The Dynamics of Restraint: An Analysis of Changes in Rival State Behaviour in Cyberspace from 2000-2020

Herrmann, Anna

The Dynamics of Restraint: An Analysis of Changes in Rival State Behaviour in Cyberspace from 2000-2020

Master Thesis

Anna Herrmann

MA International Relations Specialising in Global Conflict in the Modern Era

Leiden University

Supervisor: Dr. Lukas Milevski

Second Reader: Prof. Dr. Isabelle Duyvesteyn

Word Count: 14,992

Acknowledgements

First and foremost, I express my gratitude to my supervisor, Dr Lukas Milevski, for his guidance throughout this research process. I would also like to thank my parents, who have demonstrated unwavering faith in me throughout my academic career. Finally, I am indebted to the friends who made this year truly memorable.

Table of Contents

Introduction

The past two decades have borne witness to the evolution of cyberspace as a domain used by states to engage in operations against rivals within the international system.[1] With this escalation in cyber activity came 'cyber-hype' especially within the media and policymaking fields concerning the catastrophic potential of cyber incidents, referencing a 'cyber-Pearl Harbour', or a 'cyber-9/11' (Lee and Rid 2014, 4; Schneider 2022, 22). However, the reality of state behaviour in cyberspace is vastly different to this dramatization, with evidence pointing instead to low-level conflict. In 2014, Brandon Valeriano and Ryan Maness published their theory of state restraint in cyberspace, contending that due to fears of retaliation from running cyber operations that threaten or breach the threshold of war, states will conduct low-level operations against their rivals (Valeriano and Maness 2014). With these conclusions based on records of cyber incidents from 2001-2011, there was clear potential for further research to test the congruence of this theory on cyber incidents from 2012-2020 in order to analyse changes in state behaviour in cyberspace over the two decades. Therefore, this thesis addresses the research question 'To what degree do patterns of cyber incidents between 2000-2020 reflect changes in rival state behaviour in cyberspace?' The research aims to revise the existing theory of restraint in the context of state use of cyber operations by addressing its omission of political-strategic nuance. Rather than considering *fear of escalation* as the sole determining factor in state behaviour, this thesis contends that the *strategic utility* of cyber operations plays a pivotal role. Through examining patterns of cyber conflict, this study portrays the degradation of the dynamics of restraint, highlighting instead the increased adoption and strategic utilisation of cyberpower.

First, this thesis will lay out both the theory of state restraint in cyberspace and the new theory of strategic utility in order to frame the debate within the remainder of the research. The key academic literature on this topic will then be discussed, with the key takeaway being that while states behave with restraint in cyberspace, they also behave according to their military-political objectives. This highlights the oversight within restraint theory and justifies the need for an examination of its continued applicability to explaining state behaviour in cyberspace. After presenting the methodology that entails both quantitative analysis of the *Dyadic Cyber Incident Dataset (DCID) 1.0 and 2.0*, as well as qualitative analysis of case studies, this thesis will use the two hypotheses of the original 2014 research to structure the two analysis chapters. The first will discuss the number and

[1] This thesis uses Martin Libicki's definition of cyberspace as a domain divided between the physical layer and the syntactic layer (Libicki 2007).

frequency of cyber operations, and the second will evaluate the impact and severity of these incidents, relating the discussion back to the continued applicability of restraint theory versus the theory of strategic utility as frameworks for explaining changes in state behaviour.

The Dynamics of Restraint Versus Strategic Utility

Valeriano and Maness' 'The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011' was one of the first social science studies to systematically analyse the evolution and consequences of cyber conflict between state entities (Valeriano and Maness 2014). Centred on a database that recorded all publicly acknowledged cyber incidents and disputes between traditional state rivals, the study examined the processes of cyber conflict and evaluated the tactics, severity, and target information of the recorded incidents. The purpose was to investigate the 'cyber relations of rivals', using quantitative data to formulate an explanatory framework for international cyber behaviour, fundamentally questioning the reality of the threat from cyberspace (ibid., 347). The research, therefore, plays a constructive and valuable role in facilitating further study with the same (if updated) set of data along with the presented theoretical framework against which to continually examine state behaviour in cyberspace.

Using information from DCID 1.0, the dataset covering cyber incidents from 2001-2011, Valeriano and Maness determined that states would behave with restraint in cyberspace because of the fear or threat of retaliation, the potential for collateral damage, and the possibility of causing direct combat should these operations breach the threshold of war. Termed 'total offensive operations', these higher-level incidents would entail operations that target or destroy critical or civilian infrastructure or that infiltrate military forces (ibid., 350). Despite having the capabilities to do so, the authors contend that states will not engage in such destructive or disruptive behaviour in cyberspace because of the fear of escalation and subsequent devastating consequences. Basing their theory on the notion that states will not be reckless with their cyber capabilities, the authors instead posit that states will conduct 'low-level' operations that are limited in number, frequency, intensity, and damage (ibid., 357). Using this reasoning that states are restrained by *logic, norms, and fears of retaliation*, Valeriano and Maness explain state behaviour in cyberspace as within the 'normal relations range' for international rivalries; rival states operate as rivals should, managing tensions by forestalling violence yet prolonging hostilities for a long period of time (ibid., 347, 358).

The authors make two hypotheses for their theory of state restraint:

> H1: Due to restraint dynamics, the observed rate and number of cyber operations between rivals is likely to be minimal.
>
> H2: When cyber operations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics.

