Cyber Compellence: Applying Coercion in the Information Age

Benjamin M. Jensen
American University, School of International Service
Marine Corps University

Brandon Valeriano
Cardiff University
Marine Corps University

Ryan C. Maness
Northeastern University

Abstract

Coercive efforts originating from the cyber domain may be one of the most important strategic innovations in recent decades. According to some, cyber-attacks enable paralyzing first strikes with the potential to cripple an adversary. Yet, these claims may be premature since we know very little about the character of cyber strategies and the efficacy of cyber power empirically. This research addressed this gap through exploring compellence in the cyber domain. Examining an updated Dyadic Cyber Incident and Dispute Dataset (DCID), we review how state actors applied cyber instruments to coerce adversaries between 2000 to 2014 differentiating between cyber disruption, espionage, and degradation. We find that coercive cyber operations rarely prompt a concession in the target. Cyber disruption and espionage methods seem to achieve their goals of gathering intelligence and signaling through harassment, but do not result in an observable behavioral change in the target in the near-term. Only on limited occasion, usually associated with US activity in cyberspace, does cyber coercion, often in the form of degradation, result in concessions. The idea of quick victory in the cyber domain remains elusive.

Introduction

How do political actors apply cyber power in their strategic interactions? In July 2015, the United States government revealed that Chinese hackers stole the personal information of 21.5 million individuals targeting security clearance investigations (Davis 2015). In December 2015, the Associated Press reported evidence that the Iranian hackers stole sensitive information on at least 71 different power plants across the United States (Burke and Fahey 2015). Over the summer of 2016, Russian hackers conducted hacks that lead to leaks of embarrassing and confidential information to WikiLeaks in an effort to manipulate the U.S. election and undermine confidence in democracy (ODNI Report 2017).

Since 1991, a wide range of practitioner and scholarly perspectives emerged on how cyber operations would work as a form of coercion (Arquilla and Rondfeldt 1993; Libicki 1995; Szafranski 1995; Bunker 1996; Nye and Owens 1996; Gartzke and Lindsay 2015; Whyte 2016). Whether seen as revolutionary or limited, cyber capabilities create options for blinding an adversary's command and control infrastructure (Department of Defense 2013, 4). Cyber weapons are also thought to be low cost and secretive, giving the offensive state some degree of plausible deniability. They may even enable a paralyzing first-strike paralyzing against a country's political and economic systems (Liang and Xiangsui 1999; Lynn 2010; Peterson 2013, Singer and Friedman 2014). In the extreme, the diffusion of cyber capabilities heralds a new revolution in military affairs (Shakarian 2011; Domingo 2014).

Some analysts claim these cyber intrusions mark a revolutionary break in warfare with the potential for significant future changes in how conflicts are fought. The Head of New York State's Department of Financial Services warned that a "cyber 9/11" directed at Wall Street firms could spill over into the broader economy causing a crisis as deep as the 2008 mortgage meltdown. In a 2012 speech, then Secretary of Defense Leon Panetta warned of a "cyber Pearl Harbor" that "would paralyze and shock the nation", since then this term has become near ubiquitous in the discourse (Lawson et. al. 2016).

Echoing these fears, numerous scholars foresee a world where cyber power is the dominant coercive instrument used by political actors, even suggesting that there is an ongoing cyber revolution that doesn't fit within existing models of interstate war and statecraft (Nye 2010; Kello 2013). Brenner (2015: 191) highlights significant "vulnerabilities in U.S. civilian networks to the exercise of national power." Citing the offense-defense balance debate (Jervis 1978), other scholars see cyber capabilities as offense dominant and likely to trigger great power security dilemmas and crisis instability (Goldstein 2013; Saltzman 2013; Gompert and Libicki 2014).

Contrasting these perspectives, some scholars point to a different future where cyber power is one of many coercive instruments used short of war for limited objectives. Gartzke (2013) and Gartzke and Lindsay (2015) argue against viewing cyber intrusions through the offense-defense balance lens and question the strategic effectiveness of the instrument. In particular, Lindsay (2015) sees future cyber exchanges conforming to a modified stability-instability paradox in which a fear of military retaliation and need to maintain internet connectivity curb crisis escalation processes. Following this, Valeriano and Maness (2015) demonstrate empirically that our recent cyber history displays much more restraint that would be expected given the tone of the discourse.

The utility of cyber operations is open to debate. The Chinese OPM hack gained significant intelligence, but being able to use this information is a whole other consideration

given that the defender is aware of the theft and technical challenges associated with processing millions of files. The shock value and surprise advantage of cyber operations may also be overblown. At this stage, every government agency and critical infrastructure partner knows they are a target and invests in cyber defenses. Military exercises in multiple countries factor potential cyber effects through degraded command and control as well as GPS disruptions that might come with war onset.

We theorize that cyber power, defined as "the ability to control and apply forms of control and domination of cyberspace" (Nye 2010; Valeraino and Maness 2015: 28) is like any other technological innovation in strategic competition and warfare. It can alter calculus of conflict but impact depends on the method, target, and goals. In fact, cyber appears to have only limited coercive potential.

We examine the empirical bounds of our theory by analyzing an updated version of the Dyadic Cyber Incident and Dispute Dataset (DCID Version 1.5) providing a macro view of the outcomes of publicly documented cyber conflict between rivals in the international system from the years 2000 to 2014 (Maness and Valeriano 2017). While there are host of cyber incidents that remain concealed, these public incidents reflect a representative sample of the larger population. New additions to the data allow us to parse out each action and assess the impact of the operations in the cyber domain. Based on initial observations, cyber operations, to date, have limited coercive potential. They rarely result in a target concession. The power of cyber may lie in the future more than the present as a form of signaling that alters future crisis interaction.

The remainder of the article proceeds as follows. First, we situate cyber power in the larger literature on coercion and coercive diplomacy to situate the concept of cyber compellence. Specifically, we introduce three forms of cyber coercion: disruption, espionage (i.e., altering information asymmetries), and degradation. Next, we introduce our empirical methodology detailing how we collected data on cyber events and coding them in a manner that enables an assessment of coercive outcomes. Third, we examine cyber coercion in its international context by analyzing a representative sample of all state-initiated cyber compellent acts. Based on this analysis, cyber tactics appears best suited for limited disruption and intelligence objectives. In line with earlier coercion studies, there is no single-domain decisive "victory" through compellence if the goal is to alter the behavior of the defender.

Cyber Coercion

Coercion is the use of threats and other associated actions to alter behavior (Schelling 1966; George 1991; Byman and Waxman 2002). It is more potential than actual force, taking minimal action to alter the cost-benefit calculation of an adversary short of using "brute" force (Schelling 1966). The goal of coercion is to change the behavior of states by manipulating the costs and benefits of action (Pape 1996: 80). Given this, cyber coercion reflects efforts to change the behavior of an actor by attacking digital targets, information, or networked installations. Conventional coercion seeks to exploit weaknesses in the target and force the opponent to back down by making successful action infeasible (Pape 1996: 43). Cyber coercion can take this form as well as efforts to exploit information asymmetries are a means of forcing the opponent to change behavior.

Forms of coercion vary in relation to their objective (Schelling 1960; 1966, 69-91). As a negative action, coercion is the "power to hurt," a signal or the limited use of force of escalating

damage that pushes the opponent to yield.[1] Leaders optimize coercive strategies to influence a decision-making process as opposed to achieving decisive battlefield outcomes. They develop punishment, risk and denial strategies that often reinforce other instruments of power (Pape 1996; Overy 1996; Mueller 1998; Byman and Waxman 1999, 2000). Deterrent coercive measures preserve the status quo by dissuading an adversary from adopting a threatening strategy by escalating costs. Compellent coercive measures seek to change the status quo by altering an adversary's behavior through punishment and denial strategies.

There is a long history of the limited use of coercion in diplomatic practice. According to Lebow (2007), Thucydides documented ten attempts at deterrence and compellence in the Peloponnesian War that tended to fail, leading to provocation and escalation. Chandragupta (340 – 297 BCE) and his adviser Kautilya used coercive threats to build the Mauryan Empire (Modelski 1964). After the rise of Augustus, the Romans used what would today be called forward-deployed forces as a coercive instrument to threaten rivals (Campbell 2001). In the modern era, Cable (1981) outlined the practice of gunboat diplomacy and using displays of naval power in diplomatic crises. Lebow (1984) mapped twenty pre-World War II crises, each of which involved multiple coercive signals and threats, showing the often contingent nature of crises.

After the Berlin Airlift and Cuban Missile crises, debates about the use of coercive threats and strategic bargaining shaped the Cold War and deterrence strategies (George and Smoke 1974, Jervis 1979, Huth and Russett 1990). More recently, scholars examined terrorism as coercive instrument (Pape 2003, Kydd and Walter 2002, 2006, Abrahms 2006, 2012). This work has pushed us to consider alternative forms of action as success in changing the behavior of target is more likely when the opposition uses non-violent strategies as opposed to kinetic violence (Cheneweth and Stephan 2011).

