimes.com/2019/12/27/us/politics/american-rocket-attack-iraq.html

Barnes, J. E. (2019b, August 28). U.S. cyberattack hurt Iran's ability to target oil tankers, officials say. *New York Times*. www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Barzashka, I. (2013). Are cyber-weapons effective? Assessing Stuxnet's impact on the Iranian enrichment programme. *The RUSI Journal*, 158(2), 48–56.

Beardsley, K., & Asal, V. (2009a). Nuclear weapons as shields. *Conflict Management and Peace Science*, 26(3), 235–255.

Beardsley, K., & Asal, V. (2009b). Winning with the bomb. *Journal of Conflict Resolution*, 53(2), 278–301.
Bolton, J. (2019, May 5). *Statement from the National Security Advisor Ambassador John Bolton*. White House. www.whitehouse.gov/briefings-statements/statement-national-security-advisor-ambassador-john-bolton-2/
Booth, K., & Wheeler, N. (2007). *The security dilemma: Fear, cooperation, and trust in world politics*. Springer Nature.
Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26(3), 452–481.
Braithwaite, A., & Lemke, D. (2011). Unpacking escalation. *Conflict Management and Peace Science*, 28(2), 111–123.
Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
Carson, A. (2020). *Secret wars: Covert conflict in international politics*. Princeton University Press.
Clarke, R. A., & Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.
Craig, A., & Valeriano, B. (2016). *Conceptualising cyber arms races* [Manuscript]. 8th International Conference on Cyber Conflict Tallinn, Estonia.
Crowley, M. (2020, May 6). Trump vetoes measure demanding congressional approval for Iran conflict. *New York Times*. www.nytimes.com/2020/05/06/us/politics/trump-vetoes-iran-war-powers.html
Dunning, T. (2016). Transparency, replication, and cumulative learning: What experiments alone cannot achieve. *Annual Review of Political Science*, 19(1), 541–563.
Eckstein, H. (1975). Case studies and theory in political science. In F. Greenstein & N. Polsby (Eds.), *Handbook of political science* (vol. 7, pp. 79–138). Reading, MA: Addison-Wesley.
Eisenstadt, M. (2016). *Iran's lengthening cyber shadow*. Washington Institute for Near East Policy.
Eisenstadt, M. (2017). *Iran after sanctions: Military procurement and force-structure decisions*. International Institute for Strategic Studies. www.washingtoninstitute.org/uploads/Documents/opeds/Eisenstadt20171219-IISS-chapter.pdf
Fearon, J. D. (1995). Rationalist explanations for war. *International Organization*, 49(3), 379–414.
Fitzpatrick, M. (2017). Assessing the JCPOA. *Adelphi Series*, 57(466–467), 19–60.
Gartzke, E., & Lindsay, J. R. (2019). *Cross-domain deterrence: Strategy in an era of complexity*. Oxford University Press.
Glaser, C. L. (1997). The security dilemma revisited. *World Politics*, 50(1), 171–201.
Healey, J., & Grindal, K. (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
Hensel, P. R., & Mitchell, S. M. (2017). From territorial claims to identity claims: The Issue Correlates of War (ICOW) Project. *Conflict Management and Peace Science*, 34(2), 126–140.
Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics*, 2(2), 157–180.
Hubbard, B., Karasz, P., & Reed, S. (2019, September 14). Two major Saudi oil installations hit by drone strike, and U.S. blames Iran. *New York Times*. www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html
Huh, Y. E., Vosgerau, J., & Morewedge, C. K. (2016). More similar but less satisfying: Comparing preferences for and the efficacy of within-and cross-category substitutes for food. *Psychological Science*, 27(6), 894–903.