Valeriano and Maness' theory explains state behaviour through the lens of fears of escalation and mutual deterrence through continuous low-level cyber conflict. Upon this author's own evaluation of DCID 2.0 (the updated dataset covering incidents from 2000-2020), it became evident that such escalation had, to a degree, occurred within state rivalries over the past decade. With the above hypotheses lacking congruence with the data, the inoperability of restraint theory became evident. Through investigating cyber literature combined with the updated data, this thesis found that a central pitfall of the 2014 theory was its omission of the political-strategic nature of cyber operations. This thesis proposes a new theory of strategic utility as a suitable framework for explaining the observable changes in rival state behaviour.

In its most authentic form, strategy is "the bridge that relates military power to political purpose", the use or threat of force for the ends of policy (Gray 1999, 17; Milevski 2016, 10). Building upon Colin Gray's theory of strategic effect and John Sheldon's theory of cyberpower, strategic utility theory presents the idea that cyber capabilities are used in accordance with their optimal strategic value or worth, predominantly information control and network disruption. While still acknowledging that restraint will be operated in cyberspace, that is states having more impactful offensive capabilities yet consciously deciding not to employ them, strategic utility theory focuses on the conscious or calculated decision-making, the *intent* of states when using cyber means to execute specific military-political objectives. By analysing the motivation and the means, the framework provides sound explanations of both the observable changes in the patterns of cyber conflict and subsequently those of rival state behaviour in cyberspace. Therefore, where restraint theory explains state behaviour as driven by fear of escalation, strategic utility theory concludes that state behaviour is driven by the unique worth and thus strategic utility of cyber operations to state actors.

Chapter 1 – Literature Review

The purpose of this literature review is to contextualise this thesis' research, situating both restraint theory and the new theory of strategic utility within broader understandings of state behaviour in cyberspace. By establishing how the current body of cyber literature understands state behaviour in cyberspace, the review determines both the omission of political-strategic agency within restraint theory and the foundation for the new theory of strategic utility.

1.1 The Strategic Effect of Military Power

To begin discussing state behaviour in cyberspace, it is important to identify how military power is used, hence an overview of the concept of strategy is warranted. As stated, strategy is the bridge that relates military power to political purpose (Gray 1999, 17; Milevski 2016, 10). In his discussion of airpower, Colin Gray criticised the notion that one form of military power can be 'inherently strategic', vying that such a claim negates the contributions of other forms of power. Instead, Gray presents the idea that weapons are only strategic in their *consequence*. This is the foundation for the theory of strategic effect, where tactical weapons (the means of executing military strategy), have advantageous consequences for the attacking state in accordance with their policy (the political goals to be secured) (Gray 2009, 50-51). Lukas Milevski puts forward a triad of strategic effect being power, control, and freedom of action. He contends that to control a situation, to restrict an adversary's options, or to prevent or degrade his own instruments of military power, is to have strategic effect (Milevski 2016, 14-15). This provides the groundwork for a theory of strategic utility, with the foundational argument that weapons, such as cyber-weapons, *can* have strategic effect by bridging military power to political objectives.

In his conceptualisation of strategy, Richard Betts contends that rational strategic behaviour chooses the most appropriate means, thus maximising their value, according to cost-benefit calculations (Betts 2000, 6). In other words, the means achieve the greatest benefit with the lowest acceptable risk. While the idea of 'acceptable risk' in military operations is still contested, it is clear that for means to have an optimal strategic effect, they need to be sufficient in accordance with the ends, while minimising the risk involved (ibid., 9-10, 50). When considering state behaviour in cyberspace, in accordance with Betts' conclusion, strategic theory posits that states should engage in behaviour that maximises the value of the operation by choosing the most appropriate means and minimising any risk involved. This discussion, therefore, highlights the missing nuance from

Valeriano and Maness' theory of restraint, which attempts to explain state behaviour predominantly using escalation fears as the determinative factor, rather than considering the strategic utility of cyber operations as a means of warfare.

Focusing specifically on offensive cyber operations, Daniel Moore argues that strategic behaviour or intent leads to the use of technology (with strategy as the driving force), rather than technology creating de facto strategies (Moore 2022, 1). Putting forward the idea that military strategy utilises technology, in this case, cyber operations, to execute the political goals in question, Moore also highlights the strategic utility of such means of warfare (ibid.). What this scholarship emphasises is that the use of military power is calculated and premeditated, especially when considering the intricacies of information-based operations. States are not reckless with their military capabilities, thus indicating restraint, but they consciously utilise the appropriate means available in order to achieve the goals determined by policy.

1.2 Cyberpower

Cyberpower is the process of using cyberspace to achieve the policy objectives of the nation, similar to conceptualisations of airpower, seapower, and landpower (Sheldon 2011, 95). John Sheldon defines the overall strategic impetus of cyberpower as "the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment" (ibid.). This highlights one of the central tenets of cyberpower: control. The currency of cyberpower is fundamentally information control and network disruption, which can materialise in the disruption or sabotage of an adversary's systems, the denial of communications, the stealing of information, or the monitoring of an adversary's activities (ibid., 104). The definition also underlines how cyber conflict adds a new layer to the fog of war, blurring the lines between war and peace through persistent, if low-level, conflict, such as that described by Valeriano and Maness in 2014. Sheldon asserts that specific and unique attributes of cyberspace determine its worth as an offensive weapon, such as its stealthy and covert nature, the fact it is inexpensive to use in the grand scheme of military weapons, that its use favours the offence, and that there can be reasonable doubt planted as to the attribution of such attacks (ibid., 101).