For George (1991), there are multiple forms of coercion that can compel an adversary to act in a favorable manner. Blackmail, which he relates to Schelling's concept of compellence, is the use of threats to force an adversary to "give up something of value without putting up resistance" (George 1991, 5). In contrast, coercive diplomacy uses a mix of diplomatic instruments to signal the costs of a continued, hostile course of action while showing positive benefits of an alternative policy. In this study, we focus on compellence, seeking to determine the efficacy of cyber compellent strategies designed to either punish an actor or create asymmetries in information.

Leaders optimize compellence strategies by developing punishment, risk, and denial strategies that often reinforce other instruments of power (Pape 1996). Punishment strategies can succeed if the opposition only has a minor interest in the outcome. Risk strategies similarly fail since they are diluted punishment options. Though not traditionally factored, information asymmetries gained through espionage can be a form of risk-based coercion. Beyond their intrinsic intelligence value, these asymmetries change the probability of successful coercion in future episodes and thus operate like traditional risk strategies but in the cyber domain. Echoing Sun Tzu's maxim that the highest form of strategy is attack the enemy's plan, denial tends to be a superior approach by degrading a targets ability to achieve their objectives (Pape 1996).

Cyber capabilities reflect a form of power that gives it user, "the ability to control and apply typical forms of control and domination of cyberspace" (Valeriano and Maness 2015: 28).

[1] In this work, we do not distinguish between cyber as a signal or cyber as the limited use of force. Because we cannot know whether or not actors intended the attack to be a signal, we treat cyber coercion as more the limited use of force.

As an instrument of power, cyber may have limited coercive potential if it fails to achieve denial or punishment, which would alter behavior by changing either the calculation of cost in the future or imposing costs at the moment. This characterization is line with Gartzke and Lindsay (2016) who note that "the potential of cyberspace is more limited than generally appreciated, but it is not negligible, especially when exploited in conjunction with other forms of power such as military force." States are more likely to reach their policy ends when they integrate cyber power alongside economic sanctions, broader diplomatic campaigns and/or the limited use of coercive airpower (Byman and Waxman 2000, 11-13). Cyber coercion likely does not achieve effects in isolation, challenging the discourse on cyber warfare that characterizes the domain as decisive. Yet, before scholars and practitioners can assess the cumulative coercive potential of cyber alongside other instruments of power, we need a clear assessment of the intrinsic coercive potential cyber power offers. This research gap drives our study since we know little about the empirical realities of cyber coercion.

The application of punishment, risk and denial approaches in the cyber domain implies integrating computer network attack and exploitation to alter an adversary's behavior either short of war or as part of a larger military/diplomatic campaign. In many respects, coercion has always involved information in the form of the signaling. Cyber, dealing with networks of distributed information in the form of code, extends these coercive, predominantly compellent, approaches to a new domain. [2]

Cyber Compellence Strategies

Cyber compellence as a strategy can take multiple forms. First, cyber compellence can take the form of punishment. Coercion by punishment "operates by raising the costs or risks to civilian population" (Pape 1996: 13). Attacks could include events that limit internet connectivity society wide, such as the Russian denial of service attacks against Estonia and Georgia in 2007 and 2008, respectively. Punishment strategies in cyberspace could also take the form of disruptive operations that temporarily take out the opposition's ability to communicate and present information. Simple website defacements on strategic networks could achieve this goal. While the attacks tend to not very severe and are easily eradicated, they can still be an effective form of signaling to an enemy of things to come if they do not change behavior.

Second, cyber compellence can take the form of manipulating information asymmetries, which is analogous to risk strategies in Pape (1996). As a form of punishment, risk strategies seek to alter the projected utility of future coercive exchanges by gaining a position of relative advantage. In their original articulation, Pape argued that risk strategies "raise the probability of suffering costs" (Pape 1996, 18). These operations seek to coerce in increments, holding at risk something the target values and promising future action as a means of changing the utility of further resistance (Pape 1996, 18-19).

A risk-oriented approach to coercion in the cyber domain involves manipulating information and creating asymmetries that can be exploited in future strategic exchanges both in the cyberspace and conventional domains. In a competitive bargaining situation, each actor has private information that alters strategic interaction (Fearon 1995). There is some information, such as their relative power, that they wish to conceal. There is other information (e.g., the

[2] In the United States military and intelligence communities' cyber is a domain, like land, sea or air. For a definition of these domains, see Chairman of the Joint Chiefs of Staff, JP 1-02 "Department of Defense Dictionary of Military and Associated Terms." Available at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

characteristics of a particular weapon system, the numbers of high value systems in their inventory) that they wish to exaggerate. Consistent with bargaining theory, deception and bluffing have coercive potential.

In a crisis, actors engage in careful perception management, including creating information asymmetries through denial and deception as they seek to force concession. This is *manipulation of information* in that it alters the projected utility of future coercive exchanges by gaining an information-based position of advantage. With cyber, this form of manipulating information asymmetries also takes the form of theft, blackmail, and outright destruction. Computer network exploitation methods can steal plans for future weapon systems like the F-35 fighter schematics, or be used to release damaging information such as through WikiLeaks. In this frame, manipulation of information is a form of espionage and deception (Gartzke and Lindsay 2015), which has the potential to spiral, escalating tensions and possibly creating new conflicts.

Finally, cyber coercion can take the form of degradation. Cyber degradation is analogous to denial. Coercion by denial implies a strategy that seeks to "prevent the target from attaining its political objective" (Pape 1996: 13). In 1982, the CIA supposedly executed a covert action operation, Line X, adding a logic bomb to software they knew the Soviets would steal. The result was a massive explosion that destroyed segments of the Trans-Siberian pipeline and made the Soviets more cautious in attempting to steal future technology (Reed 2005). In addition to sabotage, cyber compellence by denial includes degrading infrastructure and blinding adversaries. Examples include the threatening of critical infrastructure, such as Iranian attempts to target the Saudi Arabia national oil company (Bronk and Tikk-Ringas 2013). Similarly, the targets can be economic or entertainment sectors as seen in the attacks against Sony (2014). The greatest threat from the denial track is the idea of a "cyber 9/11", an attack on domestic crucial infrastructure that is so violent that it obliterates civilian systems such as dams, power plants, or nuclear facilities.

In Pape's (1996) original conceptualization of coercive airpower, he distinguishes among approaches based on the target. Punishment strategies target civilian populations. Risk strategies target civilian populations and use force in an escalating manner. Alternatively, denial strategies target the military, not civilians, and seek to deny the target from achieving an objective. All three approaches are compellent in that they seek to alter the behavior of the target. Pape (1996) finds that denial strategies tend to have a higher success rate in generating concessions.

While we build on the concepts of punish, risk and deny, we note that important difference in cyber operations than prevents our categorization of each incident in such a strict manner. Cyber operations seeking to punish can target both civilians and the government. Denial strategies, in the form of cyber degradation, can target civilians, the most likely objective, because they may seek to sway opinion in target populations or restrict access. In cyber operations, there is no responsibility by the government to protect the civilian industry before or during an attack unless it is defined as critical infrastructure. Risk in cyber operations generally target government contractors and the military, rather than civilians as these actors have information of value.

Coercion and Effectiveness

Assessing whether cyber capabilities herald a disruptive change in the character of war or simply extend military coercion to a new domain is a central question for scholars and

practitioners. The work we undertake here is critical in beginning to answer the central question about the utility of any weapon, tactic, or method of influence - *does it work*? The utility of any coercive instrument is determined by whether or not 1) it actually succeeded (i.e., did the initiator meet the initial objective to disrupt, conduct espionage, or degrade) and 2) whether or not the successful attack caused a concession in the target (i.e., identifiable behavior change).

For Schelling (1960, 1966), increasing the costs of resistance causes the target to concede. In cyber operations, concession can take a very different path, especially if one considers that most states operate from a position of weakness and attacks exposing vulnerabilities may harden the target in the future. Escalating costs will certainly have a breaking point where a concession is made, but in cyber operations costs might be useful in exposing and patching vulnerabilities much in the same way that companies will employee white hat hackers (friendlies) to expose weaknesses. Deception (Gartzke and Lindsay 2016) and resilience are keys to survival in cyber security, altering the calculation between costs and concessions in favor of the target. It is also important to note that many forms of coercion are about future interactions more than they are about current interactions. That is, the concession may occur in future bargaining situations.

