Sharkey, Veronica (2016) *Signaling in cyber disputes.* [MSc]

Copyright © 2016 The Author

Copyright and moral rights for this work are retained by the author(s)

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This work cannot be reproduced or quoted extensively from without first obtaining permission in writing from the author(s)

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author

When referring to this work, full bibliographic details including the author, title, institution and date must be given.

http://endeavour.gla.ac.uk/133/

Deposited: 9 December 2016

Enlighten Dissertations
http://endeavour.gla.ac.uk/
deposit@lib.gla.ac.uk

School of Social and Political Sciences

Signaling in Cyber Disputes

September 2016

1101319

Presented in partial fulfilment of the requirements for the Degree of M.Sc. International Relations

Wordcount:
16,486

Abstract

As states begin to deploy cyber tactics as part of their wider strategic arsenal questions arise around how these cyber tactics may alter the processes of international relations, including those pertaining to coercive diplomacy and inter-state negotiation. This dissertation endeavours to address the possibility that states may utilize cyber tactics to signal their resolve to the bargaining approach or policy stance adopted by their leaders during periods of interstate crises, asking what impact such cyber-signals may have on dispute dynamics in terms of escalating or restraining hostilities between the disputants.

To do so it has employed a multi-method approach, applying Schultz's model of signaling during crisis bargaining to three qualitative case studies, drawn from each of the three kinds of cyber disputes identified by Valeriano and Maness in their pioneering Dyadic Cyber Incident and Dispute dataset(2015). Additionally, this in-depth contextual analysis is supplemented with a basic statistical analysis of the DCID data-set combined with that of the Correlates of War Militarized Interstate Dispute data(Ken- wick et al. 2013) to compare such basic dispute features as length and severity be- tween cases, in order to identify wider trends between the varying strategic environments in which each of the three case study dyads operate.

Though it was posited that cyber-signals would have impact when acknowledged by the perpetrating state and visible to the domestic audiences able to pressure on state leaders during the decision making process, evidence did not support this hypothesis across every case studied. Despite this line of inquiry failing to be fulfilled universally, between them these three cases do still indicate that there are indeed circumstances under which states may deploy impactful cyber-signals, albeit driven by particular, salient or emotive contextual settings. I therefore conclude, upon reflection, that while not perfect, this dissertation finds grounds for further investigation of the cyber signal concept and represents at least a start to unpicking the complex issues which underpin this vital area of international relations.

Acknowledgments

An enormous debt of gratitude is owed to Dr Brandon Valeriano, for many years of continued encouragement, guidance and inspiration. To Dr Valeriano, Dr Ryan Maness and all who worked on the DCID dataset, thank you for making this research possible.

A final thank you too to my family and loved ones, for all their endless support and patience.

Contents

Introduction

The emerging cyber dimension to international relations has variously been described in academic literature and public discourse as, on the one hand fraught with the potential to inspire an act of war with near apocalyptic consequences, and alternatively, of having precipitated little alteration of existing patterns of behaviour between states. Proponents of the former, doom laden 'cyber-war' scenario include both academics, politicians and policy makers - with Mazanec warning of the "real and growing threat" of cyber tactics outpacing "the development of constraining international norms,"(2015:208), whilst then US Defense Secretary Leon Panetta cautioned that cyber strikes could constitute a form of attack powerful enough to deliver a "cyber pearl harbour"(Panetta, 2012). In contrast, following the latter position, Gartzke argues that the evolution of cyber tactics represent merely the latest "phase in the ongoing revolution in military affairs"(2013:41), while Maness and Valeriano reflect that cyber strikes are yet to "significantly affect foreign policy interactions on the balance"(2015:312).

In this dissertation I intend to explore the possibility that as states begin to view and employ cyber tactics and tools as part of their wider strategic arsenal, when faced with conflict over an issue of contention they may engage in practices of signaling resolve through both cyber and traditional military means. Thus far, while scholars have hinted at this possibility, there has been something of a dearth of research into this important area of international relations - on the cyber side

Maness and Valeriano highlight the deficit writing "we know very little about the impact of cyber actions, and we know even less about how it is connected to conventional coercive tactics utilized by states(in Friis and Ringsmose[Eds], 2016:49), while one of the original proponents of state signals during interstate crises, Kenneth Schultz, himself calls for renewed focus on moving forward academic thought on the "deeper issues" surrounding "strategic interaction in international crises"(2012:372-3).

Essentially, therefore, this is a gap in academic inquiry which I intend to address with this dissertation through in-depth analysis of the role cyber tactics may have with regard to the development of interstate crisis. My over-arching goal in pursuing this line of inquiry is to assess what impact cyber-signals may have on dispute dynamics, investigating whether the use of offensive cyber tactics in a signaling capacity may act as an effective precursor to negotiation during periods of interstate crises, lead to an escalation of hostilities, or be of negligible impact, failing to effectively communicate the commitment of a state or leader to their chosen policy stance.

To this end, I will follow the work of scholars such as Lawson, recognizing that the innovative, novel nature of the cyber phenomena itself requires fresh thinking and possibly the adaption or challenging of existing theories should they prove an obstacle to uncovering what, if any, impact new cyber capabilities have on the conduct of interstate relations(2012:online; see also Kello 2013:7). This work therefore seeks to objectively evaluate what kind of role cyber tactics might play in the escalation or restriction of interstate disputes in which both parties seek to communicate their resolve through diplomatic or military acts, for example engaging in a show of force or fortifying border defenses, arguing that cy-

ber signals in certain circumstances - where visible to domestic audiences and acknowledged by the perpetrating state - may indeed engender similar outcomes to those of the traditional foreign policy field(optimally recognition of the need for negotiated dispute settlement, but also inclusive of misperception and possible escalation, or in some cases a continuation of the status quo punctuated with brief bouts of hostility(Schultz, 2001*a*:27-8), albeit carrying different operating costs and consequences.

Thus, whilst the thrust of this research is to examine the impact of cyber signaling practices on dispute escalation, these cyber incidents and confrontations will be investigated in tandem with Schultz's theory of signaling and state behaviour in crisis bargaining games itself(2001*a*). To pursue both of these aims, my research will unfold in five main stages: after a review of relevant signaling and cyber literature, engaging with and situating my study in existing academic debate, I will proceed to set out and justify my methodological approach before its employ across the subsequent three chapters of analysis. Drawn at random from the combined resources of the Dyadic Cyber Incident and Dispute Dataset, Version 1.5(Valeriano and Maness, 2015c), and the Correlates of War Militarized Interstate Dispute Data version 4.01(Kenwick et al. 2013), these mixed quantitative analyses and qualitative case studies dissect periods of hostile interaction across three different forms of interstate dispute involving cyber tactics, comprising: a disruptive, low severity series of clashes between India and Pakistan; a coercive feud involving Japan and the Republic of South Korea; and finally an espionage fuelled dispute between the United States of America and the People's Republic of China.

The validity of this approach is two-fold, for by using a well picked-over theoretical concept such as Schultz's crisis bargaining model(2001*a*) to assess the impact of cyber technology on interstate disputes and the tactics employed by those waging them, I hope to evaluate both the existing theory and new technological development simultaneously. Indeed, as Maness and Valeriano assert, the lack of knowledge surrounding the impact of, or reaction to, cyber actions in the international arena is - given their potential import to military affairs and state security - not only of detrimental affect to the ability of the academic or policy community to conduct accurate or meaningful analysis, but seems almost foolhardy when one considers that conflicts which originate in cyberspace may not necessarily remain there(2015*a*:303-4). In short, the very originality of this dissertation concept combined with the contemporary nature of the burgeoning cyber field arguably renders research of this ilk a worthy addition to the expanding body of work designed to develop our understanding of the cyber realm and how it interacts with the wider processes of international relations.

Chapter 1 - Review of Literature

As alluded to in the introduction, there is a vast pool of academic work from which to draw parallels to inform and guide my research. This literature review is intended to engage with these studies; from the wider cannon of research concerning state signaling practices and escalation of interstate disputes, to the more recent works regarding the growth of the cyber field in international relations; situating this dissertation between these bodies of research as it seeks to determine what impact state instigated cyber-signals may have on dispute dynamics. Thus, before moving on to the growing collection of studies which represent the work to-date on cyber interaction, there will first follow an examination of the concept of state signaling practices, from its roots in the 1980s to the revisions and adaptations made at the present time of writing.

How then, do states signal resolve and how significant is this practice in dispute escalation or resolution? Academic analysis of the concept of credibly signaling resolve during interstate crises arguably stems from the early works of scholars such as Putnam, whose 1988 theory of two-level games paved the way for analysis of the theoretical linkage between factors from the domestic and international level which when combined, could interact to shape complex interstate bargaining processes - for example where domestic constituencies could bring pressure to bear on governments and leaders to adopt certain or more favourable policies, and thereby exert an influence on policy outcomes in the international

arena(1988:436). Viewed alongside analysis from the likes of Fearon, for whom domestic political audiences played an essential role in the potential for escalation of interstate disputes(1994), it could be suggested that such theoretical innovations as these served to open up the field of international relations to forms of research which were not limited to a single level of analysis, but could examine both domestic and international influences on events in international politics. Indeed, for Schultz, and his theory on how states signal resolve during interstate crises, such a development could be considered pivotal, as the success of state leaders in sending credible signals of resolve was partially contingent upon the awareness and ability of their domestic audiences to respond to policy stances - whereby constituents could inflict some form of sanction or cost on a leader that reneged on, or drew back from their original dispute position - an inherently 'risky' strategy as by resorting to triggering such a potentially potent domestic backlash, state leaders concerned for their own political survival could be more inclined to stand firm in the face of reciprocal demonstrations of resolve, such that through their own attempt to display the force of their intent, leaders may inadvertently raise the chances of full military escalation to conflict(1998:830).

Prior to engaging critically with this concept of signaling practice and the theoretical mechanisms on which the theory is founded, however, some clarification of the key terms and ideas which underpin this paradigm ought to be outlined. First and foremost amongst these is the concept encompassing the practice of signaling resolve itself. 'Signaling games' as termed by Walsh, can be understood as bouts of strategic interaction in which states make clear their preferences to a rival during a dispute by engaging in some costly sort of action - for example by build-

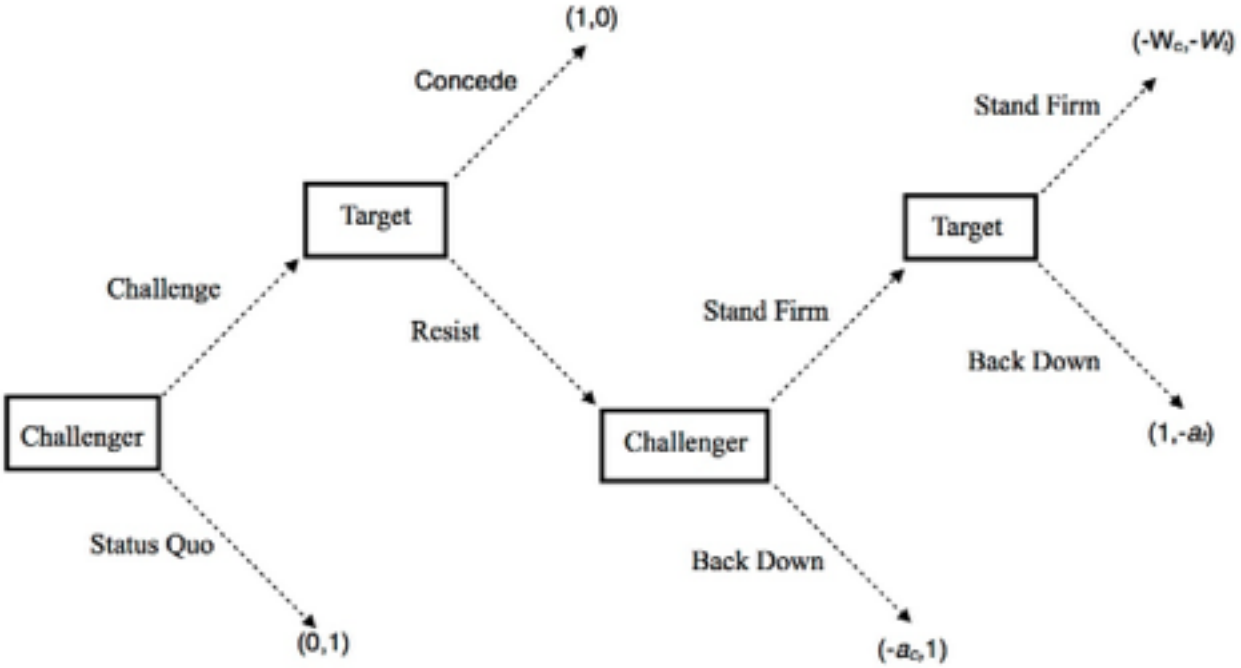
ing up their armed forces, their offensive capabilities, or instigating a limited form of military operation(2007:442-3). Needless to say, therefore, the action which forms the signal event must communicate the instigating state's intentions, their resolve to follow through on their chosen path in contending an issue of dispute, and though on the surface it would appear that cyber means are less overt, more hidden than something so notable as the mobilization of a state's armed forces, it is arguable, as shall be further elaborated in the forthcoming review of cyber literature, that not all cyber tactics are accurately described as hidden - just as military players make themselves known in a battlefield, so cyber operators become apparent in cyberspace - "by interacting with external networks threat actors maker their presence known... language traits, common techniques and malware, and motive plus historical context give us a great deal of information about who is attacking whom,"(Valeriano and Collier, 2016:online).

Returning for now to the signaling process itself, however, the domestic- sanction mechanism comes to the fore when a state leader or decision maker seeking to underline his or her dedication to their course of action, commits to their chosen policy stance publicly and initiates one of the actions outlined above. In so doing, they place national prestige on the line and potentially invoke or expose themselves to 'audience costs' - electoral or other forms of domestic sanction which would blight or even terminate a leaders tenure in office if triggered - whereby the strength of the leader's intent with regards to the issue of dispute is validated by the damages they would incur domestically should they step back from their publicly stated negotiating position(Fearon, 1994:577).

Consequently, in addition to the signaling act itself - whether of military or diplomatic nature - the triggering of such audience costs is thought to be of great import in terms of ensuring the signal to the rival state is perceived as credible, with the potential for damage to the decision maker should they step back from their stance potent enough to ensure that they are somewhat entrenched and obliged to see their decision through - a position Fearon refers to as "tying hands" in which leaders take "an action that increases the costs of backing down if the would-be-challenger actually challenges but otherwise entails no costs if no challenge materializes"(1997:70). Following this pattern, as illustrated overleaf in Figure 1, states may signal, and depending on whether their target resists or concedes, take further steps to demonstrate their resolve, such that - should both sides continue to hold firm and reciprocate shows of resolve - the dispute may either escalate to full-scale conflict, as set out in Schultz's game theoretic model of crisis bargaining, or fall short of war with the substantial costs borne by one disputant only.

There exist, however, a number of critical questions raised by scholars of the signal and audience cost concept which merit some attention. The idea of signaling resolve in disputes, and associated audience cost literature, has come some way since Schultz's original works, with the most pressing concern relevant to this work revolving around the audience cost mechanism which underpins the ability of foreign policy decision makers to signal resolve, and whether or not it is as straightforward as assuming domestic audiences will always punish leaders who lose face and climb down from foreign policy stances. After rigorous empirical analysis Moon and Souva conclude that signals of resolve which rely on audi-

Figure 1. Model of Signaling Practices during Interstate Crises



Source: Adapted from Schultz, 2001*b*:37

ence costs being invoked by state leaders work as a credible demonstration of the strength of state leaders' intent only under specific circumstances: where there are informational imbalances to overcome signals may allow states to entrench their bargaining position and begin negotiation, yet where highly salient issues are at stake, particularly with regard to territorial disputes, signaling practices are somewhat eclipsed, and therefore less likely to prevent escalation(2014:20- 1). Indeed, the suggestion appears vindicated by Gibler and Hutchison, who also emphasize the need to include contextual factors such as issue salience, or symbolic, emotion-laden territorial claims in understanding when threats are effective, and how both state leaders and domestic populations respond to them(2013:882;886; see also Tomz,2007:830-1). On the balance, therefore, far from detracting from the purpose of this research, these concerns rather amplify the value in further ex-

amination of dispute escalation and signaling mechanisms - arguably the arrival of a new potential means of signaling resolve represents a fresh opportunity for study of the concept, warrant- ing both empirical and contextual analysis of they dynamics at play in state behaviour during crises and disputes.

Ergo, drawing towards a conclusion of this brief investigation of the academic literature surrounding state signaling practices, it is worth not- ing, as Schultz himself does that no theoretical model of behaviour can perfectly 'capture' real-world crises, nor do they seek to - rather, it is the insight into state behaviour which can be understood through contrasting where it diverges from the strategic-rationality of the signaling game and crisis behaviour model which is so valuable(2001*a*:31). With this in mind, and prior to applying this theoretical insight to real-world cases, it is to the comparatively more recent, emerging field of cyber studies, which this literature re- view now turns, the second of the two main bodies of academic work at whose interface this dissertation research sits.

Even upon light reading of the cyber cannon it is fair to say that there is something of schism in the positions adopted by academics and commentators regarding the threat presented by expanding cyber capabilities and technology. Indeed, as Valeriano and Maness observe, this schism is perhaps best characterized as comprising of two extremes - one which envisions cyber conflict as a given and "regular aspect of international relations" and the other, which tends towards a skeptical view of the threat of cyber conflict, instead anticipating a "safe digital future"(2015*a*:39). Of the former, scholars such as Stone maintain the alleged ease of use of cyber tactics will almost inevitably result in the translation of

virtual cyber strikes into real world violence(2013:107), while in the latter camp Rid argues that far from facilitating greater conflict, engaging in cyber disputes may lessen the risk of actual political violence as it allows both states and individuals to act out aggression by means short of war(2013:online).

Unlike either Stone or Rid, however, I intend to take something of a more equitable approach towards analysis of the cyber field, neither ruling out the possibility of cyber conflict in the future, nor assuming that this conflict will necessarily escalate to epic or unprecedented proportions. Instead, following Gartzke(2013:41) and Valeriano and Maness, the stance adopted for this research pursues a definition of cyber technology and tactics which treats them as "a tool in the arsenal of diplomacy and international interactions, just as other forms of threats, and offensive and defensive actions in the toolbox of a state's arsenal of power"(2015*a*:31). Accordingly, to bring discussion of cyber technology back to basics in advance of deeper engagement with existing academic literature, as well as for the purposes of analytical clarity, I will treat cyber incidents - offensive, defensive or disruptive tactical strikes against a given target - as the events which form the basis of cyber conflicts, which are themselves constituted as "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities"(Ibid:5). Following on logically, therefore, it is in fact possible to argue that cyber capabilities could be deployed in some capacity during the course of a dispute between states, or potentially even ignite a dispute between states, under which circumstances - should cyber conflicts or incidents of this kind seep

into traditional militarized and diplomatic dispute arenas - the process can be termed “cyber spillover”(Maness and Valeriano, 2016 - forthcoming).