Relating cyberpower to the strategic theory discussed previously, Sheldon contends that cyberpower is not directed towards its own objectives but instead serves the needs of policy, with

strategy as the mechanism for converting those needs into action (ibid., 103). For example, even if a state's cyber capability would allow for the total disabling of a foreign state's power grid, the needs of policy may demand that a lower-level operation is conducted to ensure that the power remains on. Linking this analogy to the idea of restraint, Sheldon argues that there could be multiple explanations for such a move, ranging from the fear of the unknown to the unwillingness of the attacking state to reveal its capabilities, to the requirements of policy and subsequent military strategy (ibid.). This identifies the point where Valeriano and Maness' theory of restraint, and this thesis' theory of strategic utility, differ. While it is agreed that restraint is exercised, the two theories offer different frameworks for understanding the reasons behind it.

David Betz and Tim Stevens place cyberpower theory into a more macro context. The authors note that when considering the current strategic context of warfare, one that is dominated by non-military capabilities such as propaganda, sabotage, and espionage, it is important to acknowledge cyberpower as a complementary capability (Betz and Stevens 2011, 96). This line of reasoning argues that cyberspace is primarily a force enhancer or multiplier and that beyond disruption, those cyber operations that degrade or destroy rarely emerge as an independent coercive instrument (Moore 2022, 6; Sheldon 2011, 104). Instead, they are likely to be used by states alongside other, more conventional, forms of military power.

This discussion of cyberpower frames both the theory of restraint and strategic utility, identifying the deviation between the two and the potential driving forces behind state use of cyberspace. It furthermore explains the link between military power and political purpose, or the military-political objectives driving state use of cyberspace. Combining this with a discussion of the unique attributes of cyberspace that make it a useful military weapon, this literature contributes to contextualising the remainder of the research.

1.3 Authoritarian and Democratic Cyber Thought

Having discussed conceptual understandings of state behaviour and the use of cyberspace, it is complementary to consider how states *understand* cyberspace. By discussing state thought surrounding cyberspace or the information domain, it can give insights into why and how states utilise offensive and defensive power in different ways in pursuit of national interests.

Danny Steed notes that "what constitutes security in Washington D.C. is radically different to what it means in Moscow or Beijing" (Steed 2021, 3). Focusing firstly on the offensive use of cyberspace, Steed argues that while the central concern of liberal democratic states is limiting cybercrime and cyber espionage, authoritarian states are far more concerned with maintaining control of their domestic population and ensuring regime survival (ibid., 36-38). Using Russia as an example, Steed uses the idea of an 'information autocracy', the use of cyber operations as a tool of state power and a global force projection platform (ibid., 48). To contrast, democratic states predominantly publicly adhere to restraint and regulation in cyberspace, demonstrated by their support of normative milestones such as NATO's *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt 2017). Gregory Rattray and Jason Healey go as far as to say that democratic states are far more constrained in their offensive behaviour because of their adherence to moral norms. Therefore, conducting operations such as disinformation campaigns within foreign states would be far more problematic for these states than it is for authoritarian powers (National Research Council 2010, 90).

Another key differentiation between how democratic and authoritarian states think about cyberspace stems from understandings of cyber sovereignty. Cyberspace, often characterised as unbounded and free from politically established terrestrial borders, poses a challenge to conceptualisations of violations of sovereignty. Scholars such as Betz and Stevens contend that due to state-on-state cyber intrusions becoming increasingly common, such incidents no longer constitute breaches of Westphalian sovereignty that could trigger escalation (Betz and Stevens 2011, 62). It is this normalisation of low-level conflict that also informs Valeriano and Maness' theory of restraint, arguing that incidents that don't breach the threshold of warfare by being destructive or disruptive against critical infrastructure, aren't violations of state sovereignty and thus don't warrant retaliation (Valeriano and Maness 2014). Alternatively, documents such as the *Tallinn Manual* apply conventional norms of sovereignty and intervention to cyberspace, proclaiming that such intrusions do in fact constitute violations of state sovereignty (Schmitt 2017).

There is a consensus within cyber scholarship that authoritarian schools of thought tend to align with the notion of non-intervention. China takes a similar line to violations of cyber sovereignty to that of territorial sovereignty, gradually implementing doctrines such as the 'Great Firewall' to secure its internet systems from all foreign intrusions and interference (Barrass and Inkster 2018, 51; Steed 2021, 65-66). Juha Kukkola discusses the similar approach of the Russian Federation (from here on termed as Russia), and the concept of 'RuNet' (Russian internet). This is an attempt

of the Russian state to construct its own national, moated information environment. Kukkola notes that not only would this project facilitate increased state control of the domestic population's information systems and online presence, but a secure internet would also contribute to an asymmetric military advantage within the great power relations (Kukkola 2020, 10).

What this discussion of norms in cyberspace shows is that the cyber domain remains an essentially contested space that lacks a consensus as to the use and behaviour within it. This conversation is valuable to this thesis' research as it acts as part of an explanatory framework for variations in authoritarian and democratic behaviour in cyberspace, highlighting that different understandings and conceptualisations of this new military domain can contribute to determining actions.