Huth, P. K. (1999). Deterrence and international conflict: Empirical findings and theoretical debates. *Annual Review of Political Science*, *2*(1), 25–48.
Hyde, S. D. (2015). Experiments in international relations: Lab, survey, and field. *Annual Review of Political Science*, *18*(1), 403–424.
Jensen, B. (2017). The cyber character of political warfare. *The Brown Journal of World Affairs*, *24*(1), 159.
Jensen, B., & Valeriano, B. (2019a, March 27). *Cyber escalation dynamics: Results from war game experiments international studies association*. Annual Meeting Panel: War Gaming and Simulations in International Conflict.
Jensen, B., & Valeriano, B. (2019b). *What do we know about cyber escalation? Observations from simulations and surveys*. Atlantic Council. www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf
Jensen, B., & Work, J. D. (2018, September 4). *Cyber civil-military relations: Balancing interests on the digital frontier*. War on the Rocks. https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/
Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.
Jervis, R. (2017). *Perception and misperception in international politics*. Princeton University Press.
Johnston, T., Lane, M., Casey, A., Williams, H. J., Rhoades, A. L., Sladden, J., Vest, N., Reimer, J. R., & Haberman, R. (2020). *Could the Houthis be the next Hizballah? Iranian proxy development in Yemen and the future of the Houthi movement*. RAND Corporation.
Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. Simon & Schuster.
Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
Kinzer, S. (2008). *All the Shah's men: An American coup and the roots of Middle East terror*. John Wiley & Sons.
Kirkpatrick, D. D., Perez-Pena, R., & Reed, S. (2019, June 13). Tanks are attacked in the Mideast, and U.S. says video shows Iran war involved. *New York Times*. www.nytimes.com/2019/06/13/world/middleeast/oil-tanker-attack-gulf-oman.html
Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*, *63*(2), 317–347.
Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, *5*(1), 1–11. https://doi.org/10.1093/cybsec/tyz007
Krugman, P., & Wells, R. (2008). *Microeconomics*. Macmillan.
Krugman, P. R., Robin, W., & Olney, M. L. (2008). *Fundamentals of economics*. Reversed.
Kube, C. (2019, June 6). U.S. Commander says American Forces face "Imminent" threat from Iran. *NBC News*. www.nbcnews.com/news/military/u-s-commander-says-american-forces-face-imminent-threat-iran-n1014556
Lerner, K. L. (2020). *The American Assassination of Iranian Gen. Qassem Soleimani: Strategic Implications, Asymmetrical Threat Risks, and US Congressional Reporting Requirements*. Taking Bearings.
Levy, J. S. (2008). Case studies: Types, designs, and logics of inference. *Conflict Management and Peace Science*, *25*(1), 1–18.
Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. RAND Corporation.
Lin-Greenberg, E., Pauly, R., & Schneider, J. (2020, August 18). *Wargaming for political science research*. SSRN. http://dx.doi.org/10.2139/ssrn.3676665
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.
Lindsay, J. R., & Gartzke, E. (2018). Coercion through cyberspace: The stability-instability paradox revisited. In K. M. Greenhill & P. Krause (Eds.), *Coercion: The power to hurt* (pp. 179–203). Oxford University Press.

Maness, R., Valeriano, B., & Jensen, B. (2019). *Dyadic cyber incident and campaign dataset* (Version 1.5) [Data File].
Marshall, A. (1890). The principles of economics. McMaster University Archive for the History of Economic Thought.
Martelle, M. (2018, August 13). *Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War against ISIL*. National Security Archive. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil
Milner, H. V., & Tingley, D. H. (2011). Who supports global economic engagement? The sources of preferences in American foreign economic policy. *International Organization*, *65*(1), 37–68.
Most, B. A., & Starr, H. (1983). International relations theory, foreign policy substitutability, and nice laws. *World Politics*, *36*(3), 383–406.
Most, B. A., & Starr, H. (2015). *Inquiry, logic, and international politics: With a new preface by Harvey Starr*. University of South Carolina Press.
Mousavian, S. H., & Toossi, S. (2017). Assessing US–Iran nuclear engagement. *The Washington Quarterly*, *40*(3), 65–95.
Nakashima, E. (2019, June 22). Trump approved cyber-strikes against Iran's missile systems. *The Washington Post*. www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html
Nasri, F. (1983). Iranian studies and the Iranian Revolution. *World Politics*, *35*(4), 607–630.
Newman, L. H. (2019, June 20). The drone Iran shot down was a $220M surveillance monster. *Wired*. www.wired.com/story/iran-global-hawk-drone-surveillance/
News, B. (2018, August 7). Iran sanctions: Trump warns trading partners. *BBC News*. www.bbc.com/news/world-us-canada-45098031
Olorunnipa, T., Dawsey, J., Demirjian, K., & Lamothe, D. (2019, June 21). "I stopped it": Inside Trump's last-minute reversal on striking Iran. *The Washington Post*. www.washingtonpost.com/politics/i-stopped-it-inside-trumps-last-minute-reversal-on-striking-iran/2019/06/21/e016effe-9431-11e9-b570-6416efdc0803_story.html
Palmer, G., & Bhandari, A. (2000). The investigation of substitutability in foreign policy. *Journal of Conflict Resolution*, *44*(1), 3–10.
Pauly, R. B. (2018). Would US leaders push the button? Wargames and the sources of nuclear restraint. *International Security*, *43*(2), 151–192.
Perla, P. P. (1990). *The art of wargaming: A guide for professionals and hobbyists*. Naval Institute Press.
Pomerleau, M., & Eversden, A. (2019, June 24). *What to make of US cyber activities in Iran*. Fifth Domain. www.fifthdomain.com/dod/2019/06/25/why-trump-may-have-opted-for-a-cyberattack-in-iran/
Powell, R. (2002). Bargaining theory and international conflict. *Annual Review of Political Science*, *5*(1), 1–30.
Pytlak, A., & Mitchell, G. E. (2016). Power, rivalry and cyber conflict: An empirical analysis. In K. Fris & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 81–98). Routledge.
Ramazani, R. K. (1989). Iran's foreign policy: Contending orientations. *Middle East Journal*, *43*(2), 202–217.
Reddie, A. W., Goldblum, B. L., Lakkaraju, K., Reinhardt, J., Nacht, M., & Epifanovskaya, L. (2018). Next-generation wargames. *Science*, *362*(6421), 1362–1364.
Renshon, J. (2015). Losing face and sinking costs: Experimental evidence on the judgment of political and military leaders. *International Organization*, *69*(3), 659–695.