Cutting through some of the hysteria in rhetoric around a potential “cyber Pearl Harbour”(Panetta, 2012) it is also of the utmost importance to examine what patterns of behaviour are actually evident, and supported by empirical research, in the cyber realm thus far. Though dismissive of the manifestation of outright conflict involving the use of cyber tactics, Rid is quite correct in his assertion that there has been a great deal of political cyber crime - that is to say sabotage and espionage - since the advent of the present cyber era(2012:15). He is vindicated in this by the findings of a number of scholars: from Lindsay who also highlights espionage and financially motivated malicious activity in cyberspace(2013:370); to Maness and Valeriano whose exhaustive quantitative analysis of cyber incidents since the turn of the century demonstrate the majority of incidents observed to-date to comprise of “Espionage, theft, propaganda through vandalizing websites and denial of service campaigns”(in Friis and Ringsmose, 2016:49).

Given that these kinds of cyber interactions are not largely considered to be of drastic severity to state security it is perhaps not so surprising, as Lind- say, Cheung and Reveron suggest, that “the history of minor irritants and tolerable abuses experienced thus far suggest that restraint and limited effectiveness is the norm”(2015:online). Indeed, as Valeriano and Maness also argue, “A protocol of restraint has emerged as the volume of cyberattacks has increased. State-based cyberattacks are expected, and in some cases tolerated, as long as they do not rise to the level of total offensive operations - direct and malicious incidents that could destroy infrastructure or critical facilities. These options are apparently off the ta-

ble for states, since they would lead to physical confrontation, collateral damage, and economic retaliation"(2015*b*:online).

Arguably therefore, with the current, even similar dynamics of restraint operating in the international system as to those governing traditional military or diplomatic interaction, states are no less likely to respond with aggression to a cyber strike as they are to a display of force - for example a scrambling of fighter jets in international airspace, or naval vessels in international waters - suggesting that while cyber tools could have the potential to become devastating weapons, it is unlikely that they will be deployed in the kind of devastating capacity envisioned by Stone(2013:107) or other proponents of all-out cyberwarfare.

How, then, does this reflect on the possibility that states may signal resolve by cyber means during disputes? Somewhat problematically at first glance, given the basic premise of signaling resolve is to underline the preferences of the initiating state within a dispute, the less-than-clear issue of attribution associated with cyber incidents envisioned by many scholars casts doubt on how accurate a means of communication cyber strikes are. Gompert and Libicki, for example, point out that cyber operations may be carried out without the knowledge or official sanction of state leaders, casting doubt on the intentions behind the strike and potentially fostering miscalculation and dispute escalation - "Given the stakes in a crisis, would the targeted state be willing to bet that a cyber attack was unauthorized? Or would it presume that the attack was a prelude to conventional war, and be inclined to strike first?"(2014:14; see also Kello, 2013:34-5). Furthermore, as Gartzke argues, cyber weapons, as they are employed currently, have yet to exhibit the ability to inflict the kind of durable, lasting harm of the traditional military

tools deployed in interstate disputes, effectively casting doubt on the ability of states to efficiently threaten their rivals as "targets must believe both that an attack is likely to follow from noncompliance and that the attack is destined to inflict unacceptable harm"(2013:42).

Yet whilst these arguments may on the surface appear to damage the utility of cyber-signals in international disputes, in the first instance, and building on the logic of Valeriano and Collier, set out previously in this work, I would disagree that there can be no attribution for cyber strikes - on the contrary, through careful forensic examination of the system targeted and coding or malware used, common characteristics pertaining to the attacker can be uncovered or reverse engineered back toward the perpetrator, rendering the issue of attribution, as envisioned by the scholars above, "overstated"(2016:online). There remain certain aspects of the use of cyber tactics which could also serve to negate the limited nature of cyber strikes - short- lived though the less severe denial of service or website defacement cyber strikes may be, the psychological toll they exact on the target population should not be underestimated in terms of the fears and perceptions citizens hold, and thus the pressure they may subsequently exert on their state leaders to respond could serve to render important what on the surface appears a cyber strategy of low severity(Maness and Valeriano, 2015*a*:313).

Context too, as Lindsay notes is crucial(2013:374), and when related to the perceptions of target state audiences, particularly if the dispute surrounds a highly emotive issue likely to resonate strongly with both state populaces - for example a contested territory(see Vasquez and Valeriano(2008) for an excellent dissection of intractable territorial issues and impact they have on dispute escala

tion) - it could have an enormously amplified effect on hostility levels, as perceived by domestic audiences and by extension state leaders. It is arguable, therefore, that when visible to domestic audiences - for example in a disruptive strike on widely used websites or online services - and when acknowledged by the instigating state as an action aimed at a rival state target, it is indeed possible for states to use cyber tactics to signal resolve as they would any other militarized or diplomatic option.

Moreover, it could also be suggested that these cyber practices in themselves carry their own unique operational costs associated with their use, different to militarized alternatives though they are. In the first instance, the use of cyber weapons can be considered costly in the sense that the state deploying the strike cannot do so again - the coding and system vulnerability exploited to carry out the strike is necessarily unveiled by the act itself after a great deal of work and thus will not be so easy to target in the future(Lindsay, 2015:33), while, depending on the type or sophistication of cyber strike, operations themselves can require a great deal of time, expense and effort in preparation for a strike which can be used once only by its creator, whilst the malicious coding used in the attack may also be turned against the original perpetrator in a form of blow-back(Valeriano and Maness, 2015*a*:4). Ergo, while it is true enough that the costs carried by cyber tactics are different to those of a traditional military tactic, it cannot be said that these strikes carry no costs at all - to the contrary, costs such as those outlined above ought to demonstrate the importance or commitment a foreign policy decision maker may attach to his or her dispute stance when choosing to signal resolve, rather than undermine it.

In summary, thus, and within the theoretical parameters of this research, cyber tactics of the kind outlined above will be assessed alongside traditional militarized or diplomatic means of signaling in the hope that this expanded understanding of how states may signal resolve can shed light on contemporary disputes in the international arena. This review of literature has sought to engage with existing academic debate surrounding the two fields of international relations most relevant to the overarching aims of this dissertation research, and by drawing on the findings of this diverse array of scholars I hope to establish a better understanding of the mechanisms at play in state cyber signaling practices as I move onward toward my own analysis.

Chapter 2 - Methodological Approach and Theoretical Overview

Here I outline the methodological approach which forms the foundations of the analytical and theoretical framework employed in my research. This chapter will therefore begin with the presentation and explanation of the reasoning behind my research aims, questions, rationale and hypotheses, before setting out in earnest the means through which I hope to examine the possibility of states signaling resolve in the cyber realm, and how this may influence dispute escalation. Whilst there will also be a brief introduction of the cases for analysis and the datasets used to support this process, greater in-depth and contextual case-study-specific details will be explored in the subsequent analytical chapters.

Research Aims, Rationale and Hypotheses

Reflecting on the arguments presented in the review of academic literature which suggest that cyber strategies can be deployed alongside conventional military tactics in interstate disputes - indeed Jensen, Valeriano and Maness suggest that “Cyber strategies likely do not achieve effects in isolation”(2016 - forthcoming) - the principle aim of this research is to assess if states are engaging in signaling practices with cyber means, and how these potential actions could influence dispute dynamics during interstate crises.Therefore the first, and per-

haps most obvious, research questions are as follows: **[RQ1]** Do states engage in practices of signaling resolve through cyber means either interchangeably with militarized tactics during interstate disputes? And, if so: **[RQ2]** What impact does cyber signaling have on dispute escalation and inter-state relations?

More specifically, in applying Schultz's crisis bargaining model to cyber as well as militarized incidents I intend to establish if cyber interactions mirror the established patterns of behaviour associated with militarized disputes; if selected real-world disputes follow Schultz's theorized interaction models, and ultimately escalation[operationalized for this research in line with the Correlates of War Project as ranging from: a threat of the use of force; a display of force; actual use of force; or lastly, war]. Finally, therefore: **[RQ3]** Does greater cyber interaction between states in disputes lead to escalating levels of severity, as in Schultz's traditional crisis bargaining model?

Building on the perspective that cyber and military tactics form part of the same spectrum of strategic capabilities, I posit that cyber methods will be used alongside traditional foreign policy tools by states embroiled in disputes, and thus:

> **H1:** During interstate crises and disputes states engage in cyber signaling practices interchangeably with traditional military and diplomatic means.

Though different to traditional military and diplomatic means of signaling resolve, as discussed in the literature review, there remain, arguably, several aspects of the use of cyber tactics which do generate certain costs to the decision taker, and therefore represent enough credible commitment to the chosen course of action as to symbolize their resolve to hold firm - in particular the potential for blow-back

in either releasing malicious cyber coding and tools, or opening up the decision taker's own cyber networks to retaliation; the surrender of knowledge of a point of vulnerability in a rival state's cyber defenses, and by extension the opportunity to exploit it again; in addition to the amount of time, expense and effort expended in carrying out the strike itself. Therefore, in attempting to establish if and when states engage in signaling practices with cyber means, I posit that under certain circumstances states will successfully employ cyber strikes to signal state resolve, with the outcomes ranging from positive and restraining, with negotiation or mediation tempering hostilities, as successful communication of resolve deters state leaders from risking all out war; to negative and escalatory for either or both cyber and military interaction; or simply neutral where cyber-signals will have negligible effect on interstate relations. As such:

> **H2**: Cyber signaling practices will exert observable impact on dispute dynamics, either restraining or escalatory, where: cyber strikes are visible in scope, such that domestic audiences are aware of them; and where instigating states acknowledge publicly their action, such that the possibility of domestic sanctions to governments and state leaders are made manifest.

Alternatively, where this cannot be verified, the null hypothesis - that cyber-signals will impart negligible impact on interstate disputes - shall instead be accepted. Deeper introduction to the methodological approach adopted to investigate these possibilities will follow a brief outline of the theoretical parameters which define and guide this work.

Theoretical Overview - the Signaling Model

As has been noted previously, Kenneth Schultz's 2001 model of crisis bargaining forms the main theoretical framework which structures this dissertation's multi-method approach to analysis. Crucially, however, and where appropriate, the analytical lens provided by this paradigm has been expanded to include cyber and military interactions alongside one another, recognizing both as part of the same strategic spectrum. Based on the relative losses and gains of game-theory rationale, Schultz's model charts the options open to states during periods of crises and examines the possible logics driving leaders' choices as the dispute unfolds and they must consider further resistance or conceding in the face of a challenge(2001*a*:26-9).

Of particular theoretical value to this dissertation, is the mechanism Schultz's model supplies for explanations of why signals of resolve may impart an impact on the direction of disputes - that of the audience cost concept, which when triggered through the process of publicly signaling to rival states can lock leaders "into intransigent bargaining positions from which they cannot climb down" such that even if "a mutually beneficial deal exists ex ante, once the leaders have bid up the audience costs to a high enough level, neither can give in, and war becomes inevitable"(2012:371). Fundamentally this mechanism is of the utmost importance to this dissertation as it gives reason to the suggestion that cyber-signals will have impact, either escalatory or restraining, on disputes where they are publicly acknowledged and the possibility of audience costs are made manifest - where damages meted out by domestic audiences to leaders who renege on previous dispute or bargaining positions are so severe they can terminate a leaders

period of office, ensuring that during disputes, when public sentiment begins to run high, leaders appreciate that they must either diffuse the situation and accede to negotiation, or face either outright conflict through escalation or some form of sanction from their domestic constituents.

Using an established and rigorously assessed theoretical model is particularly beneficial as not only has the concept been carefully critiqued and tested by a number of scholars over the years, that it has remained relevant to the present time of writing also indicates its ongoing importance to the field of international relations, and indeed our understanding of conflict escalation and resolution. As such, in applying a tried-and-tested model to analysis of a newer phenomenon, I hope to gain the most accurate possible theoretical insight to the dynamics which drive state behaviour, and strategic choices during international disputes.

Further, in defence of drawing inspiration from a form of rational-choice model I hasten to point out, as Schultz himself does, that I do not suggest this model is a perfect replica of state behaviour, rather it is intended to clarify and identify where interaction between disputants is significantly influenced by factors such as the domestic governance or oppositional structure, domestic public audiences, or contextual, strategic considerations(2001*a*:31). Indeed, by applying the zero-sum framework of the model to the selected case studies enables an empirical and consistent assessment across differing contexts of how each state involved in a dispute fares as they invoke signaling games and respond accordingly.

Methodological Approach

To set about approaching an answer to the question of whether or not states engage in signaling practices during cyber disputes, this work employs a mixed method approach which draws primarily on the application of Schultz's model of crisis behaviour, outlined above, to qualitative case studies of periods of escalation and coercive diplomacy between rival states, supplemented by additional policy and literature analysis of material collected from sources including news outlets and state sponsored websites. Selected at random from samples of the three types of cyber dispute identified by Valeriano and Maness(2015*c*), and with the aid of the RAND function of Microsoft Excel, these case studies cover a disruptive cyber dispute between India and Pakistan; the coercive cyber interactions of the Republic of South Korea and Japan; and finally, the espionage fueled dispute between the United States of America and the People's Republic of China.

Complementing this contextual case-specific analysis, is a basic comparative quantitative analysis of combined cyber and militarized interaction data sourced from the Dyadic Cyber Incident and Dispute Dataset, Version 1.5(Valeriano and Maness, 2015*c*), and the Correlates of War Militarized Interstate Dispute Data version 4.01(Kenwick et al. 2013). This brief statistical evaluation will largely take the shape of calculating and comparing the differences between dispute features including, for example, length of interaction in days; mean severity levels and intensity of interaction, in order to lend greater empirical depth where possible to the contextual environment of the case studies selected and identify patterns of behaviour between states engaging in different forms of dis-

putes, utilizing different forms of offensive or defensive strategies, and across varying periods of time.

A note on Case Studies

By selecting a disputing dyadic pair from each category of interaction type in the Valeriano and Maness DCID data-set(2015*c*) - disruption, coercive and espionage orientated disputes - I hope to not only capture what impact cyber-signals may have on dispute dynamics, I also seek to understand how this may differ according to dispute or interaction type, and ultimately assess under which circumstances cyber-signals fit with Schultz's theory of signaling and crisis bargaining. With the aim of best assessing how interaction unfolds between states, I have selected at random a case study from each of the three types of cyber dispute which displays above average interaction and as such provide adequate scope for analysis of dispute dynamics over time.

Across the entire cyber data-set this represents all disputes which comprise of a number of incidents equal to or greater than the mean interaction level of three incidents per dispute, and generates from the three cyber dispute categories a distribution of five disruption driven and coercive disputes eligible for selection each, in addition to six espionage related conflicts. Considering the importance of the militarized element to this work alongside the hypothesized role of government acknowledgment in cyber signal- ing practices, however, these samples were further reduced to only three potential cases each, when disputes with no militarized incident crossover within a calendar year, and no governmental comment, or denial of responsibility for cyber strikes, were eliminated.

Hence, pulled from the disruption, coercion and espionage driven disputes of above average levels of interaction were: from those disputes best characterized as disruptive India and Pakistan's ten year period of hostilities, which, despite its relatively high number of cyber incidents, has a low severity ranking equitable to cyber harassment spread across these ten encounters. Secondly, of conflicts which are coercive in nature the dispute between Japan and the Republic of South Korea with a similar severity level to that of India and Pakistan, but with fewer cyber incidents - numbering only four - and, finally, from the espionage driven encounters the dispute between the United States of America and the People's Republic of China was drawn from those available, including an enormous number of incidents, forty-three in total, and experiencing a more serious severity ranking equitable to attempted destruction of critical networks.

With regard to selecting case studies as a means of analysis themselves, not only do I hope to strike a balance between in-depth contextual analysis in addition to the wider statistical review of state cyber interaction, it is arguable that conducting case studies allows the application of Schultz's crisis bargaining model to the best of its potential, while also accommodating the unique contextual backdrops eliminated from the model's stylized assessment of crisis events.

Data, Measurements and Quantitative Analysis

Considering that this dissertation's overall aim is to focus on what impact cyber-signals have on dispute dynamics, only a brief statistical examination of the wider cyber and militarized interaction data will be conducted. It will simply revolve around the identification of disparities and trends in mean dispute

length, severity and intensity(in terms of the number days between incidents); the rate of success in achieving the objectives of individual cyber strikes within disputes; and also the rate of government acknowledgment of culpability in instigating cyber strikes between all of the recorded disputes featuring cyber interaction to date, the three forms of cyber dispute - disruptive, coercive and espionage driven - and the final case selected for analysis in each category. As such, this basic analysis will simply draw out patterns in behaviour and rough correlations in macro-terms between different sorts of conflicts - it is therefore intended only to complement and guide the micro, contextual analysis of the specific disputes selected for case study examination, not act as a response to the hypotheses and research questions outlined above in its own right.

With regards, then, to the data component of this analysis, as noted formerly two main datasets have been consulted for the purposes of this research - the Dyadic Cyber Incident and Dispute Dataset, Version 1.5(Valeriano and Maness, 2015*c*), and the Correlates of War Militarized Insterstate Dispute Data version 4.01(Kenwick et al. 2013), hereafter known as the DCID and MID datasets respectively. These represent some of the most comprehensive databased accounts of state interaction during disputes in their respective fields, whether through militarized or cyber means, and are particularly useful for this research as they group interactions during disputes over time, such that when combined, enable the identification of detailed patterns of behaviour between states engaged in cyber conflict. Together they yield a population of 21 disputing dyads engaged in 51 cyber and 55 militarized disputes, and which accrue 164 cyber and 599 militarized incidents respectively. In terms of distribution, only seven of these dyads do

not feature militarized interaction, whilst the split with regard to type of cyber interaction generates 13 disputes which are coercive in nature, and a further 19 each for disruptive and espionage driven disputes, from which the case studies introduced above have been drawn.

Thus, to operationalize processes of dispute continuation or escalation and bargaining, I have drawn from the frameworks of both datasets to define state responses which fall under the category of resisting a signal(on behalf of the target) and standing firm in return(for the challenger) as necessitating either: in militarized terms a display or actual offensive use of force(adapted from Kenwick et al. 2013); or in the cyber field a display of cyber strength - such as a website defacement or denial of service - or use of cyber force to conduct an offensive strike with some form of intrusion or infiltration and damage to the rival state's network(adapted from Valeriano and Maness, 2015*c*).