1.4 Strategic Attribution

Engagements in cyberspace have brought a new dimension to interstate conflict in the form of attribution. Early literature on the techno-political process of the 'attribution problem' cited the practical difficulties of finding enough technical evidence to attribute cyber-attacks with a reasonable degree of certainty to a specific threat actor, as well as the perpetrator's ability to exploit the issue with claims of plausible deniability (Brenner 2007). However, with time this technical problem is much less of an issue due to technological developments and understanding. It was in 2018 that the co-founder of Crowdstrike Dmitri Alperovitch stated "The good news is that attribution – identifying who is responsible – is now largely a solved problem" (Alperovitch, 2011). It is, therefore, now the process of public attribution – what one does when you think you know who is responsible – that remains unresolved. This process of political or strategic attribution is a far more nuanced debate than technical attribution.

Thomas Rid and Ben Buchanan argue that the process of strategic attribution "is what states make of it" (Rid and Buchanan 2015, 7). An art, as well as a science, strategic attribution is a function of what is at stake politically, a process that can impact all forms of coercion and deterrence, as well as a state's credibility (ibid., 4-5). Putting forward that attribution can rest on a number of factors ranging from financial to reputational, the authors also discuss the importance of communicating attribution (ibid., 27). This determines how activities will be perceived both in the political and public spheres, a practice which they acknowledge is exercised with caution such as limiting public information releases (ibid.). This 'culture of secrecy' can be linked to differences between authoritarian and democratic behaviour, as the political stakes may be higher for an authoritarian

state whose reputation and regime survival is paramount. This could, in turn, mean that such a state would not publicly admit a successful cyber-attack due to connotations of weakness and lack of control.

Florian Egloff and Max Smeets take a similar line of thinking, proposing that states' attitudes towards public attribution are ones of "strategic, coordinated, pragmatism" (Egloff and Smeets 2021, 1, 22). They emphasise that attribution is equally driven by states' desire to shape the political and normative environment of cyber operations, putting the increase in public attribution over the past few years down to the desire of states to create a more stable cyberspace, or "set the rules of the game" (ibid., 2-3). Furthermore, these authors emphasise the aspect of timeliness within attribution operations, suggesting that politically, other time-sensitive political agendas have to be considered that attribution could either be detrimental to or supportive of (ibid., 14-15). Longer-term, political or public attribution comes with the consideration of whether it would be contributing to the interests of the actor, with the harm from toleration of behaviour or a lack of attribution potentially contributing to a narrative of acknowledging and accepting its legitimacy. This, the authors argue, can move attribution beyond being a dyadic activity, but one that has consequences internationally, such as future emulation of 'tolerated' cyber activity (ibid., 16). Overall, literature on the topic of strategic attribution labels it as a legitimate tool of statecraft, a highly politicised process of state behaviour that is crucial to the analysis of operations in cyberspace. This reinforces the previous conclusions in this literature review concerning state behaviour in cyberspace as intrinsically strategic and calculated.

The purpose of discussing this specific political nuance unique to cyberspace is to further indicate why and how states act in the cyber domain, driven by individual military-political or strategic objectives. Reviewing the concept of strategic attribution contributes to the understanding of state motivations, the formulation of responses to cyber incidents, and generally the dynamics of cyber conflict between state actors. In relation to this research specifically, this discussion explains some of the data in terms of the limitations of publicly acknowledged cyber incidents that shall be explained in further detail later.

In conclusion, this literature review has contextualised research on state behaviour in cyberspace, exploring academic consensuses on how and why states conduct cyber operations. A key takeaway is that the use of cyber operations is heavily influenced by the military-political motivations in play, with states making calculated strategic decisions based on the exertion of cyberpower as a military

means of executing policy goals. While the literature emphasises the prevalence of restraint in cyberspace, it has also identified the deviation between the two proposed theories of restraint dynamics and strategic utility. Whereas restraint theory is based on the avoidance of escalation as the determinative factor behind state behaviour, the literature emphasises how states make conscious and calculated decisions concerning their use of cyberpower as a military means to execute policy goals. This conclusion, therefore, justifies the proposition of the alternative theory of strategic utility as a framework for understanding the observations of escalation in cyberspace from 2000-2020. Hence, this chapter has shed light on the complexities and nuances involved in the subsequent analysis of rival state behaviour.

Chapter 2 – Methodology

The *Dyadic Cyber Incident Dataset* (DCID) is an open-source and peer-reviewed collection of state-perpetrated cyber incidents from 2000-2020. In 2014, Valeriano and Maness collated the first generation of this dataset (1.0) against which to build and test their theory of restraint, covering the years 2001-2011. The most recent update of the DCID (2.0) was in 2022, which is the collection this research will use. Allowing for a time lag for the accurate reporting of events, DCID 2.0 stops at 2020, which is therefore where this thesis will also conclude. The dataset has over 20 variables, coding incidents that are confirmed to be government-sanctioned and that have targeted a state's national security apparatus. The attribution of operations is checked against multiple sources such as government websites and cybersecurity corporations like McAfee, Kaspersky Lab, and Symantec. If attribution is in serious doubt, the incident is not recorded. The DCID also does not include multilateral cyber incidents or those that have been initiated by non-state actors. These factors ensure that the data focuses on interstate cyber conflict and that it is a reliable and accurate source, making it appropriate for the use of further research (Valeriano *et al.* 2022; Valeriano and Maness 2014).

In this research, a 'cyber incident' refers to an individual cyber conflict or campaign. While an incident may include thousands of individual intrusions, documenting all of these would be unfeasible for this study (Valeriano *et al.* 2022).