Previous studies on the effectiveness of U.S. coercive diplomacy campaigns suggests that coercion "works" between 19 and 30 percent of the time (Blechman and Kaplan 1978; Art and Cronin 2003; George and Simons 2004; Sescher 2010; Horowitz 2010). Sescher (2010) argues powerful actors often find coercive diplomatic campaigns less effective because assessments of military power interfere with the ability to estimate resolve leading to suboptimal crisis outcomes. Powerful actors over estimate their own capabilities and discount the ability of weaker actors to endure pain, a similar logic which might apply to cyber.

Actor motivation (including fear, honor, and salience) can determine the relative impact or failure of coercion. Almost all episodes of compellence reviewed in Thucydides end in failure highlighting two important aspects of coercion, "the widespread belief that others can be dissuaded or persuaded by credible threats based on superior military capability; and 2) the propensity of people who are the targets of threats to downplay risks and costs when it is contrary to their desires or needs" (Lebow 1984: 170). Similarly, Missiou-Ladi (1987) finds that five seminal cases of compellent threats by Sparta all failed despite the military imbalance due to the targets ideological motivation and willingness to pay short term costs in blood and treasure to preserve long-term strategic advantages. In theory, the use of cyber capabilities should demonstrate the same difficulty in utilizing coercive threats. There is limited coercive potential when trying to change an actor's behavior depending on the issue and the target's willingness to suffer costs.

Multiple intervening and antecedent conditions affect efforts to coerce an adversary. Regime type can create audience costs or domestic blowback from backing down in a crisis (Fearon 1994; Weeks 2008). Past crisis behavior and the survival interests of the weaker party can alter rational crisis bargaining (Press 2005; Haun 2015). Costly signals can reveal the actor's willingness to risk escalating a crisis into war and their level of commitment either moderating or maximizing coercive attempts (Fearon 1997).

Abrahms' (2006, 2012) work is illustrative of the exploration of coercion from the frame of an alternative and non-conventional tactic, terrorism. Terrorism is a strategic signal (Kydd and Walter 2006) where Abrahms (2006) finds that although terrorism, on some levels succeeds in combat effectiveness (i.e., causing causalities), yet the overwhelming majority of terrorist attacks fail at the strategic level. Of the 42 terrorist attacks in the Abrahms' study, less than ten percent

actually achieve their strategic political objectives. Similar to Pape's denial strategy, Abrahms (2012) also finds that when terrorists target military over civilian victims, the political objectives of the group are much more successful.

Statements by pundits and scholars alike have pointed to the demonstrated efficacy of cyber tactics. Singer notes, "cyberweapons have proven their value in espionage, sabotage, and conflict. And the digital domain will be as crucial to warfare in the 21st century as operations on land, air, and sea" (Singer 2015). Our expectation is the opposite, cyber coercion as an effective instrument that can alter behavior through degrading and denial is dubious given the history of compellence. Compellence is difficult. Leveraging new weapons to compel may prove even more difficult.

Gartzke and Lindsay (2015: 325) offer an important starting point by noting that "offense dominance may exist only for nuisance attacks that are rarely strategically significant, such as piracy, espionage, or "hacktivist" protests." In examining the history cyber incidents, we note that what might be termed severe cyber actions are rare and often strategically insignificant when put into proper context (Valeriano and Maness 2014). Borghard and Lonergan (2016) note that attrition, denial, and decapitation cyber strategies might be effective, but punishment and risk operations are less likely to achieve results.

We expect that cyber compellence designed as denial or degrade is difficult and will rarely have a meaningful impact. As Gartzke (2013: 57) notes, "harm inflicted over the internet or any other medium will matter politically when it alters the subsequent balance of power, or when it indicates enemy capabilities that must be taken into account in future plans. Because cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted will have a short-term impact on its targets." Important military targets like American and Israeli military networks are hardened. Therefore, using cyber compellent efforts to alter the behavior of the enemy will often be limited and ineffective. Actor resolve still matters, using cyber compellence to exploit information asymmetries (i.e., espionage) or cause disruptions is likely to be operationally successful (i.e., achieves initial objective) but also will have a limited impact at the strategic level (i.e., produces concessions). Cyber might be more a demonstration effect or, in the extreme, death by a thousand cuts, rather than a quick method to achieve diplomatic of battlefield impact.

Research Design and Hypotheses

Measuring Cyber Coercion

The approach here is to survey the entirety of the known incidents that involve the use of cyber technology for malevolent purposes between states in a specific domain. While there is always some uncertainty about cataloging conflict events of any sort, this problem is multiplied in the cyber domain where most actions are thought to be secret. In fact, most cyber operations do not remain secret after a time given the intense media interest in the topic, the need for governments to justify their budgets no matter what system they operate in, and the plethora of cyber security firms trying to justify their detection capabilities. To that end, an early study collected an extensive amount of data regarding cyber conflict between rival states from the years 2001 to 2011 (Valeriano and Maness 2014) and this method has been extended here.[3]

[3] Machine learning methods could be used to scrape new corpuses for data, but this method is unreliable without human coders supporting the effect to insure the cases coded are attributable, code the specific variables needed for

While any examination will miss cases and sources, this data snapshot represents a focused, reliable, and verified method of examination part of the universe of cyber operations.[4] Rival states (Diehl and Goertz 2001) are utilized since this subsample of states is the most conflict prone, likely to utilize cyber tactics, and represents an achievable data collection strategy (Valeriano and Maness 2012).

The data utilized here represents a clear advance on the DCID version 1.0 in that we expand the coding to include outcomes, strategies, and new actors (Valeriano and Maness 2014). While the focus remains on rival states given our general inability to code all state actions, we also include conceptions of critical national security targets that are not specifically agents of the states. More importantly for this analysis, version 1.5 of the data includes the coding of interactions from 2000 to 2014 with the specific intent of consideration goals of operations, the achievement of objectives, and whether targets were compelled to change their behavior as a result (see Appendix A).

The DCID version 1.5 utilizes 126 rival state pairs that are extracted from the Klein, Diehl and Goertz (2006) enduring rival dataset as well as Thompson's (2001) strategic rival dataset including 165 incidents within 51 disputes.[5] The initiation must come from the government or there must be evidence that an incident was government sanctioned. For the target state, the target must be a government entity, either military or non-military or a private entity that is part of the target state's national security apparatus (i.e., power grids, defense contractors, and security companies), or an important multinational corporation. Non-state actors or entities can be targets but not initiators as long as they are critical to state based systems (DHS 2016).

The coding method specifically follows the Correlates of War procedures in examining sources throughout history, in the media, and, new for cyber conflict, from government or critical cyber security firm reports. Most incidents and disputes must be verified and attributed using more detailed sources such as cyber security company reports, long form investigative reporting, and government policy reports.

To be counted as an incident, an event requires the manipulation of code or hardware for malicious purposes.[6] For the purposes of this study, we coded goals and intent based on the political objectives for each cyber incident initiated by states. *Cyber disruption* operations are low-cost, low-pain initiatives that harass a target to change their decision calculus. Examples of cyber disruptions include DDoS attacks or defacements of high profile government webpages, or escalating risk by hacking in financial services networks via Trojans, viruses, or worms that are simple to design, easy to employ, require limited resources, and have short term goals. Cyber disruptions are typically short duration operations that do not invest extensive resources.

Cyber disruptions upset some aspect of the target's presence and posture in cyberspace as a means of signaling. Specifically, they can be thought of as bargaining efforts designed to signal that a particular course of action is undesirable to the initiator. In this respect, the attack signals

---

our analysis, and to avoid duplication. Such an effort would require a massive amount of funding that is yet unavailable.

[4] Our data is subjective (as is most data) but we set out to minimize this with overlapping coding efforts, full rechecks by the primary authors, and support from a collection of cyber scholars. This research is an example of a representative sample of incidents and disputes and future coding efforts will seek to continue to flesh out these questions and provide more data as incidents occur. The outcomes of the disputes are defined by our criteria and reinforced by multiple coder reliability checks and advice from the cyber security research community.

[5] For a complete overview of the dataset, the codebook and data are available at drryanmaness.wix.com/irprof.

[6] Electronic manipulation such as electromagnetic pulses and radar jamming either damage or destroy circuitry through radio waves and/or directed energy are not included.

the ability to inflict future pain, makes the target question their network security, and casts a shadow of the future. The target, knowing they will interact with the probable initiator in the future, may alter their decision calculus. Cyber disruptions meet their objective if they successfully disrupt some aspect of the target's network. For example, during the 2008 Russian invasion of the Georgian separatist region of South Ossetia, widespread defacements plagued the Georgian government's websites for a time in order to sow confusion in the government and larger populace. The damage is usually not severe enough to cause long-term damage. Cyber disruptions produce concessions if there is an observable change in the target's desired behavior. Given that cyber disruptions are low-cost, low-pain the probability of a behavior change is low.