Similarly, in assessing the severity of incidents, comparative of both cyber and militarized actions, a combined scale will be used to objectively compare dispute severity between cases in this dissertation research, ranging from the threat of force, whether cyber or militarized, to the display or use of force through either of these mediums, and eventual escalation to actions which have the potential to place states on war footing, as outlined in Table 1(p33). Through the amalgamation of these two scales of different lengths I arrived at a cut-off point matching cyber strikes of highly destructive severity to militarized escalation to war, in line with the policy position adopted first by the US government in 2011 that serious cyber strikes capable of creating civilian casualties through, for example the disruption of power-sup- plies or emergency responder networks, can be treated as

Table 1. Overview of comparative severity and hostility scales

	Cyber Severity	Militarised Hostility	Combined level of Escalation
Severity 1	Probing without kinetic cyber	No militarised action	No malicious action taken
Severity 2	Harassment, propaganda, nuisance disruption	Threat to use force, blockade or occupy territory	Threat to use force - whether cyber or militarised
Severity 3	Stealing targeted critical information	Show of force, including militarised or nuclear alerts	Militarised display of minimal force; or form of cyber disruption inclusive of website defacement with propaganda, or denial of service attacks
Severity 4	Widespread government, economic, military or critical private sector theft of information	Substantive show of force, including mobilization of armed forces, border fortification or violation.	Militarised display of substantive force; or offensive cyber action involving intrusion or infiltration to critical networks to steal information
Severity 5	Single critical network and physical attempted destruction	Use of force through blockade, occupation of territory, or border clash.	Militarised use of force; or offensive cyber strike with, at minimum, widespread theft of critical information or the intent to destroy a critical network
Severity 6	Single critical network widespread destruction	Substantive use of force through attack, declaration of war, or use of CBR weapons	Militarised escalation to use of substantive force; or offensive cyber strike resulting in the destruction of a critical network
Severity 7	Minimal death as a direct result of cyber incident	Begin or join interstate war	Militarised escalation to war; or offensive cyber strike resulting, at minimum, in fatalities
Severity 8	Critical national economic disruption as a result of cyber incident	-	-
Severity 9	Critical national infrastructure destruction as a result of cyber incident	-	-
Severity 10	Massive death as a direct result of cyber incident	-	-

Sources - Dyadic Cyber Incident and Dispute Dataset, Version 1.5 (Valeriano and Maness, 2015); Correlates of War Militarized Insterstate Dispute Data version 4.01 (Kenwick et al. 2013)

'acts of war'(BBC News, 2011:online). Finally, in searching for possible cyber spillovers to militarized interaction, militarized incidents occurring within one calendar year of the identified signal event highlighted for each case were included for consideration, although where necessary, I have also referred back or further forward in time to significant events out-with this period if relevant.

Chapter 3: Investigating Disruptive Disputes: India - Pakistan Case Study

At first glance, of the three cyber dispute types available for analysis, those which are characterized as disruptive might fairly be assumed to be the ones in which signaling practices during interstate disputes are most evi- dent, owing to the more visible nature of disruptive cyber tactics with regard to the both the challenger and target state's domestic population. Though se- lected at random from the pool of disruptive disputes drawn from the DCID data-set, the Indo-Pakistani disruptive dispute is a most interesting subject for analysis under these circumstances, and can be argued to represent one of the most antagonistic or embittered dyads recorded, having engaged in multiple wars, numerous border clashes and many diplomatic fallouts(BBC News, 2001:online; see also Kenwick et al. 2013). Therefore, prior to the deeper foray into analysis which forms the basis of this chapter, it is first appropriate to examine at least in brief what insights previous academic commentary may shed on the issues at stake in the Indo-Pakistani dispute, as well as the wider context of their "tortured history"(Stolar, 2008:7). Thus, the chapter will precede as follows, with a brief overview of existing literature covering Indo-Pakistani relations, compounded by subsequent quantitative and greater in-depth qualitative analysis, in which key episodes and incidents within the dispute will be highlighted and contrasted with the aim of understanding more fully the impact and context of cyber signaling in this dispute.

Understanding the issues at stake in the Indo-Pakistani Dispute

Of all the sources of conflict between India and Pakistan, that which has been most frequently addressed in academic literature, and is indeed of most relevance to this research, concerns the conflicted territory of Kashmir, shared for the moment and split by the Line of Control(LoC), but claimed by both states. Pakistan, as Cheema writes "...has long believed it has moral, political, historical, and strategic reasons to stake a claim to Kashmir, which was taken by India through conspiracy and deception during the 1947 division of the Indian subcontinent... Kashmir has taken on such enormous political and psychological proportions that it is hard to imagine any Pakistani leader agreeing to give up this cause"(in Lavoy[Ed], 2009:42-43). Indeed, in the minds of Pakistani nationalists their state is "'incomplete' without Kashmir", and as such "Pakistan's claim to Kashmir was and remains irredentist"(Ganguly, 1995:169).

For India, on the other hand, claiming Kashmir - as a lone majority Muslim province, in contrast to the rest of India's administrative regions - bolsters its secular democratic credentials and national identity, the very reverse of the nationalistic Pakistani arguments which in effect assert that Kashmir's religious makeup naturally ought to have made it a part of Pakistan's territory following partition(Cheema, in Lavoy[Ed], 2009:43). Between them, India and Pakistan have fought three wars over Kashmir; during 1947-8, 1965 and again in 1999 - and as Ganguly notes, despite being of 'low intensity' this conflict has dragged on one way or another for over fifty years, such that "its significance overshadows all other issues in the region"(1995:168). This significance is often most visible in both militarized and cyber incidents between the two states, particularly, for ex-

ample, in the aftermath of an attack - or attempted attack - by Pakistani-based militants operating in Indian territory after covert entrance via the LoC separating Pakistani and Indian-administered Kashmir. Common estimates suggest that around the beginning of the Indo-Pakistani cyber dispute there may have been as many as 3000 such militants - motivated at least in part by the desire to see Kashmir fully ceded to Pakistani jurisdiction - operating in Indian controlled territory, with, as Kampani suggests, the ongoing issues created around the activities of and attacks carried out by these Pakistani-backed or based militants in Indian land amounting to one of the most significant obstacles to better relations between the states, eroding Indian trust in commitments made by Pakistan across a variety of treaty or other agreements(2002:online).

Essentially, thus, for both India and Pakistan, whilst the issue of Kashmir itself is not always at the immediate fore of hostilities, the territorial conflict at the heart of their interstate dispute is of such huge import and symbolic value it remains critical to the tenor of their interstate relations, at the very least linked in some aspect, to almost every one of the issues of contention which spring up between them - whether through the operations or even underlying motivations of militant groups, or in quarrels over policies or local governance issues in the Kashmir region - and is therefore, unsurprisingly, the driving motivation behind many of the cyber disputes, assessed in the remainder of this chapter.

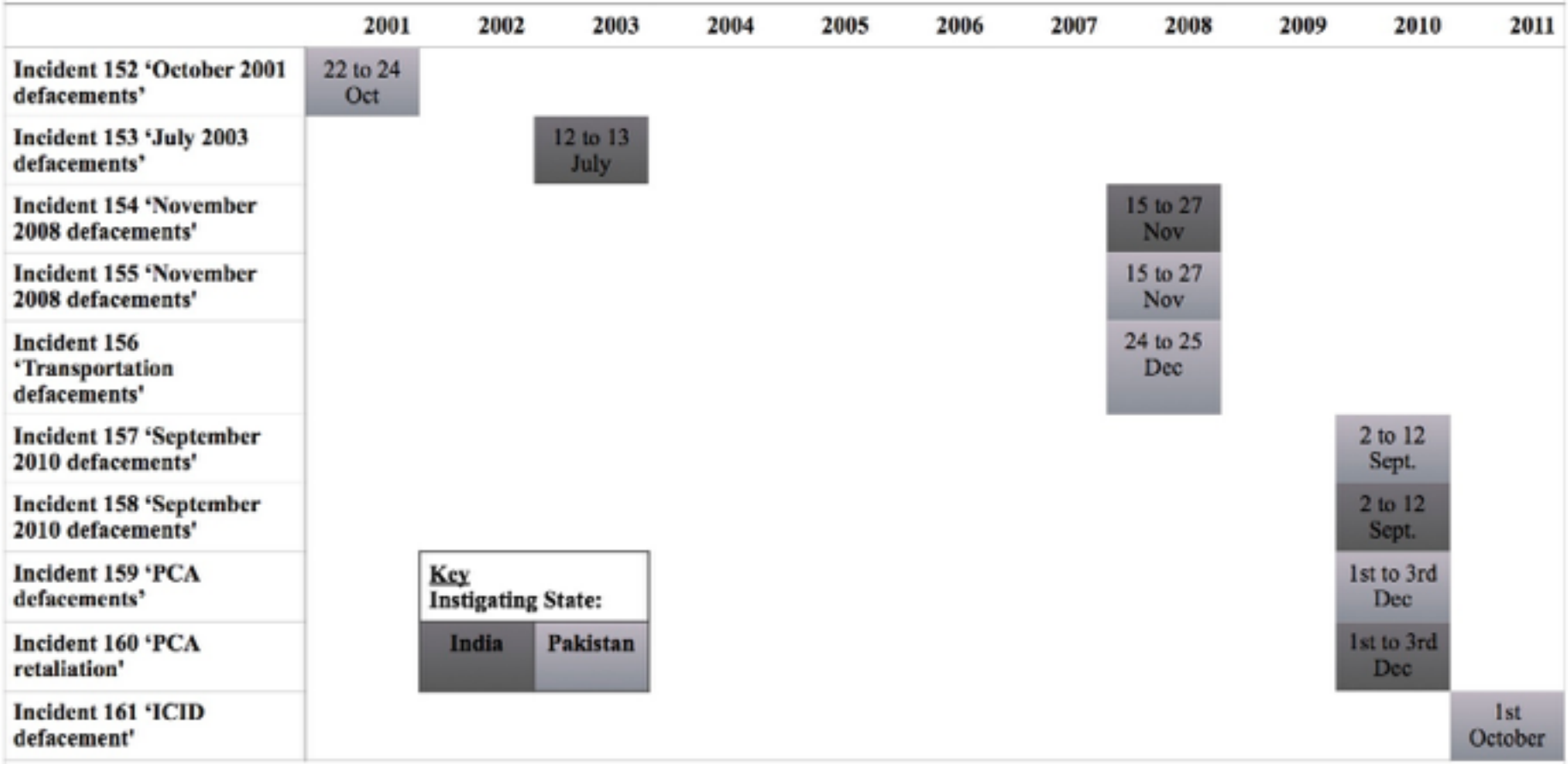
Analysis

What nuances or dynamics, then, can some comparative statistical analysis of the combined DCID and CoW MID datasets reveal with regard to the

Indo-Pakistani dispute and disruptive disputes more generally? Initial observations would suggest, not wholly unexpectedly, that in comparing the the India-Pakistan case to all disruptive disputes, this is one of the longest running conflicts of the set, with a total of 10 cyber incidents spread over 3632 days, and is of roughly the same level of cyber severity, containing mainly defacement and denial of service strikes which harass rather than cause system-wide damage(see Figure 2, overleaf and Table 2,p.40). Indeed, the type of damage created by these cyber strikes tended both in the wider disruptive dispute data, the final sample and Indo-Pakistani case study to be of direct and immediate impact, however somewhat differently, in the Indo-Pakistani dispute these strikes can be seen to have been consistently more effective in achieving their disruptive target objectives, with a thirteen per cent greater rate of success than the mean rate across the disruptive disputes as a whole and the final sample. Similarly, and again unsurprisingly given the intransigence of the territorial issue at stake of the Indo-Pakistani dispute, cyber interaction for this case is by far more visible than disruptive disputes or cyber disputes more generally - with every single incident acknowledged by the perpetrating state, perhaps reflecting the febrile, emotive nature of the conflict.

Finally, and most interestingly, after comparing the volume and severity of cyber and militarized interactions, it appears evident that as the level of cyber severity increases, so do the number of cyber interactions, whilst the inverse is true of militarized interactions - with the most severe forms of cyber disputes associated with the fewest number of MIDs per dyad(Kenwick et al. 2013, and Valeriano and Maness, 2015*c*; see also appendix for further details). Consequently,

Figure 2. India - Pakistan : Overview of Chronological Cyber Interaction



Source: DCID Dataset, Valeriano and Maness (2015).

1101319

Table 2. Statistical Comparison of the Indo-Pakistani Dispute Against Wider Cyber Interaction

	All Disputes	Disruptive Disputes	Final Sample of 3	India - Pakistan
Total Number of Incidents	164	45	21	10
Mean Number of Incidents	3.22	2.37	7	-
Length of Dispute [days]	38,952.00	7,113.00	6448.00	3632.00
Mean Length of Dispute [days]	763.76	374.37	2149.33	-
Dispute Intensity [days per incident]	228.47	70.06	302.49	363.20
Mean Severity Equivalent to	Stealing target critical information [2.94]	Harassment, nuisance [2.11]	Harassment, nuisance [2.00]	Harassment, nuisance [2.00]
Prevailing Damage Type	Direct and Immediate	Direct and Immediate	Direct and Immediate	Direct and Immediate
Rate of Success	60%	67%	67%	80%
Rate of Incidents Acknowledged by States	37%	48%	76%	100%

Source: DCID Dataset (Valeriano and Maness, 2015).

there are several possible avenues for exploration which follow logically from the above - do cyber disputes with lower severity coincide with greater military interaction, as states gravitate more towards military escalation as a means of expressing their resolve rather than employing escalatory cyber tactics? By the same token, do disputes with higher cyber severity levels foster fewer incidences of military interaction because most of the coercive diplomacy and signaling is done through cyber interaction? Certainly, it would appear that for the Indo-Pakistani dispute that bouts of hostile militarized interaction are not only routine, but outstrip cyber strikes in terms of regularity, with 114 MIDs occurring within 3457

calendar days, thereby creating a dispute intensity of only 30.32 days per incident(against the 363.20 days per cyber incident). Until digging deeper into the case specific figures of the South Korea-Japan and US-China disputes no wider comparison may yet here be made, but the possibility of spillover from cyber to militarized conflict, and the implications this may have for cyber signaling practices merits further investigation as this chapter delves deeper into analysis.

Episode 1 - 2001 Indo-Pakistani Kashmir Dispute

Between the 22nd and 24th of October 2001, Pakistan instigated what would be the first of many spells of hostile cyber interaction at times against and at others perpetrated by their neighbour and enduring rival, India(Valeriano and Maness, 2015*c*). The cyber strike, which revolved around the defacement of Indian government websites, occurred in a highly charged atmosphere in the wake of an attack at the start of the month on Kashmir's state legislature - the Srinagar Assembly, located in Indian-administered Kashmir - which claimed the lives of 38 people, and was perpetrated by Pakistani-based militants, perceived in India as enjoying Pakistan's full state-support, though denied by the Pakistani government, despite the failure to control their side of the border dividing Kashmir, or apprehend the militants responsible(*Ibid*; BBC News, 2002:online).

Asides from marking the beginning of tactical cyber strikes between the two states, this bout of hostile interaction also represents the first potential evidence of cyber signaling in the Indo-Pakistani dispute, where Pakistan chose to underline the strength of their commitment to the position adopted by President Musharraf in the following diplomatic fallout initially through cyber and not the

rather more frequently selected option of military displays, or the actual use of force. Indeed, with regard to the wider strategic context in which this portion of the Indo-Pakistani dispute took place, during the six months prior to this cyber incident there had been two recorded MIDs between the sides, and a further 17 in the same period following, the bulk of which involved small scale clashes, with few known fatalities, across the state borderline(Kenwick et al., 2013). Despite this relatively high density of hostile militarized interaction there were no further cyber incidents in the same calendar period, the vast majority of state interaction carried out instead through militarized terms.

What impact, therefore, can Pakistan's cyber signal be seen to have had on the crisis dynamics? Figure 3(p.43), displays the pattern of interaction between India and Pakistan, with Pakistan beginning engagement in the first instance through cyber defacement strikes against Indian government web- sites, and within the same period, between the 22nd and 24th of October, displaying force through a militarized alert which concluded on the 26th of October, ranking at three - displaying force only - on the combined severity scale for each. India's response was also militarized, upping the ante and severity level to five - the use of militarized force - as they instigated a border clash on the 11th of November, which was then reciprocated by Pakistan over the next twenty four hours, in which time Indian fatalities were recorded at five, Pakistani fatalities unknown(Kenwick et al., 2013;Kampani, 2002:online). Following Pakistan's retaliation, no further bouts of cyber or militarized hostility were recorded in the following calendar month, with India, the target state, losing out in the zero-sum calculus of

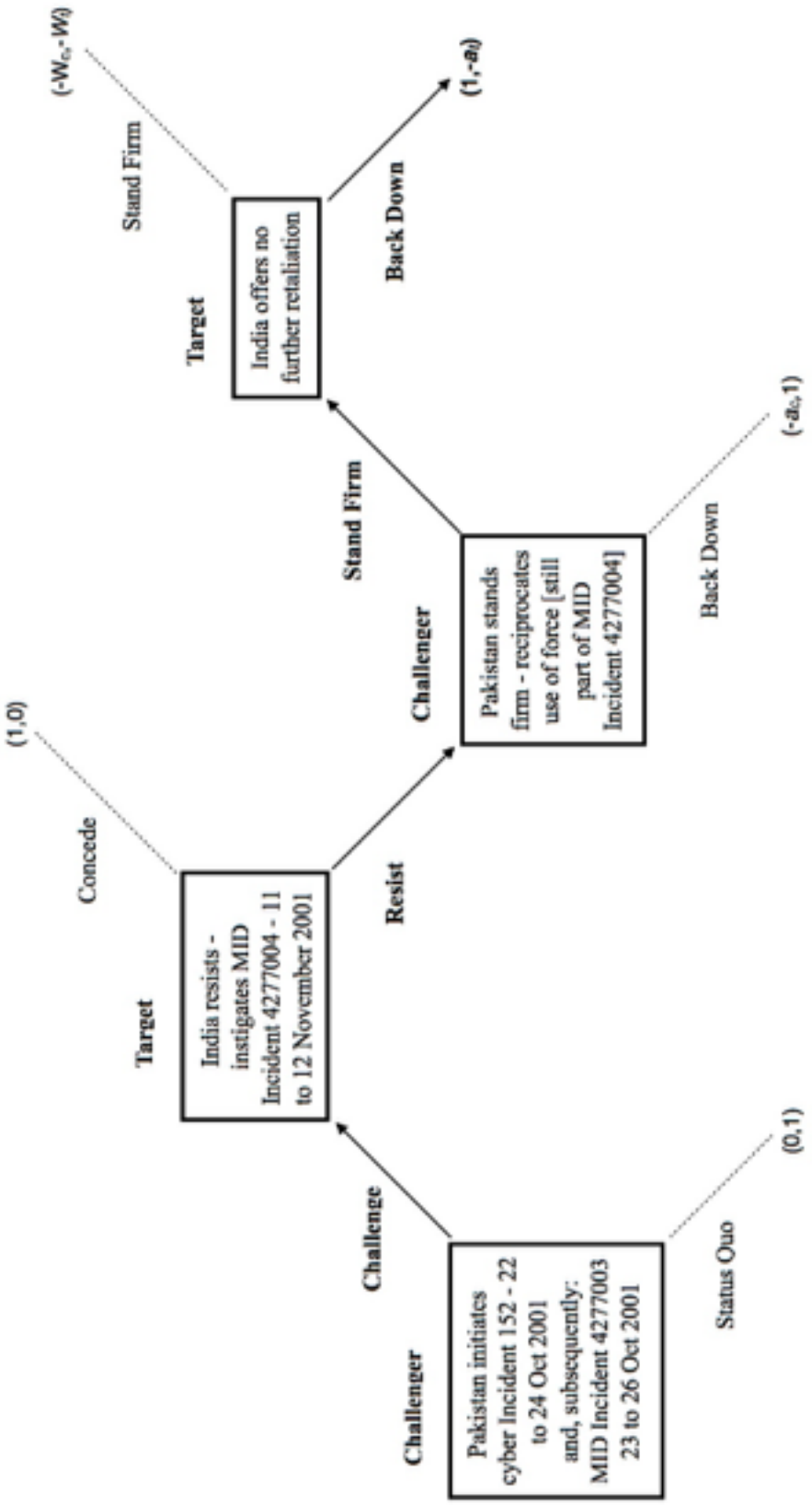


Figure 3. India - Pakistan October 2001 Kashmir Dispute Chronological Interaction

Schultz's model, initially resisting, but after the clashes of the 11th and 12th of November offering no further hostile action.