Using the two hypotheses mentioned in the introduction to structure the two analysis chapters, this thesis will answer the research question 'To what degree do patterns of cyber incidents

between 2000-2020 reflect changes in rival state behaviour in cyberspace?'. Using DCID 2.0, changes or deviations in patterns of cyber incidents perpetrated by state actors will be identified. This data will then be operationalised within the theoretical framework of the dynamics of restraint, originally proposed in 2014 to explain rival state behaviour in cyberspace. Using qualitative analysis of case studies to reinforce arguments, the testing of the continued operability of restraint theory will determine whether the data congrues with this understanding of cyber behaviour. Concluding minimal degrees of congruence, this thesis proposes the alternative theory of strategic utility as a new framework that reflects the DCID 2.0 data and explains the observable changes in rival state behaviour in cyberspace, again using case studies as empirical evidence to support each argument. This method demonstrates that the observable changes in patterns of cyber incidents do reflect changes in rival state behaviour in cyberspace, moving away from restraint and towards the increased adoption of cyber operations into state repertoires as military means of executing political goals.

The parameters of the research will be consistent with Valeriano and Maness's work. When discussing how the number and frequency of cyber operations will be 'minimal', this is defined as one incident per year for each rivalry dyad (Valeriano and Maness 2014, 355). Regarding 'impact' and 'severity', the authors do not specifically define their meaning of a 'limited impact', however, they note that "the damage done and intensity will be limited and mainly focused on low-level operations" (ibid., 351). Based on the DCID 2.0 codebook, this author's interpretation of this statement is as follows. Firstly, the severity score of cyber incidents (documented in Chapter Four) will predominantly be either disruption or espionage, rather than the higher levels that entail significant degradation or destruction. Secondly, cyber operations are unlikely to target critical infrastructure (Maness *et al.* 2022).

There are some notable limitations to this research. State cyber operations are inherently secretive, leaving scholarship to base conclusions off only those that have been publicly acknowledged. Furthermore, Valeriano and Maness acknowledged that the DCID data is, for reasons such as language constraints and institutional openness, biased towards the West (Valeriano and Maness 2014, 352). Finally, this research is limited to subjective interpretations of the *perceived* strategic utility of cyber operations due to the difficulty of ascertaining genuine strategic utility without knowing the inner workings of nation-state governments and militaries.

Chapter Three – Frequency and Number of Cyber Incidents

Hypothesis 1: *Due to restraint dynamics, the observed rate and number of cyber operations between rivals is likely to be minimal.*

Valeriano and Maness' first hypothesis reasons that due to restraint dynamics, namely the fear of retaliation from 'total' offensive operations, as well as the potential collateral damage incurred as a consequence, the *rate* and *number* of cyber operations between rivals is likely to be minimal (Valeriano and Maness 2014, 351). They confirmed this hypothesis using DCID 1.0, recording that out of a total of 110 cyber incidents, only 20 out of 126 rival dyads engaged in cyber conflict (ibid., 359). The average number of incidents between each rival was three, with only four dyads experiencing more than ten incidents between 2001-2011 (ibid., 348, 355). The authors, therefore, concluded that very few states actually fight 'cyber battles' despite being in an active rivalry (ibid., 355). Identifying the U.S.-China dyad as the most active, this rivalry only had 22 observed incidents, with China being the predominant initiator (ibid., 348). Using these observations of low rates and numbers of cyber operations, the authors concluded that states conduct low-level cyber conflict against their rivals because to conduct a higher intensity would incur potentially 'devastating and unlimited' consequences (ibid., 350).

3.1 2012-2020 DCID 2.0 Analysis

Documented in the tables below are summaries of the DCID 2.0 data from 2012-2020. This provides the basis for the conclusions made in the remainder of this research, so the reader can refer back to this information when needed. The DCID 2.0 codebook provides a reference point for explaining the different variables, as well as the coding within the tables (Maness *et al.* 2022).

Table 3.1 – Complete findings from DCID 2.0

Rival A (Number initiated)	**Rival B** (Number initiated)	**Cyber incidents**	**Most common method type**	**Most common target type**	**Most common coercive objective**	**Most severe dispute**	**Critical infrastructure**
U.S. (4)	Russia (37)	41	3	1	2	5	11