Cyber espionage operations are efforts to alter the balance of information in a manner that produces bargaining benefits. These benefits may be long-term material components of military power, such as stealing the plans for the F-35, or they may involve short to midterm critical information such as the identities of covert operatives in conflict zones. Consistent with bargaining theory (Schelling 1962), by deceit or bluff you can create information asymmetries that increase the costs of resistance and increase the probability that you can coerce the target. Cyber espionage operations are often low cost, low risk in that escalation tends to be contained to the espionage domain but increasingly states are employing the information they use to coerce the opposition. Cyber espionage operations can include activities ranging from Trojans, viruses, worms, and keystroke logs to achieve their objective.

Cyber degradations are higher cost, higher pain inducing efforts that seek to degrade or destroy some aspect of the targets cyberspace networks, operations, or functions. These operations destabilize the target, highlighting critical vulnerabilities and pushing them onto a defensive footing that limits their ability to respond to a crisis. These operations tend to involve more sophisticated, viruses, worms, and logic bombs.

These forms of coercion are potentially compellent in that they seek to alter the behavior of a target in either the present or future. That said, the degree of behavioral change varies. Disruptions are really a low-cost signaling mechanisms designed to indicate the risk of escalating costs in future interactions. Espionage is about manipulating the balance of information in the attacker's favor for political, economic, or military advantage at a future date. Stealing intellectual property, military strategy secrets, or non-military government information are examples of this tactic, but deception operations that might include honeypots and altering of information will be operations seeking to encourage the defender to back down. Degradation operations are high-cost and also appropriately more difficult in that the targets are more substantial (nuclear facilities, power plants, military networks). Deterrent operations are possible but also very rare empirically since displaying cyber capabilities is rare (Maness and Valeriano 2016). Generally, a state will conduct cyber operations to persuade or increase access to information rather than to dissuade one from taking action in the present. Preventing action through cyber tactics is difficult because states cannot display capabilities, which limits credibility of threats and extreme vulnerabilities in target states.

Hypotheses

Some argue that cyber power and its utilization is revolutionary, and the use of cyber instruments of power tends to achieve the objective ends (Clarke and Knake 2010). If this is the case, we would see concessions in the data collected. The null hypothesis is that the application of cyber power in documented cyber incidents does not compel targets into changing their

behavior as a result of the cyber action. There would be no observable change in the targeted actor's behavior across a number of cases. We assess this hypothesis by seeing if there is a statistical evidence for either rejecting or upholding the null hypothesis between different applications (disrupt, espionage, degrade) of cyber power and the inferred objective as well as whether or not there was a concession and observable behavioral change. This leads us to the first of our hypotheses:

H1: The application of cyber power is sufficient but not necessary to alter the behavior of the targeted state and extract concessions.

We hypothesize that cyber power is effective regardless of the form. That is, it usually is succeeds in infiltrating a target's network more often than not even if it does not ultimately generate a concession. We assess this hypothesis by determining whether or not there was variation between the form of cyber power and the inferred successful breach (or failure) as well as if the target state conceded to the attacking side in some way, leading us to our second hypothesis. Cyber power is an important dimension of modern statecraft but it may not be as revolutionary or decisive as pundits claim. It may only be suitable for limited objectives, such as temporary disruption events that sow chaos or espionage attacks seeking information.

H2: The application of cyber disruption and espionage events achieve only limited objectives and often fails to extract concessions.

Going further, the three objective methods of cyber coercion may have differential rates regarding successful breach rates as well as behavioral change rates. Disruptions, which have low-costs and limited objectives, may have more success but little impact on the behavior of targeted states. Defacement or denial of service techniques against government networks and websites could evoke a response but not be compellent in terms of a concessionary response in the target; the probability of behavior change is low given limited objectives. Similarly, as the objectives of espionage campaigns are to steal sensitive information from adversaries are deceptive, the successful breach rate should be relatively high, however a concession may never occur. Turning stolen information into competitive advantage will be delayed as the information is processed or the initiator waits for the right time to use the information against the target to maximize coercive potential.

H3: Cyber coercion strategies involving degradation methods will be relatively more effective in the behavioral change of states

Contrary to the easier to initiate, cyber coercive methods with the intent to degrade a state by raising the costs may see more success. Degradation strategies require a higher level of impact on the target. That is, they require that the specific target in question be disabled or destroyed for extended periods of time so that the government capitulates to the demands of the initiating state. In a domain with low costs of entry, completely denying the target of its objectives is a very difficult goal in the cyber realm. Therefore, degradation strategies must be stealthy, sophisticated, and, require much planning before the incident is launched, and may have a lower probability of infiltrating the target, but if it does, it will have a higher probability of changing the behavior of a target state.

There are two outcome variables in this analysis. The first variable measures if the objectives of the initiating states are met. This is defined as the accomplishment of the basic goals of operation. For example, if the operation was an intelligence operation, were the plans stolen? If the incident was a disruptive effort, such as a DDoS attack, were the target networks shut down? Was the target compromised? Did the degradation-style attack breach the network and destroy files or industrial control systems beyond repair? If the operation was thwarted, who stopped it and how? These were the questions that were asked during the coding of these variables. If there was a successful breach of the target network, we code this outcome variable as "1", a "0" is coded if the effort was blocked or thwarted by the target state.

The second dependent variable measures concession: a change of behavior in the target state. For success to be coded, a political or military objective must be achieved, not simply a change such as increasing cyber security provisions. For example, if the goal of the Estonian hacks in 2007 was to alter Estonian behavior leading to respect for ethnic Russians, did the hack achieve this? An outcome for this variable is coded as "1" if it there was an observable concessionary behavioral change, "0" if there was not.

The use of binary, conditional codes is an established, even if problematic, practice in studying coercion (Huth, Gelpi, and Bennett 1993; Sescher 2011). Critics note that binary approaches that code a compellent case "success" or "failure" may not capture, "the complex and often subtle effects of coercive threats" or the ways in which coercion can backfire (Byman and Waxman 2000, 13-14).[7] Yet, in order to measure the efficacy of cyber power, each episode needs to be coded with respect to its inferred strategy and whether or not that coercive approach met its desired objective as well as had a concessionary effect on its target. This question of intent is compounded in cyber where the attacker often masks their effort. To overcome these challenges, the study relied on three independent coders and the results were reviewed by military practitioners who either had joint operational planning experience or worked at one point with cyber capabilities.[8]

As all our independent and dependent variables are categorical, cross-tabulation and chi-squared tests are appropriate. Cross-tabulations assume normal distributions and produce null-hypotheses based on expected values that are normally distributed. If the data in the sample deviate from the norm at the 95 percent confidence-level, that is if there is a significant difference between the expected and observed values, then these null hypotheses are rejected.

---

[7] An alternative approach advocated by Byman and Waxman is to analyze coercion outcomes in a, "as a marginal change in probability of behavior," (2000, 14).

[8] Rigorous coding was undertaken to investigation the reliability of our coding of the compellence variables. Experts from the Professional Military Education (both students and Professors) system were recruited to help with the subjective coding of the variables. Objective achievement and concessions can be very by the individual, therefore getting reliable variable coding is paramount. We held multiple sessions where coding was done independently and then majority opinion decided on the variables' values. Intercoder reliability tests were then estimated to establish the success of our efforts in ensuring trust and verification of the coding effort. For the objective achievement dependent variable, we obtained a Fleiss' Kappa score of .496. Fleiss' Kappa test are appropriate for intercoder reliability when there are three or more coders. This score can be interpreted as finding to what extent the observed amount of agreement among raters exceeds what would be expected if all raters made their ratings completely randomly. The score of .496 denotes moderate agreement, which is to be expected as there were 15 different coders involved in this effort. For the concessionary behavioral change dependent variable, we obtained a .497 Fleiss' Kappa score using the same amount of coders, which is also within the moderate threshold. For the independent variables of compellence type, the three authors code these variables repeatedly and then came to agreement on the final values, obtaining a substantial agreement Fleiss' Kappa score of .759

Chi-squared tests measure the 'goodness of fit' of an observed sample of variables and also assume normality.[9]

It should be remembered that here we are concerned with political, diplomatic, or military impact and victory as it relates to independent cyber actions.[10] This conceptualization is very technical as it does not focus on likely mythical idea of net warfare being able to completely dismantle and disable an enemy, but rather on the dynamics of the manipulation of information as used by cyber opponents. Our conceptualization also goes beyond technical impact. While Stuxnet was an effective technological operation in terms of implementation and delivery, taking a step back and exploring the political and diplomatic impact of the operation is the task we are faced with here.

Findings

Figure 1 breaks down each type of coercive method initiated by rival states from the years 2000 to 2014.[11] Overall there has been a rise in cyber incidents since the turn of the century, with various peaks and valleys. While cyber incidents are increasing, this increase appears to be directly correlated with espionage and disruption campaigns, not the more malicious degradation activities that many fear. In fact, currently the only type of cyber coercion on the rise is espionage.