It should be noted, however, that whilst further escalation was at this point avoided, little over a month later a further terror attack on Indian soil, again perpetrated by Pakistani-based militants, renewed hostilities which then carried on into 2002, yet being non-state sanctioned or perpetrated, this could not be not counted as part of the same state-level dispute-cycle.

Thus with reference to the hypotheses, can Pakistan's cyber display of force be considered a signal interchangeable to militarized tactics in the exchange with Indian foreign policy decision makers, and further, did it have an impact on dispute escalation or restraint? Looking solely at this bout of interaction it would seem that cyber tactics were deployed in a signaling capacity which operated alongside and interchangeably with militarized tactics, thus fulfilling H1. On the other hand, while meeting the criteria of being visible to the target state's public and openly acknowledged by the instigator, the impact of Pakistan's cyber signal is difficult to extricate from its combined effect with the militarized alert actioned to compound it.

Certainly there is evidence of an escalatory impact, posited as one of two potential outcomes in H2, yet the effect of the cyber signal alone on dispute dynamics in this instance cannot be empirically verified, and thus neither can H2 be fulfilled outright, the question of whether or not cyber signaling can impact interstate relations, for the time being, unanswered. To avoid assuming that this one episode of the Indo-Pakistani dispute can be taken as constitutive of an entire and lengthy conflict, however, I now turn to a second period of interaction in the hope

that further insight may be gained from reflection of this episode against a second, and somewhat different strand of the dispute.

Episode 2 - 2008 Indo-Pakistani Border Dispute

Though several years later, a second period which bears some potential for analysis in this long running dispute can also be described as falling within a charged context - occurring less than a month after the Mumbai Terror Attacks of November 2008. It is of particular interest as rather than the challenger signaling resolve through cyber means, this time the target can be seen to signal its commitment to resistance through the use of cyber force of greater severity than in first episode detailed in this work. In retaliation against a militarized incident not recorded in the MID data-set - in which Indian Air Force jets violated Pakistani airspace - before actioning any militarized response, Pakistan first responded to India's show of force with a crippling denial of service cyber strike, which forced offline public transportation websites on the 25th of December, a nationally observed holiday. This was followed by the mobilization of Pakistani troops, relocated in their thousands from the western border with Afghanistan, to the eastern border with India(Global Security, 2008:online), yet saw no similar or reciprocal action taken by the Indian government, and by the zero-sum terms set out in Schultz's bargaining model, represented a further loss, at the least in reputation, for Indian foreign policy decision takers. Figure 4. overleaf, replicates this pattern of interaction.

With respect to the hypotheses, it would appear that this episode again confirms the interchangeable use of militarized and cyber means in signaling tac

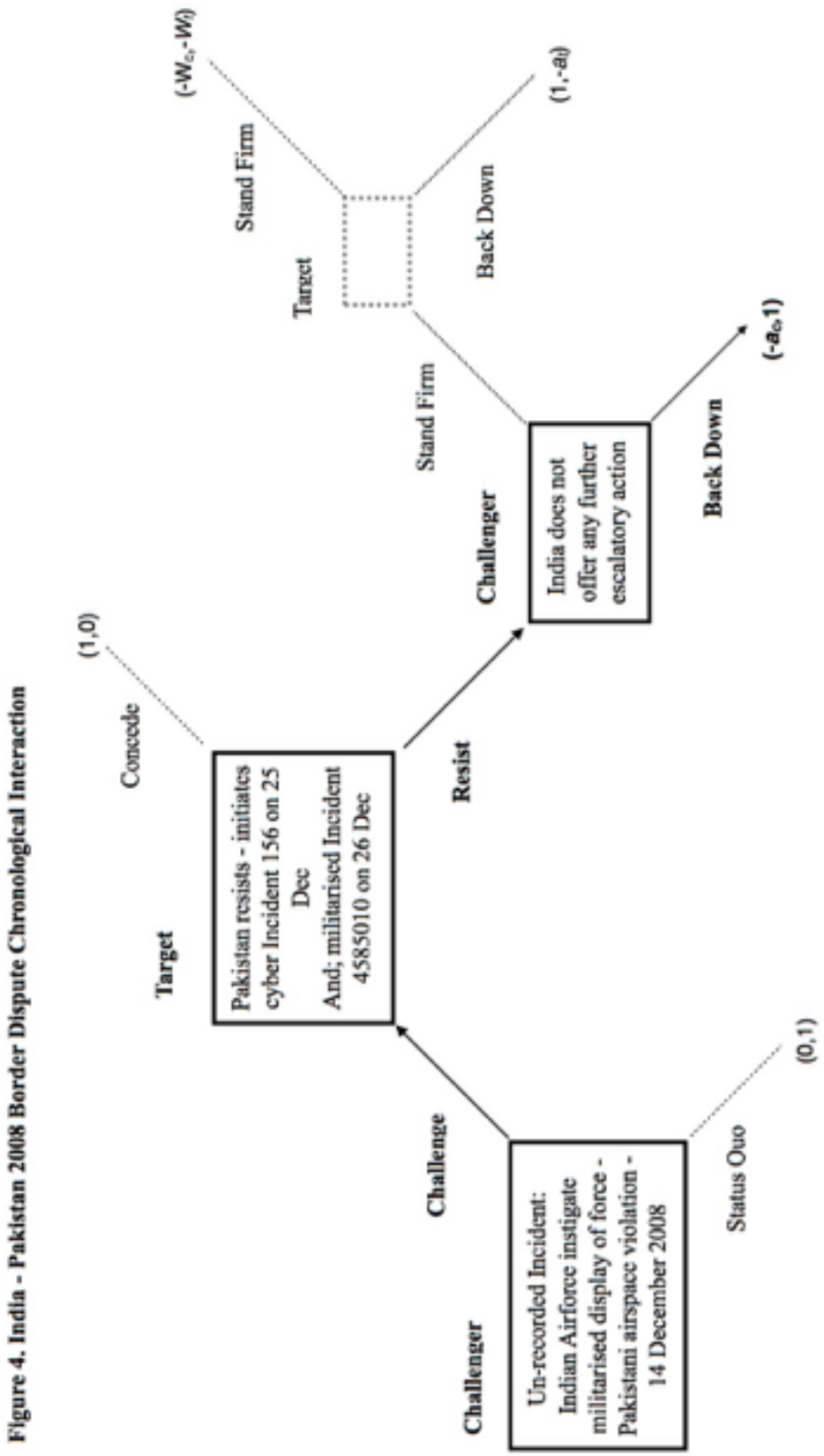


Figure 4. India - Pakistan 2008 Border Dispute Chronological Interaction

tics during disputes, albeit with the cyber interaction once again backed up by a militarized display of force. While this fulfills H1, it once more leaves question marks over H2 - Pakistan's successful denial of service attack on Indian transportation websites was publicly acknowledged and most definitely highly visible to the Indian populace, yet it was the mobilization of Pakistani troops toward the Indian border which generated the more drastic impact, certainly in terms of statements made in the accompanying news media reports in which reports of the troops amassing on the border were given greater prominence(Global Security, 2008:online; Oppel and Masood, 2008:online). In terms of actual impact to Indo-Pakistani relations, similarly to the first episode considered in this analysis, a war of words took place, with declarations of their readiness to resort to the use of force made by both sides, though fortunately, the worst of these scenarios - all out conflict - did not come to pass despite lingering hostility(*Ibid*). Thus, once more, H2 is only partially fulfilled, and cannot be accepted outright.

How then do the two episodes compare? Interestingly, in contrast to the first episode investigated in this case study, the number of MIDs experienced in the six calendar months preceding and following this bout decrease significantly from the figure of nineteen to nine, with only eight MIDs in the latter half of 2008, and one towards the start of 2009. Again differently, however, the number of cyber incidents in the same period increases from none to two - both falling in the month previous, around the time of the Mumbai terror attacks, as India sought to castigate Pakistan for its perceived support of Islamist militant groups operating on Indian soil, and Pakistan retaliated virtually in kind with its own series of website defacements(Valeriano and Maness, 2015*c*).

Does the difference in circumstances, and tactics, for each episode offer some explanation as to why in one circumstance joint cyber and militarized signaling practices appeared to escalate the dispute, while in the other restrain it toward negotiation and mediation? True enough, on both occasions cyber tactics prefaced the adoption of hostile military actions, yet arguably, the situation of episode one amongst MIDs can be seen to render it more pervasively hostile, with the prospect of all-out conflict so much more real than in the time-frame surrounding the second episode.

This is not to say, however, that cyber tactics are lost entirely in circumstances with greater military interaction, rather, that the contextual settings in both episodes play a crucial role in amplifying or detracting from the impact of the cyber signal. Indeed, as the first cyber strike between the states, use of this technology in a tactical capacity was perhaps still in it's infancy for both India and Pakistan, and as such the lesser amount of cyber interaction surrounding the first episode of interaction studied should not overly detract from the gravity of this sequence of events. On the other hand, hitting transportation websites with a denial of service strike during a national holiday is a particularly noticeable form of cyber strike with regard to the effect on India's own domestic population, and the drastic rise in tensions this has the potential to inflame would raise the stakes of the dispute, at least indirectly, with an enraged population far more likely to exert pressure on their government to exact some form of revenge. In comparison to first episode, thus, disrupting a key public service platform had the potential to send a far clearer commitment to follow through on Pakistani military officials' various oaths to robustly defend Pakistan's interests and territory(Oppel and Ma-

sood, 2008:online), as well as simultaneously creating a psychological impact on the Indian population. Arguably such a brazen manoeuvre, which risked inflaming Indian public sentiment, could apply further pressure to the Indian Government, for whom further escalation of the dispute, or a further public increase in hostility, could lock decision makers into a spiral towards open conflict.

In short, this chapter has sought to assess what influence potential cyber-signals may have had on the Indo-Pakistani cyber dispute, using Schultz's theoretical model of signals in crisis bargaining as a guide, and deploying a brief quantitative analysis to piece together a picture of the strategic context in which inter-state relations between the dyad were conducted. While not providing outright evidence of impactful cyber-signals, the use of cyber tac- tics in this case and in a signaling capacity at the very least, represents grounds for further exploration of the concept across alternative contexts.

Chapter 4: Investigating Coercive Disputes: South Korea - Japan Case Study

Reporting on anti-Japan protests in Seoul during March 2005, BBC News reporter Charles Scanlon observed, "Visitors to South Korea could be forgiven for thinking the country was on the verge of war. Newspaper headlines accuse Japan of a new invasion for claiming sovereignty over a cluster of disputed islands. Overwhelmed by fury, protesters have sliced off fingers, set themselves on fire, and in one case committed suicide by jumping off a bridge"(BBC News, 2005:online). As noted in previous chapters, precious few issues are as intractable, emotive or symbolically laden as disputed territories(Vasquez and Valeriano, 2008), and although not the soul issue at stake in the South Korea-Japanese conflict, the outpouring of fury and hysteria described by Scanlon encapsulates the potent and bitter enmity engendered by the many eruptions of contention experienced between these two states over the intervening years since World War Two. This chapter follows the same template as that of the Indo-Pakistani case study, engaging in a brief overview of the South Korea-Japan relationship, and it's historical legacy, prior to evaluating through statistical and qualitative means the patterns of behaviour of these states during an interstate dispute, with the aim of determining to what effect cyber signaling practices are deployed in periods of crisis.

Explaining the South Korea-Japan Relationship

The territorial dispute concerning the Tokdo Islands, as they are known in South Korea, or Takeshima, in Japan, is, as alluded to in the introduction, part of a wider issue of controversy rooted in Japanese colonial occupation of the Korean peninsula for some years prior to and during the Second World War, and compounded by the failure, as perceived by South Korea, of Japanese leaders to "fully atone for Japanese actions during the Second World War"(King and Taylor, 2016:115-6). Highlighted as the "key site of the history-spiral between Japan and South Korea"(*Ibid*:114), a "perennial irritant"(Scanlan, 2005:online); and "tinderbox"(Takahashi, 2005:1), the Tokdo/Takeshima Islands can be argued to embody connotations of historical animosity, and from the South Korean perspective, injustice. Indeed, as Chung Dong-young, the chairman of South Korea's National Security Council said of Japan's repeated claims to the Islands, "[T]his is not simply a territorial issue, but is nothing short of a denial of the history of our national liberation as well as a justification of past aggression"(BBC News, 2005).

While previously there has been some successful attempts at cooperation with regard to the territorial dispute, as Valencia cautions, though the Japan-South Korea fisheries agreement of 1985 allowed Japanese fisherman to operate within South Korean territorial waters, the post-WWII 'Peace Line' boundary which granted South Korea authority of the seas up to 200 nautical miles outwards from its coast and banned Japanese vessels from returning to the waters surrounding the peninsula "has not been formally withdrawn" and could yet be reinforced, should the rival claims of sovereignty over the Tokdo/Takeshima Islands continue to threaten further conflict between the states(2007:141-2). Thus, after a fashion, the issue of

the Tokdo/Takeshima territories remains somewhat precariously balanced, representing on the one hand, as Koo observes, "one of the most fundamental barriers to better bilateral relations", yet has been "contained" and "repeatedly prevented... from escalating into a full-scale diplomatic crisis" through close economic interdependence(2005:online).

However, reading further into the 2005 statement from Chung Dong-young, chairman of South Korea's National Security Council, it can also be posited that although a significant issue in it's own right, the territorial dispute surrounding the Tokdo/Takeshima Islands is inseparably bound to the legacy of Japan's colonial past in South Korea. Quite simply, as Kimura posits, conflicts involving South Korea and Japan "are not simply concerned with historical facts but rather with perceptions"(in Söderberg [Ed], 2011:21), indeed it is arguable that "international relations of Northeast Asia are seemingly being held hostage to history"(King and Taylor, 2016:111). While it is therefore unsurprising that rival claims over these small islands inflame such hostile responses as those documented above, it would also be a mistake to overlook the associated if less overtly inflammatory or militarized issues which spring from the period in which Japan occupied the Korean peninsula, committing crimes such as the forced sexual enslavement of 'comfort women' for Japanese soldiers, and the subsequent failure to fully acknowledge publicly or take responsibility for such actions(*Ibid*:115-6).

In short, ergo, I will follow commentators such as Takahashi in my own analysis, recognizing that bouts of hostility fueled by South Korean anger towards questions of atonement, Japanese revisions to or the removal of historical wartime atrocities in school textbooks, alongside symbolic visits to contentious war

shrines, find a focal point in the ongoing Tokdo/Takeshima Islands dispute, which can in turn be conceived of as representing a "microcosm of Japan's brutal colonial occupation"(2005:2) as I move forwards into analysis.

Analysis

In statistical terms the South Korea-Japan coercive cyber dispute is in some regards remarkably different, in others unexpectedly similar to that of the disruptive Indo-Pakistani conflict. Where the latter represented one of the longest running and frequently active disputes of its type in the DCID, the coercive dispute conducted by South Korea and Japan also contains more incidents than the mean number recorded both across the data-set and within coercive disputes separately, yet falls far short of the number experienced in the previous case study, as shown overleaf in Table 3 and Figure 5.

A similar pattern is evident also in dispute intensity levels, where South Korea and Japan accrue a higher number of days per incident than is the mean amount experienced again across the entire data-set and coercive disputes themselves. Unlike many of the other cyber disputes contained in the same coercive sample, South Korea and Japan have enjoyed a greater rate of success in their targeted cyber objectives - at a rate of 75 per cent in comparison to 54 - and likewise have acknowledged or accepted culpability for the cyber strikes they have actioned on every occasion as opposed to the mean rate of 49 per cent in coercive disputes, and 37 in all cyber disputes of DCID more generally.

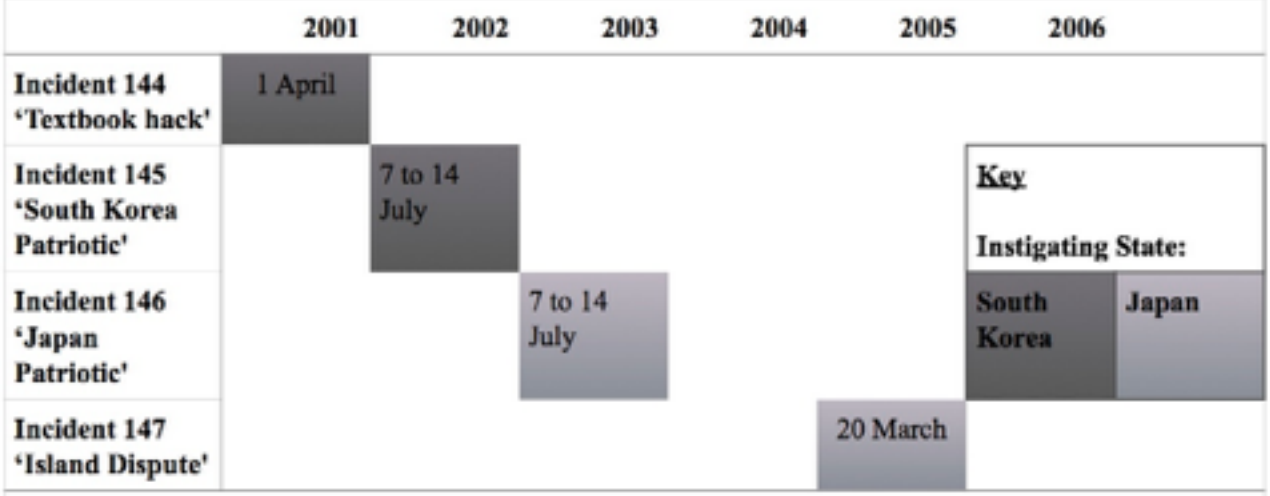
One particular item of note, however, concerns the much lower level of severity generated by South Korea and Japan's cyber dispute. Where the mean level across

Table 3. Statistical Comparison of the South Korea - Japan Dispute Against Wider Cyber Interaction

	All Disputes	Coercive Disputes	Final Sample of Three	S Korea - Japan
Total Number of Incidents	164	37	10	4
Mean Number of Incidents	3.22	2.85	3.33	-
Length of Dispute [days]	38,952.00	9254.00	2837.00	1450.00
Mean Length of Dispute [days]	763.76	711.85	945.67	-
Dispute Intensity [days per incident]	228.47	205.94	274.94	362.50
Mean Severity Equivalent to	Stealing target critical information [2.94]	Widespread theft of critical information [3.54]	Stealing target critical information [3.33]	Harassment, nuisance [2.00]
Prevailing Damage Type	Direct and Immediate	Direct and Immediate	Direct and Immediate	Direct and Immediate
Rate of Success	61%	54%	50%	75%
Rate of Incidents Acknowledged by States	37%	49%	100%	100%

Source: DCID Dataset (Valeriano and Maness, 2015).