U.S. (3)	China (38)	41	3	1	3	4	13, 11
U.S. (3)	Iran (19)	23	3	1	3	5	11
U.S. (1)	N. Korea (14)	15	3	1	3	6	11, 17
Canada (0)	Russia (3)	3	3	1	1, 2, and 3	4	8, 11, 12
U.K. (0)	Russia (9)	9	3	2	3	4	11
U.K. (0)	China (1)	1	3	1	2	3	15
U.K. (0)	N. Korea (2)	2	4.2, 3	1	3, 4	4	12, 17
France (0)	Russia (3)	3	3	1	2	5	2
France (0)	N. Korea (1)	1	3	1	3	3	17
Germany (0)	Russia (5)	5	3	1	2, 3	5	4, 11
Poland (0)	Russia (3)	3	3	2	1, 2, 3	4	11
Russia (4)	Lithuania (0)	4	3	2	1, 2	4	11
Russia (30)	Ukraine (0)	30	3	1	4	5	11
Russia (5)	Georgia (0)	5	3	2	1, 2, 3	4	11
Russia (2)	Turkey (2)	4	2	1	1	3	9, 11
Russia (1)	S. Korea (0)	1	2	1	1	2	11
Iran (7)	Turkey (0)	7	3	1	2	4	17
Iran (15)	Israel (2)	18	3	1	3	5	6, 8, 13
Iran (11)	Saudi Arabia (0)	11	3	2	4	6	8
Iran (3)	Bahrain (0)	3	3	1	1	4	8, 11, 16
Turkey (1)	Syria (0)	1	4	3	3	4	11
Turkey (1)	Iraq (0)	1	4	3	3	4	11
Afghanistan (0)	Pakistan (1)	1	3	2	3	3	13
China (8)	Taiwan (1)	9	3	2	2	4	11
China (0)	S. Korea (1)	1	3	3	3	3	6
China (9)	Japan (0)	9	3	2	3	4	9, 11
China (7)	India (0)	7	3	1, 3	3	4	11
China (6)	Vietnam (2)	8	3	2	2	4	11
China (1)	Singapore (0)	1	4.2	3	3	3	6
China (7)	Philippines (0)	7	3	2, 3	1	4	11
China (3)	Australia (0)	3	3	2	3	3	17
N. Korea (27)	S. Korea (1)	28	3	1	1	4	9
N. Korea (1)	Japan (0)	1	3	1	2	3	12

S. Korea (1)	Japan (0)	1	3	2	2	4	12
India (1)	Pakistan (14)	13	3	3	1	4	11

Table 3.2 – Number of cyber dyads and total cyber incidents by state

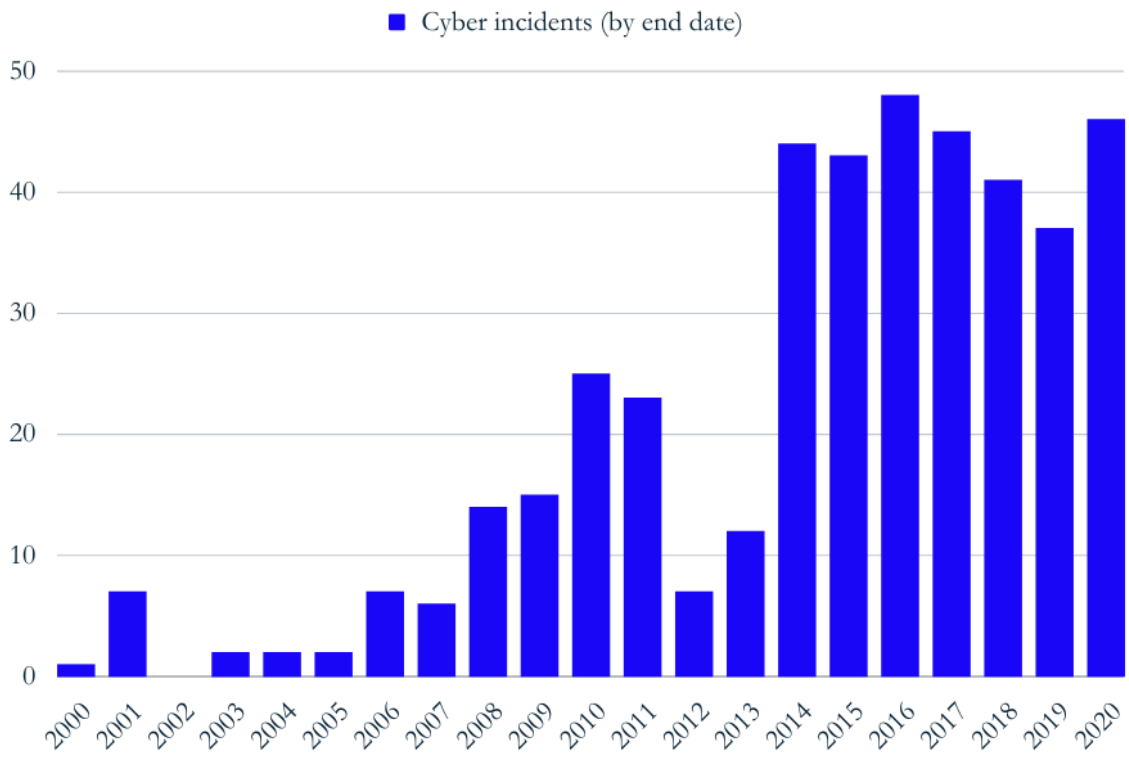
State	Number of dyads	Total incidents
Russia	12	108
China	10	87
Iran	5	62
North Korea	5	47
U.S.	5	120
South Korea	4	31
Turkey	4	13
U.K.	3	12
Japan	3	11
India	2	20

From the data in Table 3.1, key comparisons can be made to Valeriano and Maness' 2014 findings. With a total of 324 recorded incidents, 36 rivals engaged in cyber conflict from 2012-2020, an 80% increase from the initial data. The average number of cyber incidents between rival dyads is nine (three times the initial data), and whereas previously only four dyads experienced more than 10 incidents in total, from 2012-2020 nine dyads experienced over 10. Notably, this is also over a shorter time span. The U.S.-China dyad remained one of the most active, however, rivalled by the quickly surfaced U.S.-Russia dyad, both with 41 incidents. Russia and China were the primary initiators, with the U.S. initiating only seven cyber operations in total against these rivals (Valeriano *et al.* 2022).