The findings show an early spike in operations around 2001. Cyber operations appear to hold steady until a dramatic spike in 2008 after the Russian operation against Estonia. We also witness another spike around the Stuxnet operation, likely indicating the erosion of norms against the non-use of cyber operations around 2011 with a dramatic fall in 2012. After 2013 seems to highlight a new era of espionage operations including the OPM hack by China. The US response was to in some ways to suggest that these sorts of operations were expected and the normal course for espionage - escalating under a December 2015 agreement between China and the United States to limit cyber espionage for industrial purposes.

[9] A chi-squared score measures the overall difference between the expected values and observed values of all categories in a nonparametric sample. The null hypothesis is rejected if the chi-squared score is significant at the 95 percent confidence-level or higher. Given that there are a limited number of cases under consideration, more advanced statistical analysis is not possible given issues under consideration.

[10] Whether the inferred impact was the result of compounding dilemmas emerging from other actions is beyond the scope of the current research.

[11] This analysis is confined to the impact of individual cyber coercive incidents and does not include overall cyber disputes or campaigns that would contain multiple incidents. It would be difficult to objectively measure the impact of disputes with multiple incidents. For example, the Olympic Games dispute between the United States and Iran contained impactful espionage campaigns, Flame and Duqu, which led to the intelligence to launch the Stuxnet worm into Iran's nuclear network.

Figure 1: Yearly Cyber Incidents, Coercive Intent: 2000-2014

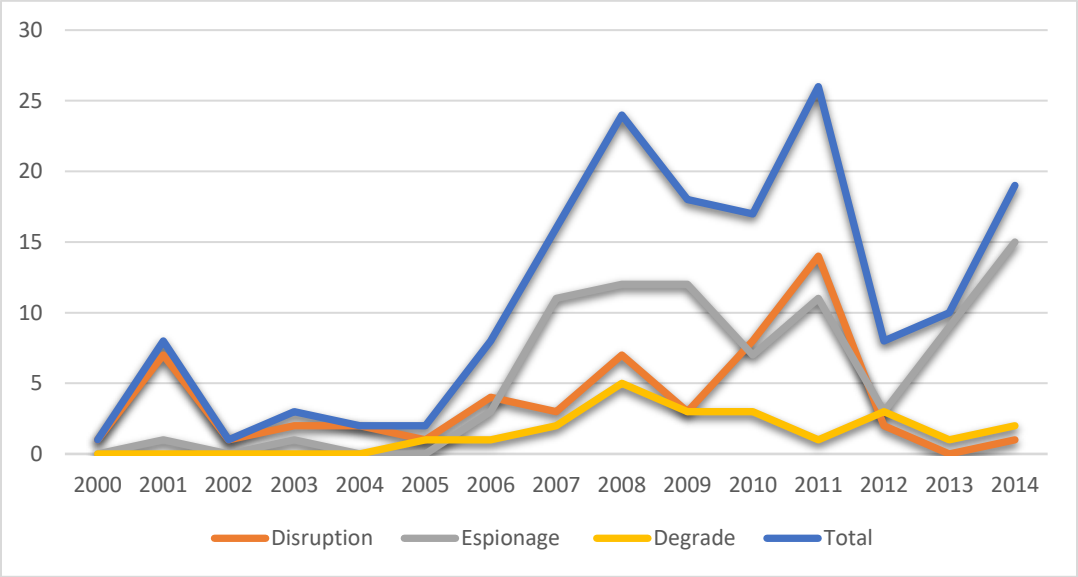

Table 1 summarizes each initiating states' cyber incidents by coercive method and whether or not the cyber action successfully achieved the goals of the operation and if a concessionary behavioral change occurred for the years 2000-2014. Here we consider the total number of operations initiated along with figures regarding success and behavioral change. Overall, regarding cyber coercion methods and the rate of success in terms of breaching the networks of targets, all three methods succeed at the levels of expectation using cross-tabulation methods and a chi-squared analysis. In terms of the objective being met, that is, whether the cyber attempt breached the network of the intended target, the success rate for all three categories do so at the expected frequency. The null hypothesis for objective achievement for all three coercive categories cannot be rejected therefore.

Regarding concessions as a result of a cyber coercive incident, Table 1 shows the cross-tabulation analysis that measures the difference between the actual counts of each political objective's concessionary success rate against the expected counts. The null hypothesis for espionage fails to be falsified, implying that this coercive measure succeeds at about the expected rate. However, disruptive techniques, which have a zero-success rate, should have succeeded at least four times according to expected values, and this is significant at the 99 percent confidence level. Degradation techniques succeed over four times more than expected, and this is also significant at the 99 percent confidence level.

Table 1: Crosstabulations of Cyber Objectives, Success, and Concessions

			Concession		Objective Met?	
			No	Yes	No	Yes
Cyber objective	Disruption	Count	56	0	7	49
		Expected Count	51.6	4.4	8.5	47.5
		z-score	0.6	-2.1**	-0.5	0.2
	Espionage	Count	81	5	12	74

		Expected Count	79.2	6.8	13	73
		z-score	0.2	-0.7	-0.3	0.1
	Degrade	Count	15	8	6	17
		Expected Count	21.2	1.8	3.5	19.5
		z-score	-1.3	4.6***	1.3	-0.6
Total		Count	152	13	25	140
		Expected Count	152.0	13.0	25.0	140.0

***** p < .001, ** p < .01**

Table 2 breaks down the data by dyadic composition, allowing to get a sense of dynamics by case. What is important for our analysis is the breakdown according to type which include disruption (harassment), espionage (manipulation), and degradation (denial) of military or public targets. We find that all coercive categories have high success rates in breaching the networks of their targets, with disruptions at a success rate of 88 percent, espionage at 86 percent, and degradation at a lower success rate of 74 percent.[12] These findings show how cyber tactics' low cost of entry and current offensive advantage equate to impressive successful breaches against state targets. When it comes to changing behavior in the target, the success rates are not very impressive. No disruptive cyber tactics have evoked an observable behavioral change, and espionage tactics have only evoked five cases of behavior change (only six percent of all attempts). What is interesting is that three of these cases were counter-espionage operations where deceptive tactics were used to compel the target to cease their own espionage operations.

Although degradation methods are generally less successful, costlier, and requiring a significant investment of time and resources these cyber coercive measures are able to evoke a concessionary behavioral change in 30 percent of cases (seven of 23). While success in changing behavior can occur, it should be clear these are not the easy and quick operations that many predict would come with cyber operations, but rather long term strategic operations always used in conjunction with conventional methods.

Table 2: Successful and Concessionary Cyber Measures by Initiating State, 2000-2014

Country	All Coercion Success	All Coercion Conc	Coercion Attempts	Disr Success	Disr Conc	Disr Attempts	Esp Success	Esp Conc	Esp Attempts	Degrade Success	Degrade Conc	Degrade Attempts
China	56 (92%)	1 (2%)	**61**	11 (100%)	0 (0%)	**11**	44 (92%)	1 (2%)	**48**	0 (0%)	0 (0%)	**2**
Russia	12 (67%)	0 (0%)	**18**	4 (80%)	0 (0%)	**5**	4 (67%)	0 (0%)	**6**	5 (71%)	0 (0%)	**7**
United States	15 (88%)	7 (39%)	**17**	0 (0%)	0 (0%)	**0**	9 (90%)	3 (30%)	**10**	6 (86%)	4 (57%)	**7**
N. Korea	15 (94%)	1 (6%)	**16**	10 (100%)	0 (0%)	**10**	2 (67%)	0 (0%)	**3**	2 (67%)	1 (33%)	**3**
Iran	6 (40%)	0 (0%)	**15**	2 (33%)	0 (0%)	**6**	2 (33%)	0 (0%)	**6**	2 (67%)	0 (0%)	**3**
Israel	9 (100%)	3 (33%)	**9**	1 (100%)	0 (0%)	**1**	7 (100%)	1 (14%)	**7**	3 (100%)	1 (33%)	**3**
India	7 (100%)	0 (0%)	**7**	6 (100%)	0 (0%)	**6**	1 (100%)	0 (0%)	**1**	-	-	-

[12] Our research assumes that documented attacks are a representative sample of the population of all attacks. It may be that attacks that fail do get publicly reported with the same degree of frequency as those that succeed.