Figure 5. South Korea - Japan : Overview of Chronological Cyber Interaction



Source: DCID Dataset, Valeriano and Maness (2015).

coercive disputes - regarded as the more severe form of cyber interaction(Valeriano and Maness, 2015*c*) - is equatable to the widespread compromise of, or theft from critical networks(at a score of 3.54), cyber operations instigated by both South Korea and Japan tended towards being disruptive and harassing in nature, involving denial of service and defacement actions against websites. Intriguingly despite this lower than anticipated severity score for cyber interaction, the South Korea-Japan dyad do not, within the same time-frame, engage in a particularly high number of MIDs, registering only six which mainly involving aerial displays of force, with fighter jets scrambled to patrol the area around contested Island chain. Previously in this dissertation work the pattern between cyber disputes of lower severity tending to experience a greater number of militarized incidents than their high severity counterparts, has been though of as perhaps indicative of states adopting militarized means to communicate resolve or anger during crisis periods without escalating issues in the cyber realm, yet following this train of thought, either the reasoning behind this logic is, for this case flawed and the trend in the statistics is purely coincidental; or the South Korea-Japan dispute represents an outlier with regard to coercive cyber disputes in terms of severity.

However, given the emotionally charged terms of the Tokdo/Takeshima dispute, as outlined in the overview above, it is entirely possible that the contextual dynamics unique to the South Korea-Japan rivalry may shed some light on why seemingly less damaging cyber strikes can still wreak a serious impact on the rival states, particularly where the terms of dispute are so loaded. This potential avenue for deeper research forms the basis of the episode-based analysis below.

Episode 1 - 2005 Tokdo/Takeshima Island Dispute

Though not chronologically the first malicious cyber interaction between South Korea and Japan, the period surrounding the 2005 uptick in the Tokdo/ Takeshima issue represents the best opportunity to examine patterns of behaviour, and potential signaling in their coercive dispute, through both cyber and militarized means. In no small part this is due to the four militarized incidents and one cyber strike carried out between the eighth and twentieth of March, of which the only cyber and two of the militarized incidents were instigated by Japan, the remaining two MIDs initiated by South Korea(Valeriano and Maness, 2015*c*). The spark for this somewhat unanticipated burst of hostilities can be found, as Koo notes, in Japan's proposed inaugural 'Takeshima Day' on the twenty-second of February, a particularly inflammatory move given that this date coincided with the "centennial anniversary of the issuance in 1905 of a prefectural ordinance that had incorporated the islands as Japanese territory", a precursor to the full invasion and colonization of the Korean peninsula five years later(2005:online).

Shortly afterwards, and in response to protests from both the South Korean civilian population and government - who demanded "genuine reflection and an apology"(Scanlon, BBC News, 2005:online) - on the eight of March Japanese fighter jets conducted a display of aerial force above the disputed grounds, triggering, as visualized in Figure 6, overleaf, a cycle of retaliatory displays of aerial force which, though initiated by Japan, was mirrored by South Korea until culminating in the cyber vandalism of South Korean governmental websites, at which point, with no further hostile interaction in the following calendar month, this particular period of the dispute can be seen to end. Excluding those involved in the

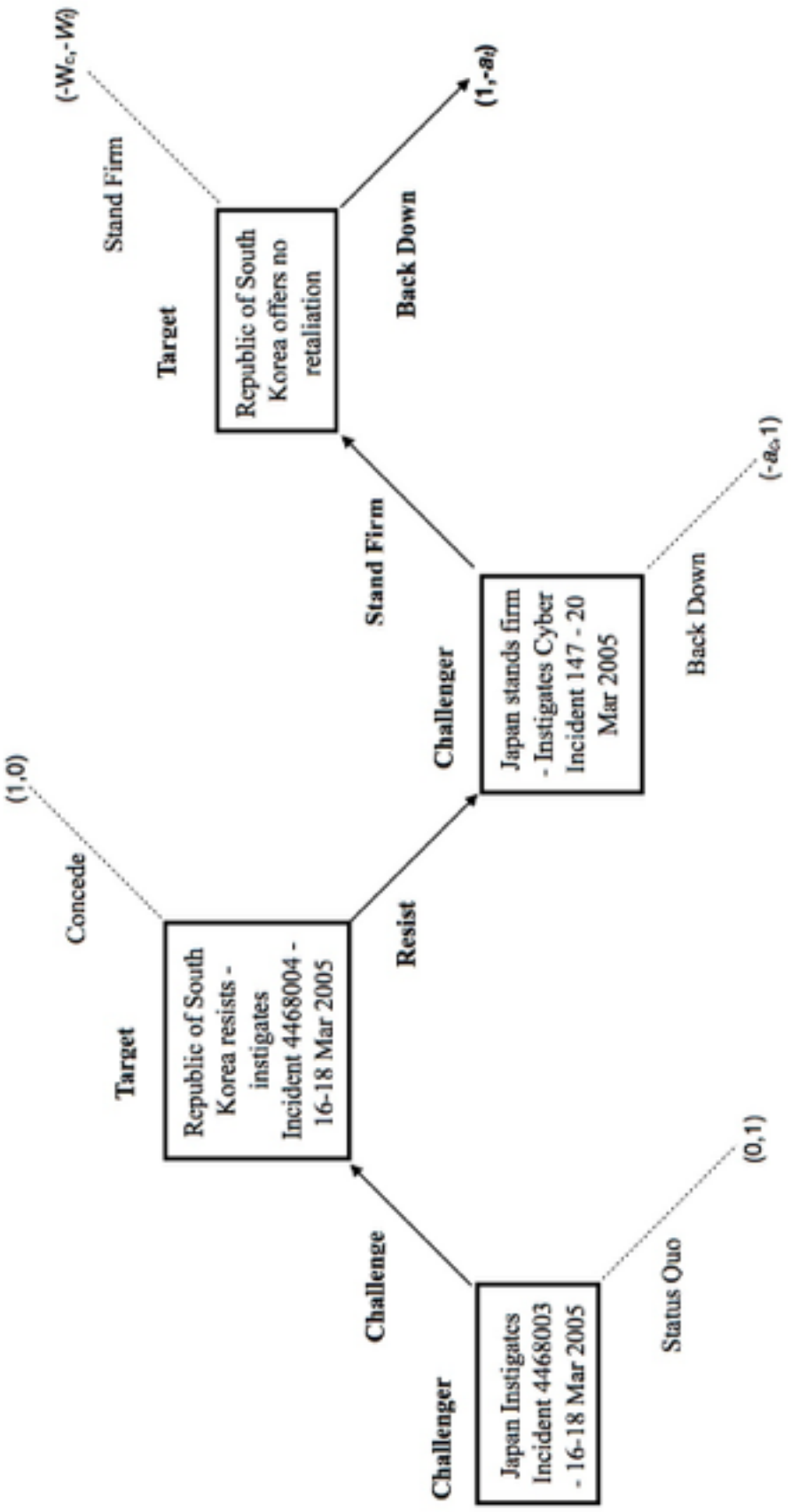


Figure 6. Republic of South Korea - Japan 2005 Tokdo Island Dispute Chronological Interaction

dispute pattern outlined in Figure 6, in the six months prior to and following this rupture between South Korea and Japan, no militarized or cyber incidents took place prior to the eighth of March, while only two militarized incidents occurred in the aftermath, almost four months later in July, involving yet another series of reciprocal aerial militarized alerts initiated by Japan in the first instance, South Korea in the second, and after which no further MIDs occurred until well into 2006(Kenwick et al, 2013).

How do these events measure against the criteria set out in the hypotheses? H1 is again fulfilled, with cyber tactics deployed interchangeably by Japan alongside militarized displays of force in it's sequence of signaling measures. In terms of repercussions or impact to relations between the states, damage was done - following Schultz's model, in relative terms South Korea can be seen to lose this round of the crisis bargaining game, taking no further escalatory action and standing down in the wake of the Japanese cyber strike, despite the outpouring of anger expressed by the domestic South Korean population. Further, as reported on by news organizations including the BBC, during the immediate aftermath the South Korean foreign minister canceled a planned state visit to Japan, whilst culture activities including football matches and exchange programmes were also called off, with the South Korean government quoted as stating "it considers sovereignty over the islands as more important than good relations with Japan"(Scanlon, BBC News, 2005:online). On the Japanese side, as Takahashi notes, "Foreign Minister Machimura Nobutaka said Tokyo would find it difficult to resume stalled talks quickly on signing a free-trade agreement with South Korea this year" in lieu of the renewed hostilities(2005:1). Yet contrary to the senti-

ment behind these statements, no retaliatory cyber or militarized measures were taken in response to this offensive tactic, which on the surface would seem to indicate its efficacy in communicating the strength of Japanese commitment to firmly defend its position in the debate surrounding the disputed Islands.

On the other hand, it has been suggested elsewhere that the defacement of South Korean government websites was of little influence to the continuation of the aerial displays and rather, it was at the behest of their mutual ally, the United States of America, that South Korea and Japan drew a halt to hostilities(Maness and Valeriano, in Friis and Ringsmose[Eds], 2016:56; see also Palmer et al. 2015). However, as far as can be seen in the CoW MID data-set, and within the scope of this work, no further militarized incident is recorded to have taken place for almost four months in the aftermath of the Japanese cyber strike in this 2005 conflict episode. Therefore, whilst I do not seek to completely contradict the argument outlined by these scholars, or undermine the mediating role played by the US in seeking to calm the situation, I believe the cessation of displays of force in the wake of Japan's cyber strike does raise the possibility that there may have been some impact associated with this cyber signal, at the very least in the short term. In fact, when considered alongside such crucial contextual features as the outpouring of ferocity witnessed by Scanlan in the anti-Japanese protests which represented a prelude to this bout of conflict, in acting so publicly, Japan deployed a cyber tactic which exerted a huge psychological impact on the target population - who in turn, in their anger exerted pressure on their leaders to take punitive action - and in doing so showed a willingness to push the South Korean

government to the brink of being locked into inevitable escalation to war, as envisioned by Schultz(2012:371)

Thus, it would appear that H2 can be considered in this instance fulfilled - while the cyber tactic was used after militarized interaction and cannot be judged independently of this context, it was nonetheless visible to the target state populace, acknowledged by the perpetrators and effectively forced the South Korean government into a position from which they would have to retaliate and risk outright hostilities, or engage, as was the option selected, in some form of negotiation(Ministry of Foreign Affairs of Japan, 2005:online). Regardless, this bout of interaction does not represent the sole period of conflict in the Japan - South Korea dispute, and as such, after comparison with an earlier period of animosity, the opportunity for further reflection on the matter will follow presently.

Episode 2 - 2004 "cyber-imjinwaeran" Dispute

In stark contrast to the episode outlined above, during this 2004 cyber scrap neither South Korea or Japan resorted to the use of militarized tactics - indeed, nor, in the 6 months either side of the event, were any MIDs recorded in the CoW data-set(Kenwick et al., 2013). Instead, and most unusually, official state responses during the flare up were limited to condemnations of the rival government's actions and retaliatory bouts of denial of service at- tacks against official state websites over the course of a week between the seventh and fourteenth of January(Valeriano and Maness, 2015*c*). After a rather more oblique fashion, the issue driving this round of hostility can also be seen as being linked to the Tokdo/ Takeshima Islands dispute, centering specifically on the publication by South Ko-

rea of stamps commemorating the Tokdo Islands, all 2.2 million of which were sold out in around three hours, and to which Japanese officials swiftly proposed a rival 'Takeshima Islands' edition as nationalist protests engulfed both states(Valencia, 2005:79).

For this episode then, no interchangeable use of cyber and militarized signals or tactics can be recorded and as such H1 is unfulfilled. Instead, as is evident in Figure 7, overleaf, a hostile bout of cyber interaction through retaliatory denial of service attacks served to communicate both states' resolve to defend their claims, dubbed "the "cyber-imjinwaeran," referring to the Korean-Japanese war of 1592-98"(Koo, 2005:online). After greater inspection of the strategic environment in which South Korea and Japan were operating at this moment in time, in truth it is questionable in this instance if there was any prospect for militarized spillover - though angered by one anothers actions attempts were made by both sides to prevent the rising hostility from transferring to open militarized interaction: Japan, for example, prevented several of its own citizens from landing on the disputed Islands against the wishes of the South Korean authorities, while the then South Korean president, Roh Moo Hyun, also sought to defuse anti-Japan protests(Koo, 2005:online). With important multi-party talks led by the US regarding North Korea's nuclear ambitions on the horizon, and increased economic interdependence in the wake of their 2003 free trade agreement it is conceivable both states were prepared to find a negotiated settlement of the issue in order to prevent wider damage to relations, and able to gauge from the fierce reactions of their respective domestic constituencies to the uptick that any further escalation could potentially lock leaders into an escalatory conflict spiral - or result in drastic

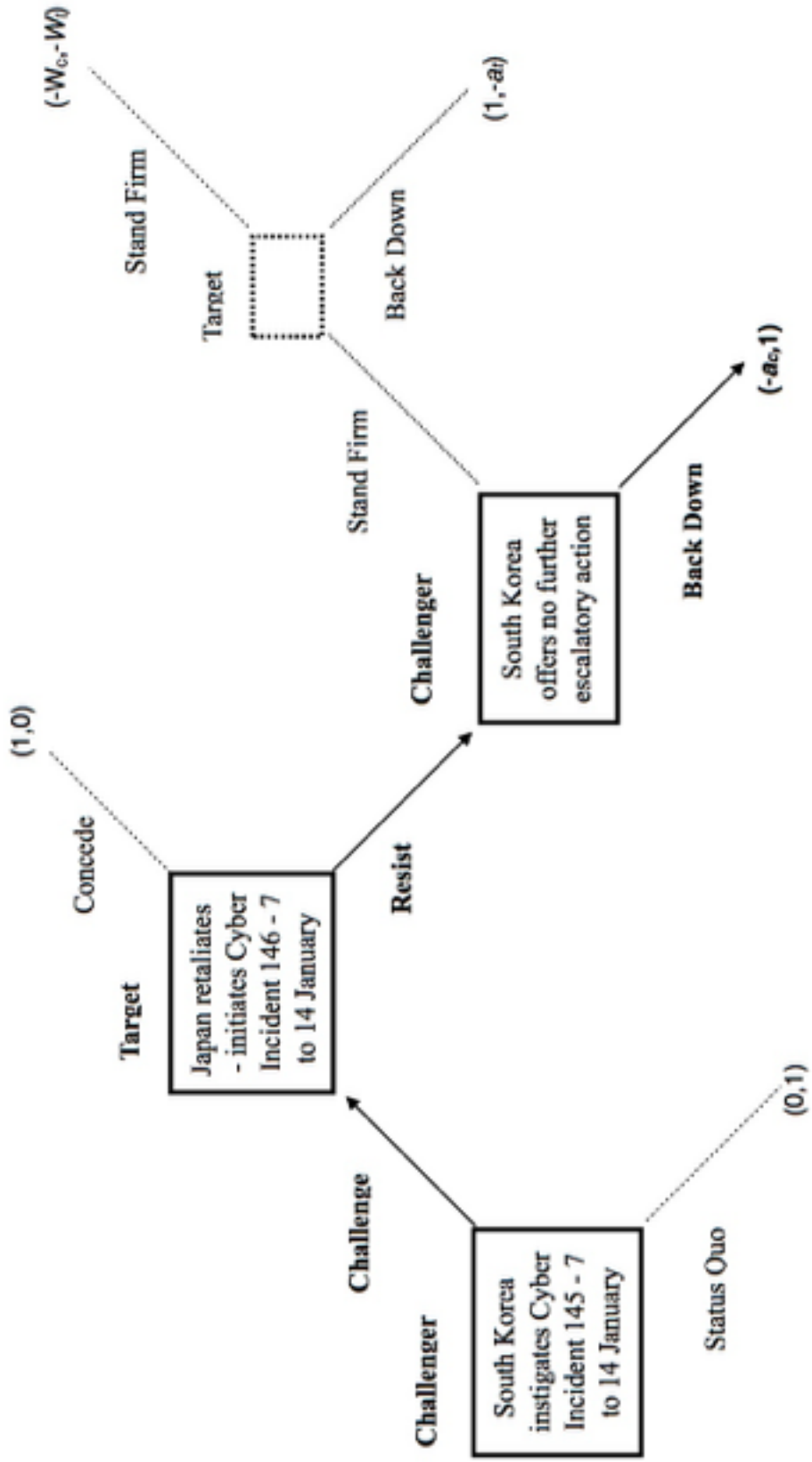


Figure 7. South Korea - Japan 2004 Tokdo Island Dispute Chronological Interaction

backlash should leaders attempt to defuse the situation at a later date(*Ibid*). As such, when set against the criteria laid out in H2 it would appear that the use cyber of cyber-signals did in this dispute have a clear impact on dispute dynamics, were both visible to target populations and acknowledged by perpetrating states, and thus H2 is also fulfilled.

Drawing towards a conclusion of this portion of analysis, in comparing this episode to that which was carried out a year later in 2005, and indeed to those from the Indo-Pakistani dispute of the previous chapter, several key points arise for consideration to take forwards, chief among which is the apparent inconsistency in the effect which the least severe Japanese cyber strike appeared to extol in an erstwhile militarized clash with South Korea in 2005. For the Indo-Pakistani dispute it is arguable that the cyber event of greater severity was that which carried greater weight, or exerted a more noticeable impact on dispute dynamics when deployed in conjuncture with militarized incidents. On the one hand this suggests that the matter of context, or circumstantial variables once again threaten to overshadow distinctions in cyber means and tactics - though a bitter dispute in its own right, at no point during the episodes covered in the Indo-Pakistani dispute were there reports matching the level of protest(including suicide, self-immolation and self-harm, Scanlon, 2005:online) as in the 2005 South Korean anti-Japanese demonstrations. Nevertheless it is also plausible that the relatively more minor skirmish from 2004, conducted purely through cyber means by South Korea and Japan itself paved the way for such considerably heightened tensions between the states, so that when MIDs did finally break out the following year, there were several in a short space of time which escalated to the use of tactics with which the

2004 online skirmish was carried out - highly visible cyber strikes which would antagonize an already impassioned South Korean population and raise the stakes of the issue towards the real prospect of outright escalation to conflict.

By way of conclusion, this chapter has focused on the coercive cyber dispute conducted by South Korea and Japan over the contested Tokdo/Takeshima Island chain. Again, as with the Indo-Pakistani dispute, though both hypotheses could not be fulfilled across all episodes analyzed in this section, there existed definite indications of cyber signaling practices influencing dispute dynamics during both the 2004 and 2005 surges of hostility. Thus, looking forwards, a final comparison of these cases might shed greater light still on the question of what impact cyber-signals exert on interstate disputes in the forthcoming examination of the last form of cyber conflict to be assessed - the U.S.-China cyber espionage dispute.