High levels of Russian and Chinese cyber activity are reflected in Table 3.2, as the two states with the highest number of rival dyads and some of the highest numbers of total cyber incidents. Interestingly, the state with the highest number of total cyber incidents is the U.S., however, this reflects the state as the primary *target* of cyber operations, rather than the *attacker*. Russia conducted 102 cyber operations (31% of total incidents from 2012-2020), China conducted 80 (25%), Iran 54 (17%), and North Korea 45 (14%).

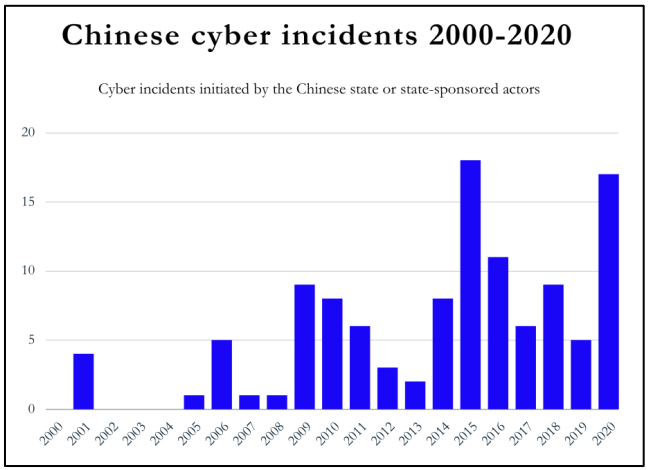
Table 3.3 confirms the observable escalation in the number and frequency of cyber operations between rival dyads from 2000-2020. Valeriano and Maness' dataset terminated at the end of 2011, reflecting their conclusion that a 'minimal' number and rate of operations were conducted by states. However, there are clear changes after 2013, with a high intensity of cyber activity maintained until 2020. Between 2000-2011, a cyber incident occurred on average nine times a year. Between 2012-2020, a cyber incident occurred on average 36 times a year, portraying a considerable increase in the frequency of interstate cyber conflict.

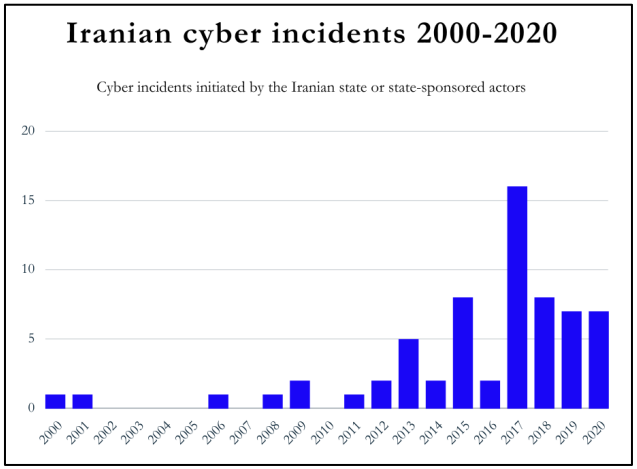
Table 3.3 Number of cyber incidents from 2000-2020

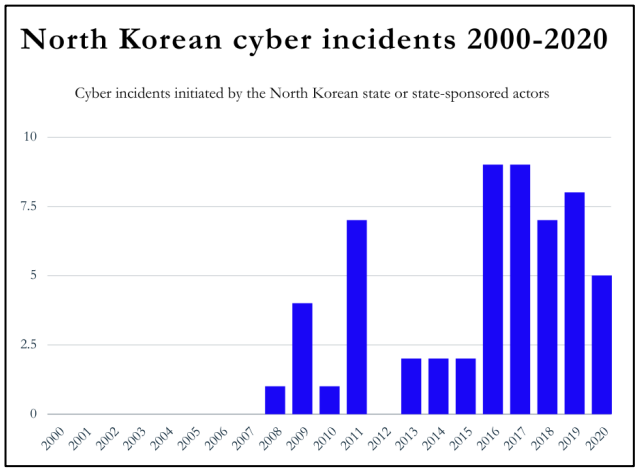


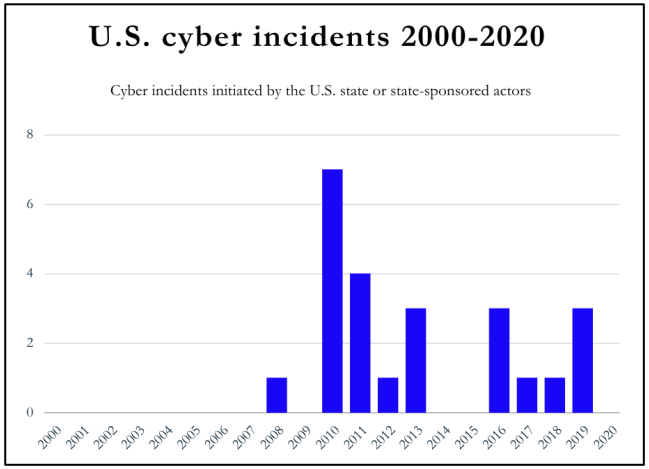
The cyber incidents of the most active states were recorded from 2000-2020, followed by the top five rival dyads, to further investigate the escalation of state activity in cyberspace.