Pakistan	7 (100%)	0 (0%)	**7**	6 (100%)	0 (0%)	**6**	1 (100%)	0 (0%)	**1**	-	-	-
S. Korea	7 (100%)	0 (0%)	**7**	4 (100%)	0 (0%)	**4**	3 (100%)	0 (0%)	**3**	-	-	-
Japan	3 (100%)	0 (0%)	**3**	3 (100%)	0 (0%)	**3**	-	-	-	-	-	-
Kuwait	1 (100%)	0 (0%)	**1**	1 (100%)	0 (0%)	**1**	-	-	-	-	-	-
Syria	1 (100%)	0 (0%)	**1**	1 (100%)	0 (0%)	**1**	-	-	-	-	-	-
Taiwan	1 (100%)	0 (0%)	**1**	-	-	-	1 (100%)	0 (0%)	**1**	-	-	-
Georgia	0 (0%)	0 (0%)	**1**	0 (0%)	0 (0%)	**1**	-	-	-	-	-	-
Lebanon	0 (0%)	0 (0%)	**1**	0 (0%)	0 (0%)	**1**	-	-	-	-	-	-

Looking at Table 2, China is by far the most active cyber instigator in the international system, with Russian and the United States a distant second. Espionage and the manipulation of information appears to be China's method of choice and they have a 92 percent rate of successful known breaches. Seen in this light, Chinese elite may see cyber as a means of catching up to the status quo hegemon, the United States. It therefore has utilized much of its cyber capabilities exploiting vulnerable information that could help narrow the technological gap with the United States. However, it remains to be seen as to how effective these exploits have been in terms of payoffs (Lindsay 2015), as only one of these espionage attempts, the OPM hack, has evoked a behavioral change.[13]

Russia's most useful tactic appears to be disruption, and this is most famously demonstrated in the 2007 attacks on Estonia and the 2008 events preceding the five-day conflict with Georgia, however these high-profile attacks did not evoke concessionary behavioral changes. More recently, the Russian APT group "Fancy Bear" has utilized espionage coercive methods, most notably the hacks on the Democratic National Committee (DNC) during the 2016 US elections and a mobile spyware campaign that compromised the locations of the Ukrainian military's artillery in the Russian-backed separatist conflict. It seems Russia is now cashing in on its espionage exploits that are gaining attention and worry among the international community. Yet, to date Russia appears to fail in any degradation campaigns, unlike its rival, the United States.

The United States succeeds in invoking a behavioral change four times out of six attempts when utilizing cyber degradation techniques. Three of these degrading operations were defensive measures that denied access to Chinese espionage attempts. The other is the oft-noted

[13] Our coding of the OPM Hack as a concession was contentious. Within the group of three primary authors and coders, two agreed that it was a concession and one disagreed. Amongst the sample of coding reviewers (a team of fifteen members of the Professional Military Education system were recruited to review the coding with many of them having engaged in or operated cyber systems for the military), ten agreed that the case was a concession while five disagreed. The disagreement is based on the judgement that the United States made a concession. The coders that counted the event as positive did so because either the diplomatic agreement between China and the United States would not have occurred without the hack, so the instance of bringing the United States to the bargaining table was a concession or change of behavior. Coders in the negative generally agree that there was an agreement after the event, but it is unclear and unlikely that the United States conceded anything. It could be that this case demonstrates a concession or change of behavior in that members of the US military and intelligence community now must behave differently knowing that they have been potentially compromised.

Stuxnet worm believed to be co-launched with Israel.[14] The U.S. also utilizes espionage techniques via its top spy agency the National Security Agency, and it has achieved behavioral changes in its targets three times. Even with the revelations of the classified documents leaked by Edward Snowden in 2013, the U.S. has shown remarkable restraint in cyberspace when one considers its enormous technological advantage in offensive cyber capabilities.

Israel is also a state with effective manipulation campaigns and also utilizes its cyber coercive power sparingly.[15] Israel has invested much in its defensive capabilities, as it is bombarded by cyber jihadists, non-state hackers, and various Middle Eastern state actors on a regular basis (Valeriano and Maness 2015: Chapter 7). The unique cyber threat environment that Israel finds itself has led to it becoming a very cutting edge and leading offensive and defensive capable cyber power (Cohen et. al. 2015). An example of Israeli cyber prowess was demonstrated in its remarkable resilient stance during its offensive on Hamas in Gaza in November 2012, where it successfully deflected millions of malicious cyber attempts on its networks (Osbourne 2012).

India and Pakistan have found disruptive campaigns to be the most useful tactic, usually on each other, and have been relatively low-level propagandist disruptions. The same dynamic exists between South Korea and Japan, two other democracies that have utilized cyber coercion on one another. North Korea is another state that uses cyber coercion as a tool, yet it along with Iran has generally failed in the international cyber realm.

The political impact of Stuxnet as a standalone coercive incident has to be questioned. The goal was to stymie and hinder Iran's ability to produce weapons of mass destruction. There is the contention that the Stuxnet operation pushed Iran to the bargaining table, yet the combination of diplomatic pressure and economic sanctions on Iran, along with the degrading act of the Stuxnet worm, and the combined effects of these action brought Iran to the negotiating table where the permanent members of the United Nations Security Council, Germany, and Iran eventually hashed out what is known as the Iran Deal. We will be dealing with the combined effects of cyber and conventional disputes more in future research. Stuxnet is arguably the most sophisticated piece of malware that any state has launched, yet it needed other conventional pressures for Iran to finally make concessionary behavioral changes.

The Shamoon operation launched against Saudi Arabia's Aramco was also technically effective, but if the goal was to decimate the oil industry and harm their ability to collect data or operate equipment, it largely failed (Bronk and Tikk-Ringas 2013). These examples illustrate the complicated nature of evaluating the impact of cyber operations and countering the myths that are built up to support new weapons. When political considerations are considered in such operations, they often are ineffective. For example, the "Wen Jiabao Retaliation" Trojan horse by China sought to punish *The New York Times* and *The Washington Post* for publishing stories critical of then-President Wen Jiabao did not stop such stories (Perlroth 2013). Cyber as a

[14] Coding Stuxnet as a concession is generally a contentious process but all coders agree that Iran conceded after the event. Whether this coding is based on a change in behaviour in light of the compromised nuclear systems or the diplomatic agreement with the United States in 2015 is up for debate. Coming the bargaining table is an example of a concession for Iran and they did change their behaviour after the incident. What is unclear is causality. Was the behaviour changed because of the Stuxnet attack or was it changed because of the other attacks made at the time, including the assassination of nuclear scientists or economic sanctions. This issue could only really be settled by an examination of decision-making within Iran at the time.

[15] This statement does not imply that Israel is not a major cyber actor or invests significant resources in its cyber capabilities. Rather, they appear to conceal that power and convert it into coercive campaigns less frequently, preferring to either collect intelligence or enable future coercive attacks in a Corbettian force-in-being strategy.

coercive tool in changing the behavior of entities must therefore be considered carefully. What remains is an examination of the question of successful and observable concessions in the diplomatic or military battlefield, an issue we turn to now.

Assessment

A potential problem with utilizing coercive tactics is that they could escalate the fight between entities rather than bring them to the negotiating table. Yet, at the same time the state could take the other route and view the use of cyber as taboo and therefore not view the initiating state as a reliable bargainer. This would lead to escalation, possibly beyond the cyber domain. States considering utilizing cyber coercion may therefore be selective about when to use the tool, and to what effect. Domain clearly matters, and the utilization of cyber tactics to this point seems limited suggesting that massive attacks could provoke the opposition into retaliatory postures therefore they are strategically avoided in the first place.

We find that measures seeking breaching target networks can be effective, but rarely achieve a change in behavior. Disruptions and espionage approaches can achieve objectives, but this is often due to their limited goals. Regardless, in-depth case study analysis, selected at random using proper theoretical justification, are needed to extract greater lessons from the patterns uncovered here and will be one of the next tasks for our research program.

Our examination so far indicates that cyber degradation strategies tend to succeed in compelling a concession at a rate of 30 percent. This estimate is consistent with other forms of coercion and the implied success rate of 19-30 percent (Blechman and Kaplan 1978; Art and Cronin 2003; George and Simons 2004; Sescher 2010; Horowitz 2010) and above the coercive threshold implied by Abrams research, ten percent (2012). Yet, it is unclear if these attacks can be assessed independently. Coercion tends to cumulative and combined, implying that what one sees as cyber coercion is not singularly the result of computer network operations. For example, the Stuxnet attack is correlated with a concession by Iran but this concession years after the cyber action and in conjunction with other actions that were likely more useful in convincing Iran to change behavior (leadership change, targeted assassinations in their nuclear program, defections, lifting sanctions, fear of conventional attack by Israel).