Chapter 5: Investigating Espionage Driven Disputes: United States of America - People's Republic of China Case Study

As noted from the outset, this form of cyber dispute is, on paper at least, the most challenging to align with the concept of state signaling in interstate disputes. By their very nature, cyber strikes actioned for the purpose of espionage are secretive affairs - if visible, or indeed announced or publicly acknowledged in some way prematurely by the perpetrators they are hardly likely to succeed in compromising secure networks and obtaining their target information. Despite this, and though few and far between, there is some evidence of the deployment of cyber-signals in the US-China espionage dispute, which for the purposes of analytical clarity has been reduced from 43 incidents to the 12 incidents concerning attempts at cyber espionage, or defence from cyber espionage, which revolve around access to military networks and information, inclusive of defence contractors and civilian DoD systems, in order to enable greater context-specific analysis. The structure of this chapter follows thus - after a short sketch of existing thoughts on the matter of US-Chinese relations and the impact of cyber espionage from the academic, news and defence communities, it will proceed to a statistical and qualitative examination of the episodes in which US-China cyber interactions, for all their secrecy, may be seen to replicate something of a signaling practice, before finally drawing from both previous analytical chapters and cases to reflect on where states may use cyber means to signal to one another during crises, yet

also what actual impact these cyber-signals may have on dispute dynamics across a variety of different contexts and circumstances.

Sino-American Relations and the Cyber Espionage Dispute

Much has been written about the ongoing cyber interactions of the United States of America and People's Republic of China - "by far the world's most cyber-active dyad"(Pytlak and Mitchell, in Friis and Ringsmose[Eds], 2016:77). In a way this is unsurprising, for as Jensen, Valeriano and Maness allude to, given that the participants include China "the most active cyber instigator in the international system" and the US - one of the few states to conduct "an impactful denial cyber coercive incident"(2016 - forthcoming) - this espionage laden dispute can be thought of as particularly significant. On the other hand, unlike either of the previous cases covered in this work, there does not exist, in the same sense, a turbulent ongoing enmity rooted in historical conflict between these states which could prolong feelings of hostility singularly between the two states - rather, as Gompert and Libicki note, if at all, the US and China would most likely be drawn into conflict through events in the South or East China Sea, for example with US escalation or intervention perhaps through defensive commitments to an ally such as Japan; to prevent the seizure by China of disputed islands or the enforcement of the controversial Chinese 'air-defence identification zone'(2014:9- 10).

In cyber terms, Maness and Valeriano suggest, the driving force behind the ongoing US-China cyber dispute can be understood from the Chinese perspective as an urgent need to address the imbalance between its own cyber and conventional capabilities in order to catch up to the international hegemon - the Unit-

ed States - with cyber espionage representing an opportunity for China to ensure that then technological gulf between the US and itself does not grow too large(in Friis and Ringsmose[Eds], 2016:49). Part of the problem of associated with this, however, is that "Chinese strategists have accused the United States of launching similar espionage campaigns, and therefore assume that the utilization of cyber tactics is now part of the normal relations range between states," and thus, with little inclination to think otherwise, the potential for escalation is misread - "For China, the concept of spill-over from the cyber to the conventional arena is expected"(*Ibid*). Moreover, as Lindsay, Cheung and Reveron point out, the distinction between forms of cyber espionage, or at least "American attempts to articulate the difference between the political-military targets of U.S. cyber espionage and the economic targets of Chinese espionage... have tended to fall on deaf ears"(2015:online), thereby frustrating attempts to build some form of consensus around what can be considered acceptable cyber behaviour, what is a viable defensive tactic, and what is economic or intellectual property theft.

As a result, as Lindsay warns, "Cyber operations and the rhetorical reactions to them on both sides of the Pacific have undermined trust in the Sino-American relationship"(2015:8), indeed, the entire relationship between the states, write Pytlak and Mitchell, is accurately "described as an uneasy balance of cooperation and competition, with each of those terms carrying more or less weight at different moments over the last half century"(in Friis and Ringsmose[Eds], 2016:77). Thus, in carrying these insights onward into the following analysis section of this chapter, I hope to establish where these issues of competition are made

manifest through cyber interaction, and the communication of resolve for both states' respective positions.

Analysis

In statistical terms, it is more than fair to describe the US-China espionage dispute as one of the largest, and most severe of all those captured in the DCID data-set While China is without doubt the more aggressive, or active, of the two disputing states - with 36 of the 43 dyadic interactions attributed to Chinese state hackers - both sides have initiated cyber strikes of startlingly sophisticated and damaging capacity. As outlined in Table 4, overleaf, with a total of 43 incidents between them, alone the US-China account for approximately 26 per cent of the incidents contained within the DCID data-set, as well as more than half of all recorded incidents in espionage disputes. Unsurprisingly with such a high number of incidents the dispute intensity score is strikingly low in comparison to the data-set as a whole and espionage driven disputes more generally, with only 110.42 days per dispute(against 228.47 for all disputes, and 402.30 for espionage conflicts), though this figure does rise to 395.67 when the US-Chinese cyber interaction is reduced to focus solely on the twelve cases of espionage related to militarized networks and contractors. Ranked in the DCID data-set as having a severity of five across the wider US-Chinese dispute, equatable to the attempted destruction of a critical network(Valeriano and Maness, 2015*c*), it is safe to say that this dispute is of greater severity in terms of the cyber tactics used and damage inflicted than either of the previous cases selected for closer analysis here, also dwarfing the mean severity level from the entire DCID data-set and across

Table 4. Statistical Comparison of the U.S. - China Dispute Against Wider Cyber Interaction

	All Disputes	Espionage Disputes	US-China - Whole Dispute	US-China - Military Espionage
Total Number of Incidents	164	82	43	12
Mean Number of Incidents	3.22	4.32	-	-
Length of Dispute [days]	38,952.00	22,585.00	4748 .00	4748 .00
Mean Length of Dispute [days]	763.76	1188.68	-	-
Dispute Intensity [days per incident]	228.47	402.30	110.421	395.67
Mean Severity Equivalent to	Stealing target critical information [2.94]	Stealing target critical information [3.37]	Attempted destruction of physical and single critical network [5.00]	Widespread theft of critical information [4.00]
Prevailing Damage Type	Direct and Immediate	Direct and Immediate	Direct and Immediate	Direct and Immediate
Rate of Success	60%	60%	74%	75%
Rate of Incidents Acknowledged by States	37%	25%	40%	25%

Source: DCID Dataset (Valeriano and Maness, 2015).

espionage disputes, even for the final sample of twelve military-espionage disputes. Interestingly however, the number of MIDs recorded between this dyad rank at only five, so that despite their vastly greater volume of cyber interactions, in militaristic terms there is little to separate this case with that of the South Korea-Japan series of displays of force.

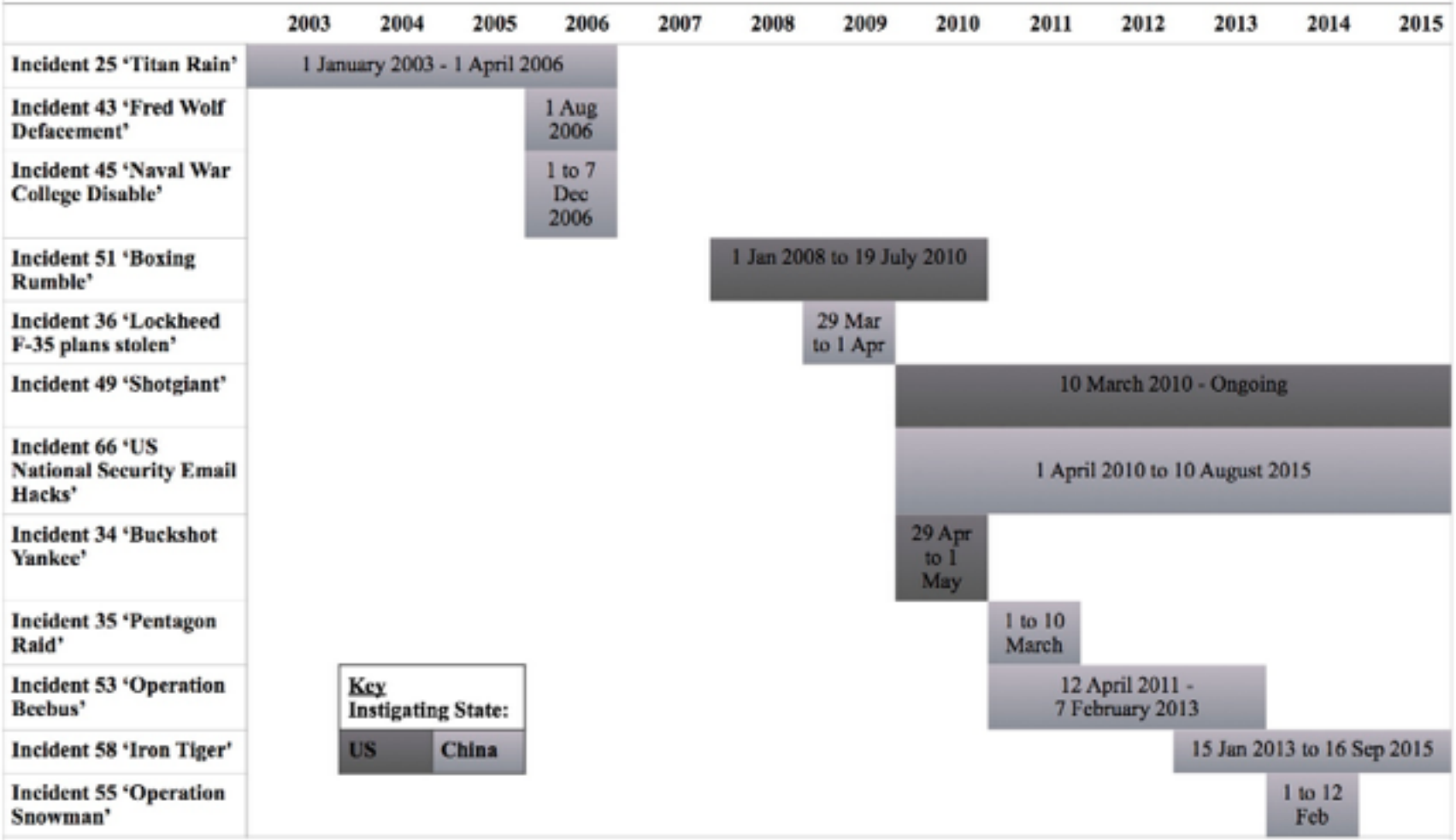
In terms of the rate of success of these cyber strikes, roughly three-quarters of the cyber espionage incidents achieved their target objectives - out

stripping the mean level of both the espionage and all disputes by fifteen per cent - while once more, damage tended as in all cases towards being of direct and immediate impact. Again, not unexpectedly, espionage driven disputes show a much lower rate of state acknowledgment or acceptance than the mean score across all disputes in the DCID data-set, and while the US- China dispute records at first glance, in the matter of military espionage it is no exception, with only a quarter of incidents admitted by the participating states. Nevertheless, slender though this rate of state transparency is when it comes to claiming espionage cyber strikes, a key component in communicating a signal, there are reasonable grounds for further examination of those few incidents which have been openly accepted by the state level perpetrators, and which form the subject of the forthcoming qualitative analyses.

Episode of Interest – 2010 Military Espionage

As can be seen in Fig 8, overleaf, even slimmed down to only those incidents concerning military and defence networks, the US-China Espionage dispute is a complex affair, with many long-running, advanced persistent threat cyber operations which overlap, and in some places are - at the time of writing - ongoing. Within these 12 incidents, as uncovered in a recent piece of research by Jensen, Valeriano and Maness, are two of the "most impactful cyber coercive incidents" recorded to date - the 'Boxing Rumble' incident of 2008 - 2010, a defensive denial operation launched by the US against Chinese espionage directed at the Departments of Defense(DoD) network, which led to the suspension of operations against the DoD through "changing the cost-benefit calculus of launching

Figure 8. US - China : Overview of Chronological Interaction



Source: DCID Dataset, Valeriano and Maness (2015).

1101319

cyber coercive methods" by essentially flooding any would-be attackers' networks with a "denial of service barrage"(2016 - forthcoming). And secondly, in addition, on China's part there was also a highly successful raid on the Lockheed Martin defence contractor's schematics for the F35 fighter jet, contained in the DoD's network, which given the highly sensitive "top secret" nature of the material stolen, can be counted as a significant blow to the target and a significant gain for those in China seeking to close the technological gulf in military capacity through espionage(*Ibid*).

The episode of the dispute most relevant to this work, however, occurs after the successes of the US' defensive 'Boxing Rumble' and China's theft of the Lockheed Martin F35 fighter jet plans, revolving instead around a sequence of cyber interactions which took place almost precisely a year after the Lockheed Martin theft, where China initiated a renewed attack on the US military complex - this time through the hacking of US National Security email systems - and the US some weeks later launched and publicly acknowledged a new defensive operation 'Buckshot Yankee', a virus aimed at comprising the networks of those who at-tempted to intrude and steal information from the Pentagon's system, similarly to 'Boxing Rumble' by raising the costs incurred through retaliation(Valeriano and Maness, 2015*c*; illustrated overleaf, in Figure 9). Though without any militarized overspill or interaction within the time-frame of six months on either side of the events themselves, this episode can be seen, if only by the intentions behind it, to represent something close to an attempted cyber signaling pattern, with the US response to Chinese espionage designed to demonstrate both resistance to the Chinese challenge and resolve in their own position.

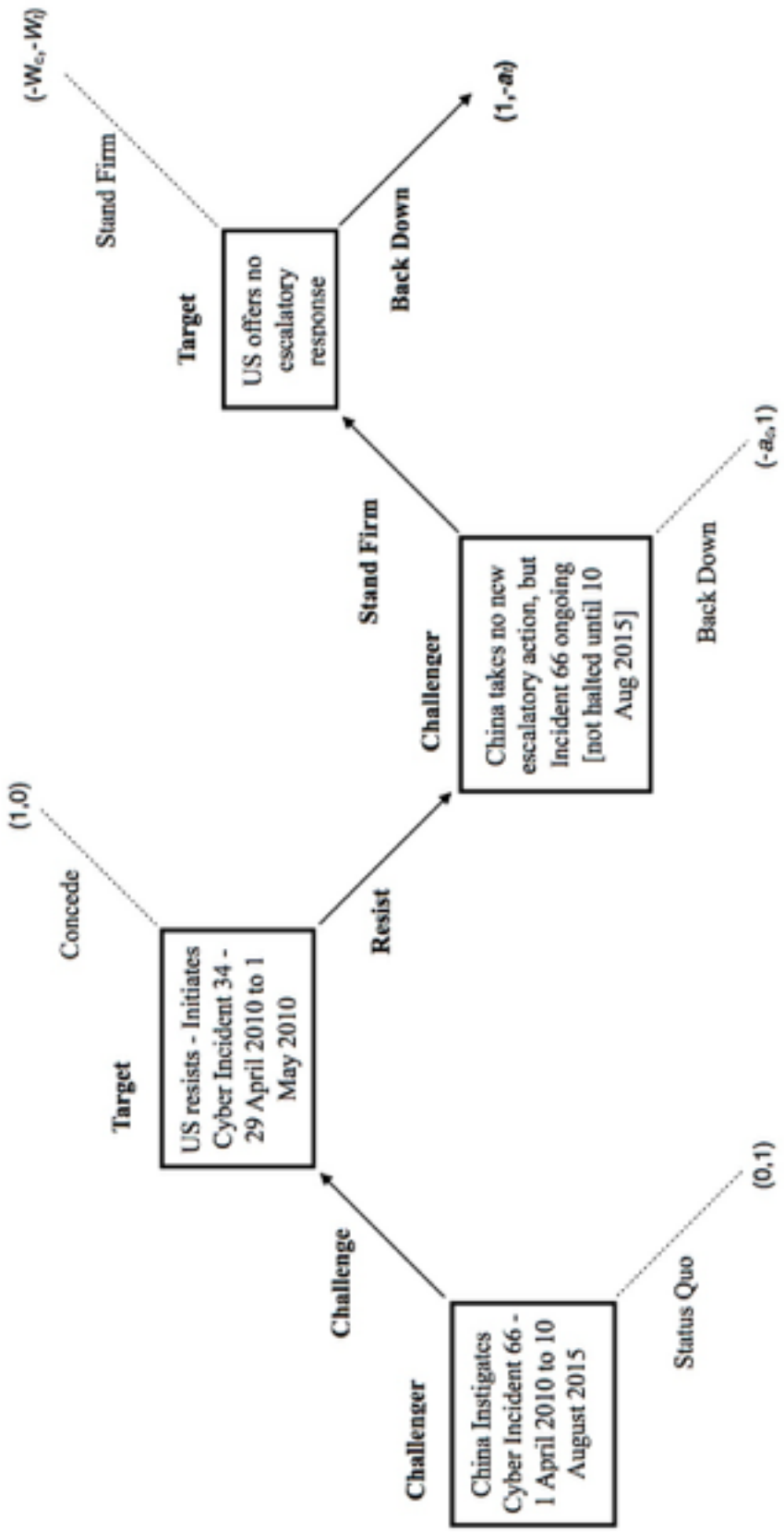


Figure 9. US-China 2010 Military Espionage Chronological Interaction

Ultimately, following the logic of Schultz's model of signals in crisis bargaining, in simple terms the US can be seen to have lost out in this bout of interaction with China, failing to counter-escalate against China's ongoing military cyber espionage, despite a further four cyber strikes over the subsequent four years, in addition to the ongoing hacking of US national security emails cyber incident which started this particular episode of cyber conflict.

Did this episode therefore translate into an event with meaningful impact on US-China relations? Arguably not. While offensive Chinese cyber strikes continued - the next almost flaunting the defensive objective of 'Buckshot Yankee' by raiding 24,000 sensitive files directly from the Pentagon's network - the US, contrary to its stated aims of raising the costs of cyber espionage through retaliation, and condemnation of further malicious cyber strikes, demonstrated a remarkable restraint, in not taking punitive countermeasures(Valeriano and Maness, 2015*b*).

Thus, it is difficult to see how in this case how the US' attempted cyber signaling through operation Buckshot Yankee exerted any particular impact on the dynamics at play in the US-China Espionage Dispute. Even despite the success of operations such as the 'Boxing Rumble' Chinese hackers were not deterred ultimately from attempting to gain access to and filter information from networks concerning the US military, or defence technology development firms, arguably switching targets from those networks the US did manage to successfully defend, but not relinquishing the overall aim to overcome American military and technological advantages through cyber theft. Ergo, in lieu of evidence to the contrary, for this episode, neither of the hypotheses can be accepted - cyber tactics were not deployed interchangeably with militarized alternatives, nor did the publicly ac-

knowledged cyber operation 'Buckshot Yankee' wreak any escalatory or restraining impact on the cyber espionage dispute dynam- ics. Consequently, H1 and H2 are rejected, and the null hypotheses fulfilled for each.