Reynolds, N. (2019). *Putin's Not-so-secret Mercenaries: Patronage, geopolitics, and the Wagner group*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Roff, H. (2016, September 28). "Weapons autonomy risk is rocketing." Foreign Policy. https://foreignpolicy.com/2016/09/28/weapons-autonomy-is-rocketing/

Rovner, J. (2019, September 16). *Cyber war as an intelligence contest*. War on the Rocks. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/

Sample, S. G. (1997). Arms races and dispute escalation: Resolving the debate. *Journal of Peace Research*, *34*(1), 7–22.

Schelling, T. (1960). *The strategy of conflict*. Cambridge: Harvard University Press.

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

Schelling, T. C. (1966). *Arms and influence*. New Haven: Yale University Press.

Schelling, T. C. (2020). *Arms and influence*. Yale University Press.

Schmitt, E., & Barnes, J. E. (2019, May 13). White House reviews military plans against Iran, in echoes of Iraq war. *New York Times*. www.nytimes.com/2019/05/13/world/middleeast/us-military-plans-iran.html

Schneider, J. (2017). *Cyber and crisis escalation: Insights from Wargaming*. USASOC Futures Forum. https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf

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.

Sechser, T. S., & Fuhrmann, M. (2017). *Nuclear weapons and coercive diplomacy*. Cambridge University Press.

Shay, S. (2017). *The axis of evil: Iran, Hizballah, and the Palestinian Terror*. Routledge.

Sheskin, D. J. (2020). *Handbook of parametric and nonparametric statistical procedures*. Chapman & Hall.

Simon, S. (2018). Iran and President Trump: What is the endgame? *Survival*, *60*(4), 7–20.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109.

Sniderman, P. M. (2018). Some advances in the design of survey experiments. *Annual Review of Political Science*, *21*(1), 259–275.

Starr, H. (2000). Substitutability in foreign policy: Theoretically central, empirically elusive. *Journal of Conflict Resolution*, *44*(1), 128–138.

Straub, J. (2019). Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios. *Technology in Society*, 59, 101177.

Tabatabai, A. M. (2020). After Soleimani: What's next for Iran's Quds force? *CTC Sentinel*, *13*(1), 28–33.

Tesler, M. (2020, January 4). Attacking Iran will not help Trump win reelection. Here's why. *The Washington Post*. www.washingtonpost.com/politics/2020/01/04/attacking-iran-wont-help-trump-win-reelection-heres-why/

Thompson, W., & Dreyer, D. (2011). *Handbook of international rivalries*. CQ Press.

Toft, M. D. (2014). Territory and war. *Journal of Peace Research*, *51*(2), 185–198.

Trevithick, J. (2019, June 20). *No easy decisions for U.S. over how to react to Iran shooting down navy drone*. The Drive. www.thedrive.com/the-war-zone/28626/no-easy-decisions-for-u-s-over-how-to-react-to-iran-shooting-down-navy-drone

Trump, D. (2018, May 8). *President Donald J. Trump is ending United States participation in an unacceptable Iran deal*. White House. www.whitehouse.gov/briefings-statements/president-donald-j-trump-ending-united-states-participation-unacceptable-iran-deal/

Valeriano, B. (2013). *Becoming rivals: The process of interstate rivalry development*. Routledge.

Valeriano, B., & Jensen, B. (2019, January 15). *The myth of the cyber offense: The case for cyber restraint*. Cato Institute. www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

Valeriano, B., & Jensen, B. (2019, June 25). How cyber operations can help manage crisis escalation with Iran. *The Washington Post*. www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

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

Valeriano, B., & Maness, R. C. (2015, May 13). The coming cyberspace: The normative argument against cyberwarfare. *Foreign Affairs*. www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace

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

Van Creveld, M. (2013). *Wargames: From gladiators to gigabytes*. Cambridge University Press.

Vavra, S. (2019, July 10). *Why cyber command's latest warning is a win for the government's information sharing efforts*. CyberScoop. www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/

Vasquez, J. A. (1993). *The war puzzle*. Cambridge University Press.

Vasquez, J. A., & Henehan, M. T. (2010). *Territory, war, and peace*. Routledge.

Wise, H. (2013). *Inside the danger zone: The US Military in the Persian Gulf, 1987–1988*. Naval Institute Press.

Wong, E., & Schmitt, E. (2019, April 8). Trump designates Iran's revolutionary guards a foreign terrorist group. *New York Times*. www.nytimes.com/2019/04/08/world/middleeast/trump-iran-revolutionary-guard-corps.html

Yee, V. (2019, May 13). Claim of attacks on 4 oil vessels raises tensions in the Middle East. *New York Times*. www.nytimes.com/2019/05/13/world/middleeast/saudi-arabia-oil-tanker-sabotage.html

Zaveri, M. (2020, February 10). More than 100 troops have brain injuries from Iran missile strike, Pentagon says. *New York Times*. www.nytimes.com/2020/02/10/world/middleeast/iraq-iran-brain-injuries.html

Zraick, K. (2020, January 3). What to know about the death of Iranian General Suleimani. *New York Times*. www.nytimes.com/2020/01/03/world/middleeast/suleimani-dead.html