Table 3 lists the cases of concession for degrade operations and espionage operations. All of the degradation incidents involve the cyber superpower, the United States, who was the initiator four times. Three advanced defensive measures launched by the United States that successfully changed behavior targeted China and North Korea: Cisco Raider, Boxing Rumble, and Buckshot Yankee.[16] Stuxnet, the advanced worm that physically destroyed centrifuges at the

[16] Cisco Raider was launched against the People's Liberation Army (PLA) to stop the tide of counterfeit Cisco software that was being downloaded online and spreading spyware in many private sector networks. The operation successfully halted these Chinese efforts. The Boxing Rumble Incident was a clever reactionary botnet to several Chinese espionage attempts on civilian DOD networks. Whenever certain strands of codes known to be of the PLA variant were launched against these networks, a successful denial of service barrage would be launched back at the source, effectively shutting the hackers' network down until the botnet could be removed.[16] Buckshot Yankee was another denial of service campaign to halt Chinese espionage attempts against the Pentagon's networks. These American efforts were time consuming and there seemed to be no answer to stopping the reaction to attempting to breach these networks, the espionage campaigns were halted and the campaigns did what were intended, which was changing the cost-benefit calculus of launching cyber coercive methods.

Iranian Natanz nuclear facility, and the Sony hack, which led to an escalatory row between the United States and North Korea, are the other two degradation successes.[17]

Table 3: Concessionary Degradation and Espionage Cyber Coercive Incidents

Initiator	Target	Name	Start date	Method
US	China	Cisco Raider	2/29/2006	Keystroke & Botnet (Degrade)
US	China & North Korea	Boxing Rumble	1/1/2008	Botnet (Degrade)
US & Israel	Iran	Stuxnet	6/1/2009	Worm (Degrade)
US	China	Buckshot Yankee	4/29/2010	Virus & Botnet (Degrade)
North Korea	US	Sony Hack	11/24/2014	Trojan & Wiper malware (Degrade)
Israel	Syria	Mossad Trojan	12/10/2006	Trojan (Espionage)
US	China	Arrow Eclipse	5/27/2007	Keystroke & Worm (Espionage)
US	China	NSA Fourth Party	7/1/2009	Keystroke & Worm (Espionage)
US	China	Shotgiant	3/10/2010	Trojan (Espionage)
China	US	OPM Hack	3/15/2014	Trojan (Espionage)

Table 3 lists the five espionage tactics that resulted in concessionary behavioral changes in the targets. It must be noted that several espionage coercive measures listed in the dataset may one day evoke a behavioral change, as these types of information asymmetry battles are delayed and make take years to manifest. As Figure 1 notes above, it is espionage coercive techniques that are on the rise, and this may be because states are finding that these methods may have the most coercive potential in the long run.

Our cases of concession during espionage campaigns seem to suggest that cyber means of information manipulation might be effective in turning an adversary and countering their own espionage manoeuvres. The problem with this frame is while these counter moves demonstrate the utility of cyber deception, they are also cases in which American counter espionage moves were discovered and made public. The effectiveness of the operations could have been extended if they had gone on longer without discovery. That there seems to be a cycle of Chinese espionage, American counter-espionage, stasis, and reset every two or three years suggests that there is a cyclical nature to espionage operations.

It could also be that the issues involved in cyber conflicts are not salient enough to provoke a strenuous effort needed to alter behavior (Vasquez 1993, Hensel 2001, Valeriano and Maness 2015), therefore we rarely see concessions. This is clearly becoming a key query in that

[17] Coding the Sony Hack as a concession simply means that North Korea changed the behavior of Sony Pictures. That change of behavior actually resulted in the release of the movie digitally and free to Netflix within a few weeks of release demonstrated an alternative mode of distribution and likely was counter to the goals of the North Korean operation. If the goal was to make sure that no one saw a film that depicted Kim Jung Un in a negative light, the hackers failed miserably.

scholars often skip the context and issues behind cyber disputes, presenting them as attacks in isolation and not part of wider diplomatic campaigns, an issue we will investigate further next.

Degradation techniques seems to see more success in evoking concessions, but these operations can be costly and more utility still may be found in conventional coercive measures in the diplomatic, economic, and military realms. Although Stuxnet as a standalone coercive tool did irreparable damage to Iran's centrifuges, the behavioral change of the ultimate signing of the Iran Deal, where Iran agreed to stop its weapons grade enrichment program with the UN Security Council, would probably not have happened without the crippling economic sanctions and diplomatic pressure. We will be analyzing the combined effect of cyber coercion with other conventional coercive measures in future research.

Conclusion

New weapons provide new opportunities, advantages, and possibilities. Yet these considerations might not extend to the efficacy of such weapons. Are cyber weapons able to help states achieve victory? This question is complex and evidence presented here initially suggests that when cyber weapons are used for coercive intent, they fail more often than not.

Given these preliminary findings, as we are only in the beginnings of the era of cyber power, we must consider caution in operations. The success of new weapons is often overestimated. Despite their use in the 1917 Battle of Cambria and J.F.C. Fueller's Plan 1919, it took over twenty-years for the battlefield power of the tank to alter operational campaigns. Conventional air power alone did not achieve its proponents' anticipated decisive success in World War II or in modern operations like Kosovo and the Persian Gulf War (Byman and Waxman 2000).

If cyber weapons are not decisive as a form of coercion, then what are they good for? The clear advantage comes in manipulating information (i.e., espionage and deception), which complement warfighting capabilities and other coercive instruments. These weapons can be cheap, easy and quick methods to collect information, but will they change or alter the balance of power? Even if you steal large troves of data, they are difficult to utilize, offer intense disadvantages in language and cultural interpretation, and once exploited, are often closed for future access.

The power of cyber instruments might reside in their cumulative effect when integrated with broader coercive campaigns. In this respect, cyber capabilities add another option to the list of available options for states to achieve their policy goals. While the degree to which an actor can integrate different instruments of power and set clear policy objectives varies widely, the fact stands that most modern governments strive to use a 'whole of government' approach to forcing their adversaries to make concessions. They combine diplomacy, economic threats, propaganda and the threat of limited military force to seek concessions. Most coercive acts, even in cyber, often accompany positive inducements forming a 'carrot and stick approach.

The next question we need to ask in a follow up investigation is how do these different coercive cyber techniques succeed when paired with other conventional coercive measures such as diplomacy, economic sanctions, or military threats. In isolation, cyber methods might not be very useful to compel, but combined with other forms power they might be more effective. No state or actor should rely on one tactic. Given the scope of this investigation, this question deserves its own careful and nuanced treatment to follow up on this scoping exercise.

Will cyber be a decisive form of coercion in the future? We find here that the utility of cyber operations for compellence is limited and occurs at a level consistent with other coercive instruments. Yet, these results are only based on the early, still emerging history of the cyber era (2000-2014). While the future might bring greater change, a careful reading of cyber history suggests we might have a reason to be more pessimistic about the utility of these technologies in the diplomatic and military battlefield (Healey 2013).

References

Abrahms, Max. 2006. "Why Terrorism Does Not Work." *International Security* 31(2): 42-78.

Abrahms, Max. 2012. "The Political Effectiveness of Terrorism Revisited." *Comparative Political Studies* 45(3): 366-393.

Arquilla, John and David Ronfeldt. 1993. *Cyberwar is Coming!* Santa Monica: RAND Corporation.

Art, Robert J. and Patrick M. Cronin. 2003. *The United States and Coercive Diplomacy.* Washington, D.C.: U.S. Institute of Peace.

Blechman, Barry M. and Stephen S. Kaplan. 1978. *Force Without War: U.S. Armed Forces as a Political Instrument*. Washington, D.C.: Brookings Institution.

Borghard, Erica and Shawn Lonergan. 2016. "The Logic of Cyber Coercion." *Security Studies*. Forthcoming

Brenner, Joe. 2015. "Correspondence: Debating the Chinese Cyber Threat" *International Security* 40(1): 191.

Bronk, Christopher and Eneken Tikk-Ringas. 2013. "The Cyber Attack on Saudi Aramco" *Survival* 55(2): 81-96.

Bunker, Robert J. 1996 "Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI" *Parameters* 26(3): 108.

Burke, Garance and Jonathan Fahey. 2015. "U.S. power grid vulnerable to foreign hacks" *Associated Press*, December 21. http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks.

Byman, Daniel and Matthew Waxman and Eric Larson. 1999. *Air Power as a Coercive Instrument.* Santa Monica: RAND Corporation.

Byman, Daniel and Matthew Waxman. 2000. "Kosovo and the Great Air Power Debate," *International Security* 24(4): 5-38.

Byman, Daniel and Matthew Waxman. 2002. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. New York: Cambridge University Press.

Cable, James. 1981. *Gunboat Diplomacy*. New York: Palgrave MacMillian.

Campbell, Brian. 2001. "Diplomacy in the Roman world (c.500 BC-AD 235)."*Diplomacy & Statecraft*. 12(1): 1-22.

Clarke Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins.

Cohen, Matthew S., Charles D. Freilich and Gabi Sibloni. 2016. "Israel and Cyberspace: Unique Threat and Response", *International Studies Perspectives.* 17(3): 307-321.