Comparing Cyber-signals Across Cases

What then can be said of the differences in contexts, motivations and actions during these three interstate disputes with regard to cyber signaling practices? Overall this dissertation unearths a mixed picture of the impact of cyber signaling on interstate dispute dynamics, with no clear or consistent patterns of behaviour common to all three kinds of conflicts - where militarized and cyber incidents were so fully intertwined in the Indo-Pakistani dispute as to fulfill H1 in both episodes studied, that very closeness and inseparability of militarized from cyber-signals also negated the possibility of verifying H2 outright. For South Korea and Japan, on the other hand, in both instances there was an impact associated with their cyber-signals - though different in each episode - yet militarized and cyber tactics were not deployed interchangeably across the dispute and as such H2 was accepted while H1 went unfulfilled overall. In contrast to either of the above, despite the potential for impactful signaling in the US-China espionage dispute, neither H1, nor H2 could be fulfilled - cyber and militarized tactics were not operationalized alongside one another, and in the event of an attempted cyber signal from the US there was no measurable impact on Chinese actions in the ongoing dispute.

Where does this leave the investigation of cyber signaling practices this dissertation set out to accomplish? In short it demonstrates the uneven variability

of the tactic - where some cyber-signals generated the kind of impact posited at the start of this research, were of positive outcome in that they restrained disputes between states by pushing both parties toward negotiation, or were of negative result - escalating hostility rather than constraining it - yet others yielded negligible influence to the ongoing conduct of cyber contests. By the same token, however, in writing the above I could equally observe the same of militarized signals, which in the selected case studies were of mixed outcome also - some of negligible impact and some escalatory or restraining ilk.

Certainly, there are issues which may undermine or influence the effect of any given signal – as Maness and Valeriano note, the fact that so many cyber disputes are conducted between regional dyads implies that territorial issues or contention over regional policies may play a role in their own right in exacerbating, even instigating hostile cyber interaction(in Friis and Ringsmose[Eds], 2016:57). Indeed, history too, after the same fashion can be argued to colour the terms of dispute, and determine at least in part, how a signal, cyber or otherwise may be received – as noted by Pytlak and Mitchell in comparing Sino-Japanese and Sino-American interactions to conclude that despite being of lesser severity, historic Sino-Japanese animosity rendered their cyber interactions more antagonistic(in Friis and Ringsmose[Eds], 2016:79). Similarly the extreme reactions documented in the South Korea-Japan dispute vindicate Gibler and Hutchison when they highlight the importance of territorial issue saliency in exacerbating the effects of the audience cost mechanism(2013:882). Arguably, though playing an important role in the signaling process, such contextual considerations as these do

not overshadow or undermine the act in itself, rather they influence how it is received and by extension, what impact it has.

Essentially, then, it would appear the success, or ability of a signal to exert a non-negligible impact on a dispute could be argued to come down to a variety of factors, yet is unequivocally dependent on the context in which it is delivered - for example, with particular reference to the fevered atmospheres of the Indo-Pakistani and South Korea-Japan disputes it is nearly impossible to judge if the measures adopted by the respective governments in authorizing cyber strikes would have had the same meaning or exacted the same response in an atmosphere or situation which was not so volatile.

I have not tried to simply explore or argue how signaling practices can work - as is shown above for both cyber and militarized forms of signaling there are plenty of circumstances in which they do not impart an impact – rather, to suggest that through misperception or miscalculation crises can escalate, or equally, through demonstrating the possibility of spiraling conflict, signals may restrain hostile interstate relations. On the basis of the conclusions reached here, while not fully confirmed across all cases it is conceivable that cyber-signals carry some impact, when issue saliency, or an embittered historical legacy, combines with public acknowledgment and cyber strikes visible to their respective target populaces to create the circumstances conducive to triggering the audience cost mechanism which underpins Schultz's theory of signaling.

Thus, by choosing not to skip over context and focus on wider macro analysis of cyber disputes, whilst this dissertation might have sacrificed some analytical clarity or universal applicability it has been able to gain better understand-

ing of the role of context, history and issue saliency in formulating the circumstances unique to each individual case in which signaling practices can wield an important influence on dispute escalation or termination.

Drawing towards a close, this chapter has in the first instance sought to apply Schultz's theory of signaling during interstate crises to the case of the US-China cyber espionage dispute, finding that for the episode analyzed, there was no clear evidence of the U.S.' cyber signal having any negligible impact on the conduct of further cyber interactions. As a result, in compar- ing all three case studies selected for analysis, it has been unable to fully conclude outright that cyber-signals are capable of influencing any dispute where they are publicly acknowledged and visible to domestic audiences, accepting instead that such effects are realized only in specific, historically-charged or impassioned environments.

Conclusion and Limitations

In final reflection, this dissertation research sought to probe the question of whether cyber-signals performed by states during periods of interstate crises could have significant impact on these crises, such that cyber tactics would be deployed alongside militarized ones as part of the same strategic spectrum. It has been guided by the works of past and present scholars including Fearon, Valeriano and Maness, Lindsay, and Gibler and Hutchison, amongst many others, and given analytical purchase and structure by Schultz's theory of signaling resolve during periods of crisis bargaining between states(2001). Drawing from the incomparable resources of the Correlates of War and Dyadic Cyber Incident and Dispute datasets has enabled a mixed methodological approach which employed both basic comparative statistical and detailed qualitative analyses, as well as providing a pool from which to extract three case studies representative of their constituent types of cyber disputes – a disruptive series of cyber and militarized clashes between India and Pakistan; a coercive conflict involving South Korea and Japan; and finally an espionage filled dispute featuring the United States of America and People's Republic of China.

After much reflection and comparison between these distinct cases and conflicts, a partial fulfillment only of the hypotheses driving this research could be accepted – where evidence of impactful cyber-signals both restraining and escalating tensions between disputants was unearthed between South Korea and Japan, so too were scenarios in which cyber-signals could be seen to have little

impact at all on the ongoing conduct of disputes, such as that of the US and China's cyber espionage encounters.

It is therefore unsurprising that there are several limitations associated with this methodological approach - not least the restriction to three cases out of many which may have proven fruitful to analysis. Indeed, ideally there could have been greater and more sophisticated empirical quantitative examination of trends in behaviour across not only the three case study disputes, but all recorded in the DCID data-set, while updated militarized incidents would also have enabled further tandem exploration of the more recent cyber incidents ongoing at the time of writing. Perhaps most seriously of all, however, the close focus on contextual settings and factors affecting the cyber disputes selected, while useful in fully understanding how cyber-signals impact interstate relations, limited the extent to which this analysis is universally applicable or comparable - the insights gained into understanding processes which determine the efficacy of cyber tactics unique to their individual circumstances. Yet, despite these drawbacks, and on balance, it is arguable this dissertation can be considered to represent a starting point, if not a foundation on which to build further and deeper study of this important, oft under-explored area of international relations.

Bibliography

BBC News.(2001). 'India and Pakistan, Tense Neighbours' Accessed on 14/06/2016. Available at: http://news.bbc.co.uk/1/hi/world/south_asia/102201.stm

BBC News.(2002). 'India-Pakistan:Troubled Relations' Accessed on 14/06/2016. Available at: http://news.bbc.co.uk/hi/english/static/in_depth/south_asia/2002/india_pakistan/timeline/2001.stm

BBC News.(2005). 'S Korea Protest over Japan Claim'. Accessed on 28/06/2016. Available at: http://news.bbc.co.uk/1/hi/world/asia-pacific/4352923.stm

BBC News.(2011). 'US Pentagon to treat cyber-attacks as 'acts of war'' Accessed on 20/05/2016. Available at : http://www.bbc.co.uk/news/world-us-canada-13614125

BBC News.(2016). 'US sentences Chinese hacker for stealing military information' Accessed on 28/06/2016. Available at http://www.bbc.co.uk/news/world-us-canada-36791114

Brown, J. N., and Marcum, A. S.(2011). 'Avoiding audience costs: Domestic political accountability and concessions in crisis diplomacy.' *Security Studies*, 20(2), pp. 141-170.

Cheema, Z. I.(2009) 'The strategic context of the Kargil conflict: a Pakistani perspective' in Lavoy, P. [Ed] *Asymmetric Warfare in South Asia: The Causes and Consequences of the Kargil Conflict*. pp.41-63

The Economist,(2005). 'Rocky Relations' Accessed on 28/06/2016. Available at: http://www.economist.com/node/3795319

Faiola, A.(2005). 'Islands Come Between South Korea and Japan' *Washington Post*. Acessed on 28/06/2015. Available at: http://www.washingtonpost.-com/wp-dyn/articles/A41813-2005Mar16.html

Fearon, J. D.(1994). 'Domestic political audiences and the escalation of international disputes.' *American Political Science Review*, *88*(03), pp. 577-592.

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

Fern, S.(1998). Tokdo or Takeshima? The international law of territorial acquisition in the Japan-Korea island dispute. *Fordham Int'l LJ*, *1606*, 1611.

Ganguly, S.(1995). 'Wars without end: the Indo-Pakistani conflict.' *The Annals of the American Academy of Political and Social Science*, 541, pp. 167-178.

Gartzke, E., and Lupu, Y.(2012). 'Still looking for audience costs.' *Security Studies*, 21(3), pp. 391-397.

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

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

Gibler, D. M., and Hutchison, M. L.(2013). 'Territorial issues, audience costs, and the democratic peace: The importance of issue salience.' *The Journal of Politics*, 75(04), pp. 879-893.

Global Security(2008). '2008 - Mumbai Attack 22/11' Accessed on 21/06/2016. Available at: http://www.globalsecurity.org/military/world/war/indo-pak_2008.htm

Gompert, D. C., and Libicki, M.(2014). 'Cyber Warfare and Sino-American Crisis Instability' *Survival*, 56(4), pp. 7-22.

Huth, P. K., and Allee, T. L.(2002). 'Domestic political accountability and the escalation and settlement of international disputes.' *Journal of Conflict Resolution*, 46(6), pp. 754-790.

Jensen, B. M., Valeriano, B., and Maness, R. C.(2016 - forthcoming). *Cyber victory: the efficacy of cyber coercion.*

Kampani, G.(2002). 'Indo-Pakistani Military Standoff: Why It Isn't Over Yet' Accessed on 18/06/2016. Available at: http://www.nti.org/analysis/articles/indo-pakistani-military-standoff/

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

Kenwick, M. R., Lane, M., Ostick, B. and Palmer, G.(2013). 'Militarized Interstate Incident Data, Version 4.0' Accessed on 08/07/2015. Available at: http://www.correlatesofwar.org/

Kimura, K.(2011). 'How can we cope with historical disputes? The Japanese and South Korean experience' in Söderberg, M. [Ed]. *Changing Power*

Relations in Northeast Asia: Implications for Relations between Japan and South Korea. London:Routledge. pp. 19-38.

Kinsella, D., and Russett, B.(2002). 'Conflict emergence and escalation in interactive international dyads.' *The Journal of Politics*, 64(04), pp. 1045-1068.

King, A., and Taylor, B.(2016). 'Northeast Asia's New 'History Spiral''. *Asia & the Pacific Policy Studies*, *3*(1), pp. 108-116.

Koo, M. G.(2005). Economic dependence and the Dokdo/Takeshima dispute between South Korea and Japan. *Harvard Asia Quarterly*, *9*(4).

Kurizaki, S., and Whang, T.(2015). 'Detecting audience costs in international disputes.' *International Organization*, *69*(04), pp. 949-980.

Lawson, S.(2012). 'Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States.' *First Monday*, *17*(7). Accessed on 10/08/2016. Available at: http://128.248.156.56/ojs/index.php/fm/article/view/3848

Lektzian, D. J., and Sprecher, C. M.(2007). 'Sanctions, signals, and militarized conflict.' *American Journal of Political Science*, 51(2), pp. 415-431.

Levendusky, M. S., and Horowitz, M. C.(2012). 'When backing down is the right decision: Partisanship, new information, and audience costs.' *The Journal of Politics*, 74(2), pp. 323-338.

Lindsay, J. R.(2013). 'Stuxnet and the limits of cyber warfare.' *Security Studies*, 22(3), pp. 365-404.

Lindsay, J.R., Cheung, T.M., and Reveron, D.(2015). 'Will China and America Clash in Cyberspace?' *The National Interest.* Accessed on 14/06/2016. Available at: http://nationalinterest.org/feature/will-china-america-clash-cyberspace-12607

Lindsay, J. R.(2015). 'The impact of China on cybersecurity: fiction and friction.' *International Security*, 39(3), pp. 7-47.

Lynn III, W. J.(2010). 'Defending a New Domain' Accessed on 30/06/2016. Available at: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Maness, R. C., and Valeriano, B.(2015). 'The Impact of Cyber Conflict on International Interactions.' *Armed Forces & Society* 2(2). pp. 301-323

Maness, R. C., and Valeriano, B.(2016). 'Cyber spillover conflicts:transitions from cyber conflict to conventional foreign policy disputes?' in Friis, K., and Ringsmose, J.(Eds.). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Abingdon:Routledge. pp. 45-64.

Mazanec, B.M.(2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons.* Lincoln, NE: University of Nebraska Press.

Ministry of Foreign Affairs of Japan.(2005). 'Statement by Mr. Nobutaka Machimura, Minister for Foreign Affairs of Japan, on the Statement of the Standing Committee of the National Security Council of the Republic of Korea'. Accessed on 28/06/2016. Available at: http://www.mofa.go.jp/announce/announce/2005/3/0318-7.html

— —(2005). 'Japan-ROK Foreign Ministers' Meeting'. Accessed on 28/06/2016. Available at: http://www.mofa.go.jp/region/asia-paci/korea/meet0504.html

— —(2005). 'Japan-Republic of Korea Foreign Ministers' Meeting'. Accessed on 28/06/2016. Available at: http://www.mofa.go.jp/region/asia-paci/korea/meet0505.html

— —(2005). 'Joint Press Statement of the Third Meeting of the Three-Party Committee of the People's Republic of China, Japan and the Republic of Korea' Accessed on 28/06/2016. Available at: http://www.mofa.go.jp/region/asia-paci/asean/conference/asean3/joint0505.html

Moon, C., and Souva, M.(2014). 'Audience Costs, Information, and Credible Commitment Problems.' *Journal of Conflict Resolution.* pp1-25.

Oppel, R. A., and Masood, S.(2008). 'Pakistan Moves Troops Amid Tension With India' Accessed on 18/07/2016. Available at: http://www.nytimes.com/2008/12/27/world/asia/27pstan.html

Paganini, P.(2016). 'Chinese hacker admitted hacking US Defense contractors' Accessed on 30/06/2016. Available at: http://securityaffairs.co/wordpress/45597/intelligence/china-hacked-us-defense-contractors.html

Panetta, L.(2012). cited in New York Times, 'Panetta Warns of Dire Threat of Cyberattack on U.S.' Accessed on 06/06/2016. Available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyber-attack.html?_r=0

Partell, P. J., and Palmer, G.(1999). 'Audience costs and interstate crises: An empirical assessment of Fearon's model of dispute outcomes.' *International Studies Quarterly*, 43(2), pp. 389-405.

Prins, B. C.(2003). 'Institutional instability and the credibility of audience costs: Political participation and interstate crisis bargaining, 1816-1992.' *Journal of Peace Research*, 40(1), pp. 67-84.

Putnam, R. D.(1988). 'Diplomacy and domestic politics: the logic of two-level games.' *International organization*, 42(3), pp. 427-460.

Pytlak, A. and Mitchell, G. E.(2016). 'Power, rivalry and cyber conflict: an empirical analysis' in Friis, K., and Ringsmose, J.(Eds.). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives.* Abingdon:Routledge. pp. 65-82.

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

Rid, T.(2013). 'Cyberwar and Peace: Hacking Can Reduce Real-World Violence.' *Foreign Affairs* Accessed on 18/06/2016. Available at: https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace

Sardar, S.(2008). 'Pakistan says Indian warplanes violated airspace' *Reuters.* Accessed on 18/06/2016. Available at: http://in.reuters.com/article/idINIndia-37019620081214

Scanlon, C.(2005). 'South Koreans Vent Fury at Japan' *BBC News.* Accessed on 28/06/2016. Available at: http://news.bbc.co.uk/1/hi/world/asia-pacific/4361343.stm

Schultz, K. A.(1998). 'Domestic opposition and signaling in international crises.' *American Political Science Review*, 92(4), pp. 829-844.

Schultz, K. A.(2001*a*). *Democracy and coercive diplomacy*(Vol. 76). Cambridge University Press.

Schultz, K. A.(2001*b*). 'Looking for audience costs.' *Journal of Conflict Resolution*, 45(1), pp. 32-60.

Schultz, K. A.(2010). 'The enforcement problem in coercive bargaining: Interstate conflict over rebel support in civil wars.' *International Organization*, 64(02), pp. 281-312.

Schultz, K. A.(2012). 'Why we needed audience costs and what we need now.' *Security Studies*, 21(3), pp. 369-375.

Smith, A.(1998). 'International crises and domestic politics.' *American Political Science Review*, 92(3), pp. 623-638.

Stolar, A.(2008). 'To the Brink' Accessed on 22/06/2016. Available at: https://www.files.ethz.ch/isn/94299/To_the_Brink.pdf

Stone, J.(2013) 'Cyber War Will Take Place!' *Journal of Strategic Studies*, 36(1), pp. 101-108

Takahashi, K.(2005). 'Japan-South Korea ties on the rocks' *The Asia-Pacific Journal : Japan Focus.* Accessed on 28/06/2016. Available at: http://apjjf.org/-Kosuke-Takahashi/1767/article.html

Tomz, M.(2007). 'Domestic audience costs in international relations: An experimental approach.' *International Organization*, 61(4), pp. 821-840.

Valencia, M. J.(2007). The East China Sea dispute: context, claims, issues, and possible solutions. *Asian Perspective*, 127-167.

Valeriano and Collier(2016). 'What Can We Know About Cyber Security Data?' Accessed on 18/06/2016. Available at: http://relationsinternational.-com/what-can-we-know-about-cyber-security-data/

Valeriano,B., and Maness, R. C.(2014). 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.' Journal of Peace Research 51(3), pp. 347-360.

Valeriano, B., and Maness, R.C.(2015*a*). *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford: Oxford University Press.

Valeriano, B., and Maness, R.C.(2015*b*). 'The Coming Cyberpeace: The Normative Argument Against Cyberwarfare.' *Foreign Affairs*. Accessed on 20/05/2016. Available at: https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace

Valeriano, B., and Maness, R. C.(2015*c*). 'The Dyadic Cyber Incident and Dispute Data, Version 1.5' Accessed on 08/07/2015. Available at: http://drryanmaness.wixsite.com/irprof

Valeriano, B., and Maness, R. C.(2016 - forthcoming). *Caution in the cyber domain: deterrence and Restraint in Cyberspace.*

Walsh, J. I.(2007). 'Do states play signaling games?' *Cooperation and Conflict*, 42(4), pp. 441-459.

Vasquez, J. A., and Valeriano, B.(2008). "Territory as a Source of Conflict and a Road to Peace" in *The Sage handbook of conflict resolution.* pp 191-209.

Weeks, J. L.(2008). 'Autocratic audience costs: Regime type and signaling resolve.' *International Organization*, 62(1), pp. 35-64.

Wolford, S.(2014). 'Showing restraint, signaling resolve: Coalitions, co-operation, and crisis bargaining.' *American Journal of Political Science*, 58(1), pp. 144-156.

Appendix

Contents:

Amalgamating the DCID and CoW Datasets

The method used to combine these two datasets was simple and straightforward. After downloading the full MID, MII and latest version of the CoW codebook(4.0), I simply filtered out all of the dyads which were not included in the Valeriano and Maness DCID.
Once completed, I then ran through all the remaining data and cut out all interactions prior to 2000, the point of earliest cyber interaction recorded in the DCID. This left me with 18 dyads, 55 disputes and 599 militarised incidents to marry up to those disputes represented in DCID.
For my case studies, I created entirely new combined datasets which included cyber and militarised incidents ranked chronologically, with the aim of enabling close inspection of the sequences of events during interstate crises, the details of which can be seen subsequently under the 'Additional information on …' sections.

Selecting cases

In order to thoroughly examine the role of cyber interactions in conflict dynamics I selected from the three forms of disputes, cases with varying severity levels and interaction types, in the hope that the differing contexts may shed light on exactly when and how cyber signalling practices may have an impact on state behaviour.

Selection rationale:
Given that the aim of the research is to analyse periods of crises in which states signal, I removed all cases which involved below average levels of interaction - which reduced the sample sizes for each of the three categories - disruptive, coercive and espionage disputes - to five, five and six respectively.

I then further removed those in which there were no incidences of public acknowledgment of the cyber strikes by the perpetrators - considered a key part of signalling - to arrive at the final sample of three disputes for each category of interaction.

At this point I then used Microsoft Excels RAND function to draw at random from these final sample sets one case each.

The final cases:

1. Disruption - India-Pakistan(Severity level 2, number of interactions 10)
2. Coercion - Japan-South Korea(Severity level 2, number of interactions 4)
3. Espionage - US-China(Severity level 5, number of interactions 43) pattern of interaction selected around Buckshot Yankee Operation - will look at preceding Chinese attacks pertinent to military espionage and subsequent responses from both sides(12 interactions in total)

The final Samples from which these were drawn:

1. For disruption based interaction : **India-Pakistan**; N Korea-S Korea(Dispute Number 42; Severity level 2; Number of Interactions 6); Iran-Israel(Dispute Number 20; Severity level 2; Number of Interactions 5)
2. For coercion based interaction: **South Korea-Japan;** North Korea-South Korea(Dispute Number 43; Severity level 3; Number of Interactions 3); Iran-Saudi Arabia(Dispute Number 22; Severity level 6; Number of Interactions 3)
3. For espionage based interaction: China-Taiwan(Dispute Number 30; Severity level 4; Number of Interactions 4); **US-China**; China-Japan(Dispute Number 36; Severity level 4; Number of Interactions 4)

Additional Information on Disruptive Disputes and the India-Pakistan Dispute

Cyber Dispute Number 48(including incident numbers 152-161),
the enduring rivalry played out between India and Pakistan in cyberspace comprised of 10 incidents between 22 October 2001 and 1 October 2011, 6 of which were instigated by Pakistan, 4 by India.
Interactions were predominantly nuisance or harassment in type through the vandalism or defacement of websites, and in some cases denial of service attacks against mainly Government, non-military targets. With 12 MIDs in 10 years, including 10 with the actual use of force, India-Pakistani military interactions can be described as fairly regular and low level - recording with a best estimate as many as 31 Indian fatalities, although precise numbers for both sides are in the main, unknown.

Full overview of cyber and militarised interaction between India and Pakistan, not included in the body of work for reasons of length:

2001

1. **MID Incident 4277002** - Instigator Pakistan - 5 October Reciprocal use of force in border clash, with fatalities unknown, and motivated by disputed territorial claims
2. **Cyber Incident 152** 'October 2001 defacements' - Initiator Pakistan - 22 to 24 October. Successful disruption attack by means of vandalism, with government(non-military) websites defaced in show of displeasure at criticism of militant groups operating inside Pakistan, and Pakistani-controlled Kashmir.
3. **MID Incident 4277003** - Instigator Pakistan - 23 to 26 October Alert, show of force, no fatalities.
4. **MID Incident 4277004** - Instigator of incident India(dispute Pakistan) - 11 to 12 November Reciprocal use of force in border clash, with Pakistani fatalities unknown, Indian fatalities recorded at 5, and motivated by disputed territorial claims

2003

5. **MID Incident 4277070** - Instigator Pakistan - 28 June to 5 July Reciprocal use of force in border clash, with fatalities unknown, and motivated from Pakistan's perspective by disputed territorial claims, for India policy change
6. **Cyber Incident 153** 'July 2003 defacements' - Initiator Pakistan - 12 to 13 July Successful nuisance, disruption attack on government non-military websites to coincide with and enhance protests over the re-opening of the only India-Pakistan bus service, which had been suspended in 2001 after attack on the Indian Parliament".
7. **MID Incident 4277071** - Instigator Pakistan - 12 to 18 July Reciprocal use of force in border clash, with fatalities unknown, and motivated from Pakistan's perspective by disputed territorial claims, for India policy change
8. **MID Incident 4277072** - Instigator of incident India [dispute initiator Pakistan] - 24 July to 4 August Reciprocal use of force in border clash, with fatalities estimated at between 1 and 25 on both sides(precise number unknown). Motivated from India's perspective by policy contention, Pakistan by disputed territorial claims.

2008

9. **MID Incident 4585008** - Instigator Pakistan - 4 November. Border attack with use of force carried out, fatalities unknown, motivated firstly by policy contentions and secondly by territorial claims.
10. **Cyber Incident 154** 'November 2008 defacements' - Initiator India - 15 to 27 November Successful nuisance, disruption attack by means of government oil and gas regulatory authority website, initially intended to conduct cyber conflict with Pakistan, and subsequently to the Mumbai terror attacks beginning on the 26th of November, to seek revenge.
11. **Cyber Incident 155** 'November 2008 defacements' - Initiator Pakistan - 15 to 27 November Successful reciprocal nuisance, disruption attack on Indian government, non-military websites by means of vandalism to retaliate against Indian defacement.

12. **MID Incident 4585009** - Instigator Pakistan - 28 November Border attack with use of force carried out, fatalities unknown, motivated firstly by policy contentions and secondly by territorial claims.
13. **Cyber Incident 156** 'Transportation defacements' - Initiator Pakistan - 24 to 25 December Successful offensive strike, with the object of causing disruption, by means of transportation website defacements and shutdowns, in order to retaliate for the violation of Pakistani air space by Indian aircraft at the start of december.
14. **MID Incident 4585010** - Instigator Pakistan - 26 December Display of force with fortification of border, driven by policy dispute.

2010

15. **MID Incident 4585031** - Instigator Pakistan - 19 August Reciprocative use of force by both sides in border clash without fatalities, driven(from Pakistan's perspective) firstly by policy contentions and secondly by territorial claims.
16. **Cyber Incident 157** 'September 2010 defacements' - Instigator Pakistan - 2 to 12 September Unsuccessful nuisance, disruptive attack by means of website vandalism(government, non-military) in order to retaliate against the Indian Government's heavy handed response to summer uprising in Kashmir, and deaths of civilian protestors.
17. **Cyber Incident 158** 'September 2010 defacements' - Instigator India - 2 to 12 September Similarly unsuccessful retaliation to Pakistani attacks, by means of website vandalism and aim to cause disruption.
18. **MID Incident 4585032** - Instigator Pakistan - 28 September to 1 October Reciprocative use of force by both sides in border clash - number of fatalities unknown - driven(from Pakistan's perspective) firstly by policy contentions and secondly by territorial claims.
19. **MID Incident 4585033** - Instigator Pakistan - 24 to 27 October Reciprocative use of force by both sides in border clash - number of fatalities on Pakistan's side unknown, 1 Indian fatality recorded - driven(from Pakistan's perspective) firstly by territorial claims and secondly by policy contentions.

20. **Cyber Incident 159** 'PCA defacements' - Instigator Pakistan - 1 to 3 December Nuisance disruption attack by means of website defacement to show strength in the wake of Indian nationalist attacks on the anniversary of the Mumbai bombings.
21. **Cyber Incident 160** 'PCA defacements' : 1 to 3 December Nuisance disruption attack by means of website defacement to retaliate against widespread Pakistani website vandalism of some 270 outlets.
22. **MID Incident 4585034 -** Instigator Pakistan - 29 December Reciprocative use of force by both sides in border clash - number of fatalities unknown - driven(from Pakistan's perspective) firstly by territorial claims and secondly by policy contentions.

2011

23. **Cyber Incident 161** 'ICID defacement' - Instigator Pakistan - 1 Oct Offensive strike against government non-military websites by means of vandalism, in order to retaliate for the deaths of civilians in Jammu and Kashmir in Indian security crackdown.

Additional Information on Coercive Disputes and the South Korea-Japan Dispute

Cyber Dispute Number 45 comprised of 4 incidents between 1 April 2001 and 20 March 2005, 2 instigated by South Korea, 2 by Japan [sequence = 732 - 732 - 740 - 740]. Mainly nuisance strikes they consisted of vandalism and Denials of Service(Predominantly the latter at 75%), with private companies and Government, non-military systems targeted(again, predominantly the latter, also 75%)

While cyber incidents tend towards coercive disruption or denial of service and defacements attacks, military actions are all restricted to displays but not use of force, with mainly tit-for-tat retaliatory scrambling of jets for example.

Both sets of interactions are driven by disputed territorial claims, surrounding the Tokdo Islands. Cyber interactions have also been driven contentious policy decisions, with South Koreans responding angrily to the publication of Japanese text books which distorted historic Japanese acts during WWII.

<u>Full overview of cyber and militarised interaction between Japan and South Korea, not included in the body of work for reasons of length:</u>

2001

1. **Cyber Incident 144** 'Textbook hack' - Instigator South Korea - 1 April 2001. Disruption by means of DDoS attack of several government and private websites in response to the release of a new controversial Japanese history textbook, which distorted Japanese acts in WWII and the invasion of China and South Korea. Unsuccessful attempt to coerce Japan into withdrawing textbook.

2004

2. **Cyber Incident 145** 'South Korea Patriotic' - Instigator South Korea - 7 to 14 January 2004. Successful disruption by means of DDoS attack

against private media websites in show of displeasure at the lifting of censorship against Japanese media outlets at the beginning of January.

3. **Cyber Incident 146** 'Japan Patriotic' - Instigator Japan - 7 to 14 January 2004. Successful disruptive retaliation also by means of DDoS attacks agains South Korean government(non-military) websites.

2005

4. **MID Incident 4468001 -** Instigator Japan - 8 March 2005 Show of force(display only), motivated by disputed territorial claims surrounding the Tokodo Islands. Airforce jets scrambled.
5. **MID Incident 4468002** - Instigator South Korea - 8 March 2005 Show of force(display only). Airforce jets scrambled.
6. **MID Incident 4468003 -** Instigator Japan **-** 16 - 18 March 2005 Show of force(display only), motivated by disputed territorial claims surrounding the Tokodo Islands. Airforce jets scrambled.
7. **MID Incident 4468004** - Instigator South Korea - 16 - 18 March 2005 Show of force(display only). Airforce jets scrambled.
8. **Cyber Incident 147** 'Island Dispute' - Instigator Japan - 20 March 2005. Disruptive attack by means of government website defacement
9. **MID Incident 4468005** : 7 July 2005 Show of force(display only), motivated by disputed territorial claims.

Additional Information on Espionage Disputes and the US-China Dispute

Cyber Dispute Number 9, the US-China espionage dispute comprised of 43[at time of writing/compiling data set] incidents between 1 Jan 2003 and is currently ongoing. Of these 7 were instigated by US, 36 by China. In terms of methodology, mainly Intrusion and Infiltration tactics were adopted, with targets from a variety of sectors including private companies, government non-military and government military bodies, although around half of those targeted comprise of government, non-military networks(21 of 43).

With regard to the type of interactions between the dyad, these were mainly espionage operations, of mixed severity, with several APTs and sophisticated intrusion and infiltration methodologies. In contrast, militarised interaction during the cyber period has as yet remained confined to displays of force - aerial, nautical and the expansion of military programs and arsenals. The disputes can be seen to be motivated by espionage, intellectual theft with the objective of gaining economic, strategic, diplomatic and military advantage on the cyber front; contentious policy with regard to disputed south china sea territorial claim in the instance of militarised interaction

<u>Full overview of Military related cyber espionage campaigns and responses between the US and China, not included in the body of work for reasons of length:</u>

2003 Instigated

10. **Cyber Incident 25** ‘Titan Rain’ : 1 Jan 2003 - 1 April 2006 - China Instigates - Aim “Espionage camapign against the DoD and defense contractors”

2006 Instigated

11. **Cyber Incident 29** ‘Cisco Raider’ : 29 February 2006 - 6 May 2010 - US instigates - “Defense countermeasure to prevent and deter further espionage through counterfeit cisco software from China”

12. Cyber **Incident 43** 'Fred Wolf Defacement' : 1 August 2006 - China Instigates - "To harass and access militantly intelligence and sensitive information from ongoing investigations regarding human rights cases, in order to gain strategic and diplomatic advantage"
13. **Incident 45** 'Naval War College disable' : 1-7 December 2006 - China Instigates - "To force offline the US Naval strategic studies group responsible for planning and practicing cyber-security tactics and operations"

2008 Instigated

14. **Incident 51** 'Boxing Rumble' : 1 January 2008 - 19 July 2010 - US instigated "The NSA was able to deflect the attack and fool the botnet into treating one of TAO's servers as a trusted command and control(C&C or C2) server. TAO then used that position of trust, gained by executing a DNS spoofing attack injected into the botnet's traffic, to gather intelligence from the bots and distribute the NSA's own implant malware to the targets,"

2009 Instigated

15. **Incident 36** 'Lockheed F-35 plans stolen' : 29 March - 1 April 2009 - China Instigates - "Espionage campaign against defense contractor Lockeed Martin and it's F-35 fighter jet plans"

2010 Instigated

16. **Incident 49** 'Shotgiant' : 10 October 2010 - Ongoing - US instigated - aim "To determine links between Huawei produced technology and PLA espionage. Secondly, to exploit Huawei technology to probe for information from and potentially to conduct offensive cyber operations against product users"
17. **Incident 66** 'U.S. Top National Security Email Hacks' : 1 April 2010 - 10 August 2015 - China Instigates - Aim "Top US national security officials emails hacked and read by ongoing Chinese cyber espionage campaign"
18. Incident 34 'Buckshot Yankee' : 29 April - 1 May 2010 - US instigated - "Defensive measure to deter further attempts to steal sensitive informa-

tion from the Pentagon through raising the potential costs incurred by US retaliation"

2011 Instigated

19. Incident 35 'Pentagon Raid' : 1-10 March 2011 - China Instigates - Aim "Pentagon Raid - Theft of 24,000 sensitive files from the Pentagon"
20. **Incident 53** 'Operation Beebus' : 12 April 2011 - 7 February 2013 - China Instigates - Aim "China hacks several US defense contractors and steals drone technology"

2013 Instigated

21. **Incident 58** 'Iron Tiger' : 15 January 2013 - 16 September 2015 - China Instigates - Aim "Chinese hackers infiltrate VVW page to access personal info of active US military personnel"

2014 Instigated

22. **Incident 55** 'Operation SnowMan' : 1-12 February 2014 - China Instigates - Aim "Iron Tiger sophisticated APT espionage on US military and defense contractors"

Background on the Signaling Model

Basic Model and game theoretic rationale adapted from Schultz(2001:37):

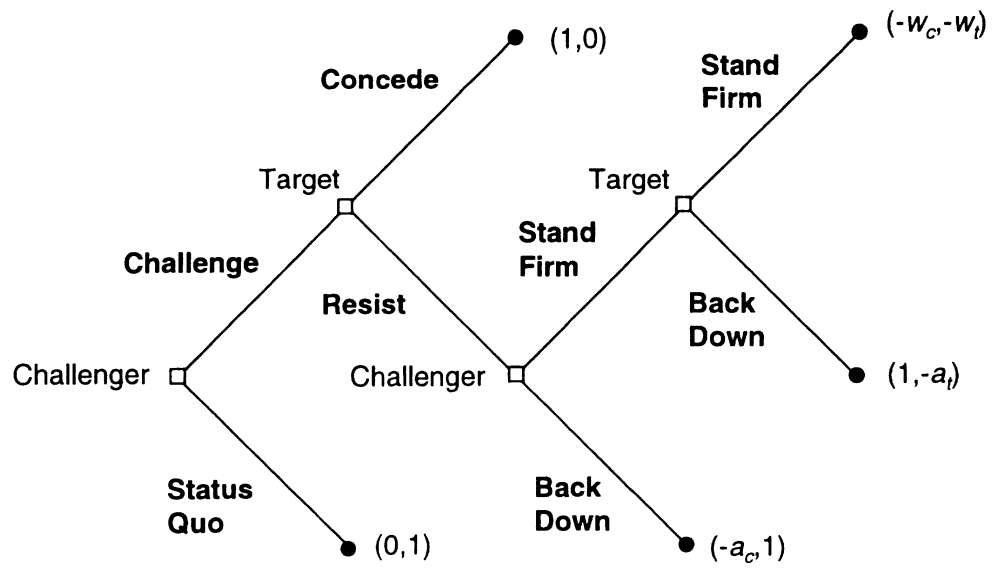


Figure 1: A Crisis Bargaining Game with Audience Costs

It was decided that a greater investigation of the game-theoretic assumptions and mechanisms detailed by Schutz with regard to this model, while interesting, did not relate fully to the central question of this dissertation - that of what impact signals have on interstate relations, not why decision makers select certain options over others during disputes.

Additionally, due to word limit constraints a more full and frank investigation of the central tenet which underpins Schultz's explanation of signalling during interstate crises was omitted but will follow below.

As was noted in the body of the text, the idea of signaling resolve in disputes, and associated audience cost literature, has come some way since Schultz's original works, with scholars such as Weeks revisiting the impact of the domestic audience on signalling practices across differing regime types to establish that contrary to the findings in previous research, leaders in democracies and non-democracies alike are equally as susceptible, albeit

in different ways, to come under pressure from, and in turn use some form of domestic audience cost or sanction in entrenching foreign policy stances(2008:59). Wolford(2014) on the other hand seeks to expand assessments of signaling resolve during international disputes to encompass coalitions of states rather that only dyads, while Lektzian and Sprecher(2007) examine the possibility of economic sanctions forming an alternative means of signaling resolve, ultimately finding that they share the same potential for escalation as the use military force.

In quantitative empirical terms there has been no real consensus as to the accuracy or validity of the signaling concept, with studies which vindicate the core assumptions on which the theory rests - such as Huth and Allee's discovery of the importance of domestic political accountability mechanism on dispute escalation(2002:755) or Kurizaki and Whang's thorough empirical defence of the role of audience costs as leverage during crisis bargaining(2015:976-7) - and those which contradict or challenge some of the key tenets of the signal and audience cost model as envisioned by Schultz in 2001. Downes and Sechser, for example, fall into the latter category, utilising new data to revisit Schultz's 2001 model and raise concerns over the empirical veracity of a central tenet of signaling theory - namely that which determines a means to measure or perceive the credibility of democratic states in issuing threats by means of invoking clear audience costs and an easy process of removal from office of leaders who renege on their commitments through electoral mechanisms - finding no evidence to support the notion of a democratic credibility in shows of resolve(2012:477; see also Snyder and Borghard, 2011).