Department of Defense, Air-Sea Battle Office. 2013. *Air-Sea Battle Concept*, Version 9, May. http://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf.

Department of Homeland Security, Cyber Security Division. 2016. *Securing Your Cyber Future,* https://www.dhs.gov/sites/default/files/publications/CSD-portfolio-guide-2016-.pdf

Diehl Paul F. and Gary Goertz. 2001. *War and peace in international rivalry*. Ann Arbor: University of Michigan Press.

Domingo, Francis C. 2014, "The RMA Theory and Small States." *Military and Strategic Affairs*, Vol. 6 No. 3, pp. 43-58.

Fearon, James D. 1994. "Domestic political audiences and the escalation of international disputes." *American Political Science Review*. 88(3): 577–592.

Fearon, James D. 1995. "Rationalist Expectations for War," *International Organization*. 49(3): 379-414.

Fearon, James D. 1997. "Signaling foreign policy interests tying hands versus sinking costs." *Journal of Conflict Resolution*. 41(1): 68-90.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth." *International Security* 38(2): pp. 41-73.

Gartzke, Erik and Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies*. 24(2): 316-348.

George, Alexander L. 1991. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington: United States Institute of Peace.

George Alexander L. and Richard Smoke. 1974. *Deterrence in American Foreign Policy: Theory and Practice.* New York: Columbia University Press.

George, Alexander L. and William E. Simons. 2004. *The Limits of Coercive Diplomacy*. 2d ed. Boulder, Colo.: Westview.

Goldstein, Avery. 2013. "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations." *International Security*. 37(4): 49-89.

Gompert, David C. and Martin Libicki. 2014. “Cyber Warfare and Sino-American Crisis Instability.” *Survival*. 56(4): 7–22.

Healey, Jason. 2013. *A Fierce Domain*. Washington: Atlantic Council

Hensel, Paul R. 2001. “Contentious Issues and World Politics: The Management of Territorial Claims in the Americas, 1816-1992.” *International Studies Quarterly* 45: 81-109.

Horowitz, Michael C. 2010. *The diffusion of military power: Causes and Consequences for International Politics*. Princeton: Princeton University Press.

Huth, Paul, Christopher Gelpi, and D. Scott Bennett. 1993. "The Escalation of Great Power Militarized Disputes: Testing Rational Deterrence Theory and Structural Realism." *American Political Science Review*. 87(3): 609-623.

Huth, Paul and Bruce Russett. 1990. “Testing Deterrence Theory: Rigor Makes a Difference.” *World Politics*. 42(4): 466-501.

Jakobsen, Peter Viggo. 2000. “Reinterpreting the Western Use of Coercion in Bosnia-Hercegovina: Assurances and Carrots Were Crucial.” *The Journal of Strategic Studies*. 23(2): 1–22.

Jervis, Robert. 1978. "Cooperation under Anarchy." *World Politics*. 30(2): 167-214.

Jervis, Robert. 1979. “Deterrence Theory Revisited.” *World Politics.* 31(2): 289-324.

Kello, Lucas. 2013. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security*. 38(2): 7-40.

Klein, James P., Gary Goertz, and Paul F, Diehl. 2006. “The new rivalry dataset: procedures and patterns.” *Journal of Peace Research* 43(3): 331-348.

Kydd, Andrew H. and Barbara F. Walter. 2002. "Sabotaging the peace: The politics of extremist violence." *International Organization.* 56(2): 263-296.

Kydd, Andrew H. and Barbara F. Walter. 2006. "The strategies of terrorism." *International Security.* 31(1): 49-80.

Lawson, S., S. K. Yeo, Haoran Yu and E. Greene. 2016. "The cyber-doom effect: The impact of fear appeals in the US cyber security debate." *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, pp. 65-80.

Lebow, Richard Ned. 1994. *Between War and Peace: The Nature of International Crises*. Baltimore: John Hopkins University Press.

Lebow, Richard Ned. 2007. “Thucydides and Deterrence.” *Security Studies*. 16(2): 163-188.

Liang, Qiao and Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Libicki, Martin C.1995. *What is Information Warfare*. Washington: National Defense University.

Lindsay, Jon R. 2015. "The Impact of China on Cyber Security: Fiction and Friction" *International Security*. 39(3): 7-47.

Lindsay Jon R. and Erik Gartzke. 2016. "Coercion through Cyberspace: The Stability-Instability Paradox Revisted." Forthcoming in Kelly Greenhill and Peter Krause, eds. *The Power to Hurt: Coercion in the Modern World*.

Lynn III, William. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs.* Sept/Oct, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Maness, Ryan C. and Brandon Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions." *Armed Forces and Society*. 42(2): 301-323.

Maness, Ryan C., Brandon Valeriano. 2017. *Coding Manual for v1.5 of the Dyadic Cyber Incident and Dispute Dataset, 2000-2014*, unpublished manuscript. Available at: drryanmaness.wix.com/irprof

Missiou-Ladi, Anna. 1987. "Coercive Diplomacy in Greek Interstate Relations." *The Classical Quarterly*. 37(2): 336-345.

Modelski, George. 1964. "Foreign Policy and the International System in the Ancient Hindu Word." *American Political Science Review*. 58(3): 549-560.

Mueller, Karl. 1998. "Denial, Punishment, and the Future of Air Power" *Security Studies* 7(3): 182-228.

Nye, Joseph S. and William Owens. 1996. "America's Information Edge." *Foreign Affairs* 75(2): March/April 1996.

Nye, Joseph S. 2010. *Cyber power*. Cambridge, Mass., Harvard Belfer Center.

Office of the Director of National Intelligence. 2017. *Assessing Russian Activities and Intentions in Recent US Elections*. January 6, Accessed 1/22/2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf

Osbourne, Charlie. 2012. "Minister: Israel deflected 44 million cyberattacks over Gaza." *ZDNet*, November 19. http://www.zdnet.com/article/minister-israel-deflected-44-million-cyberattacks-over-gaza/

Overy, Richard J. 1996. *Why the Allies Won.* New York: W.W. Norton.

Pape, Robert. 1996. *Bombing to Win*. Ithaca: Cornell University Press.

Perlroth, Nicole. 2013, "Hackers in China Attacked the Times for Last 4 Months." *The New York Times*, 1/30/2013, Accessed 12/30/2015, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0

Peterson, Dale. 2013. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies*. 36(1): 120-124.

Reed, Thomas. 2005. *At the Abyss: An Insider's History of the Cold War*. New York: Random House.

Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy*. 34(1): 40-63.

Schelling, Thomas. 1960. *Strategy of Conflict*. Cambridge: Harvard University Press.

Schelling, Thomas. 1966. *Arms and Influence*. New Haven: Yale University Press.

Sescher, Todd S. 2010. "Goliath's Curse: Coercive Threats and Asymmetric Power." *International Organization* 64(4): 627-660.

Sescher, Todd. 2011. "Militarized Compellent Threats, 1918–2001" *Conflict Management and Peace Science*. 28(4): 377–401.

Shakarian, Paulo. 2011. "Stuxnet: Cyberwar revolution in military affairs." *Small Wars Journal*. April 15.

Singer Peter W. and Allan Friedman. 2014. "Cult of the Cyber Offensive: Why belief in first-strike advantage is as misguided today as it was in 1914." *Foreign Policy.* January 15. http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/

Singer, Peter W. 2015. "How the United States Can Win the Cyberwar of the Future." *Foreign Policy*, 18 December. http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/

Szafranski, Richard. 1995. "A Theory of Information Warfare: Preparing for 2020." *Air Power Journal* 9(1): 1-12.

Thompson, William R. 2001. "Identifying rivals and rivalries in world politics." *International Studies Quarterly* 45(4): 557-86.

Valeriano, Brandon and Ryan C. Maness. 2012. “Persistent Enemies and Cyber Security: The Future of Rivalry in an Age of Information Warfare.” in Derek Reveron’s *Cyberspace and National Security: Threats, Opportunity and Power in a Virtual World*. Washington D.C.: Georgetown University Press: 139-158.

Valeriano, Brandon and Ryan C. Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research,* 51 (3): 347-360.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* New York: Oxford University Press, 2015.

Valeriano, Brandon and Ryan C. Maness. 2016. “International Political Theory and Cyber Security” to be published in *The Oxford Handbook of International Political Theory* Robyn Eckersley and Chris Brown, Eds., Oxford University Press.

Vasquez, John A. 1993. *The War Puzzle.* Cambridge: Cambridge University Press.

Weeks, Jessica L. 2008. “Autocratic audience costs: Regime type and signaling resolve.” *International Organization* 62(1): 35–64.

Whyte, Christopher. 2016. “Ending cyber coercion: Computer network attack, exploitation and the case of North Korea.” *Comparative Strategy* 35(2): 93-102.