Table 3.4 Cyber incidents by state actor









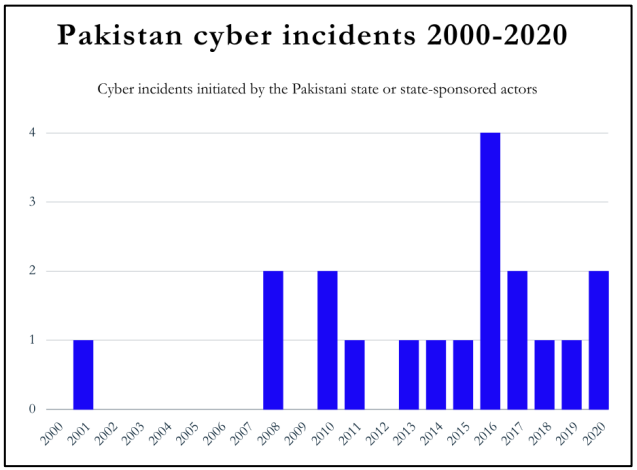
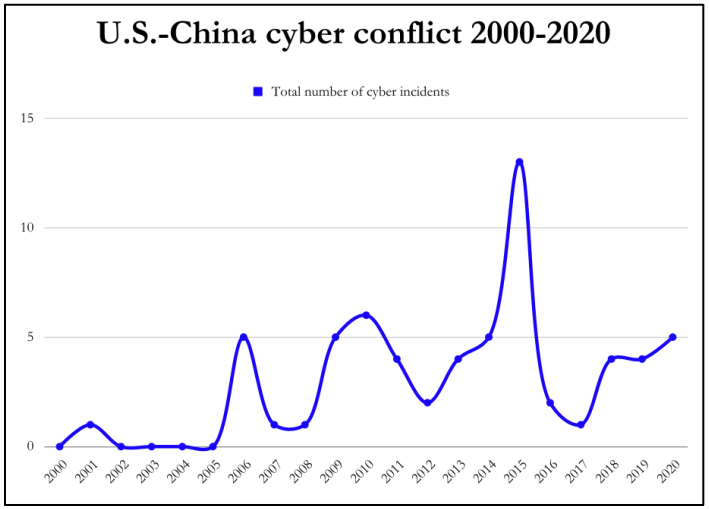
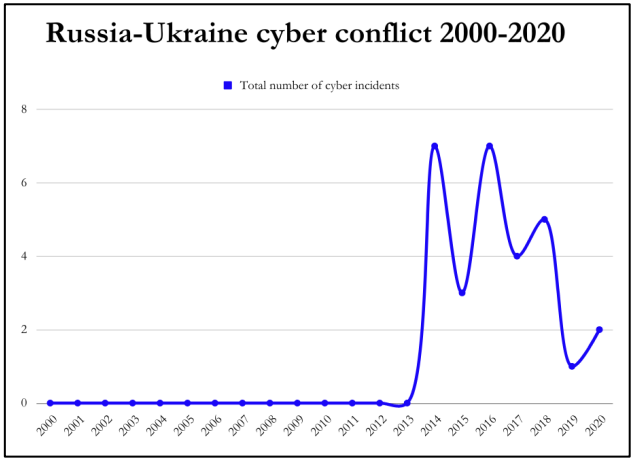
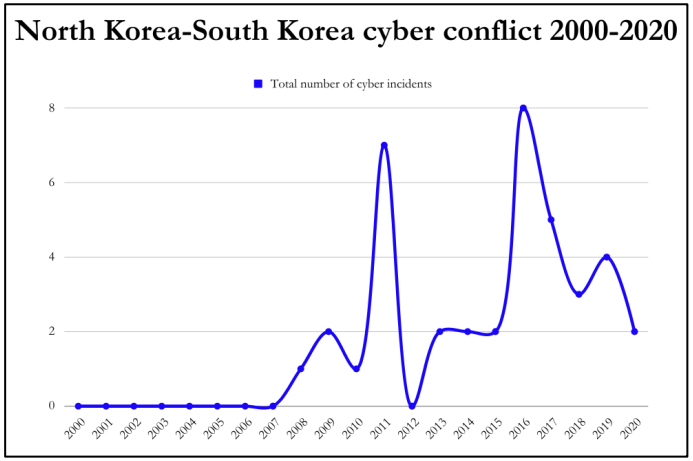
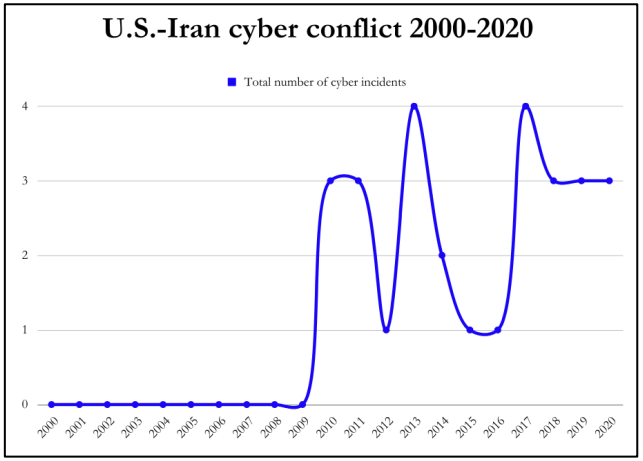


Table 3.5 Total number of cyber incidents per year by top five rival dyads









The visual representations above give interesting insights into the cyber engagements of the most active states and dyads. Russia poses an evident challenge to Valeriano and Maness' hypothesis that cyber operations will remain limited, with the sudden and significant escalation of offensive behaviour during the first half of the 2010s, mainly due to its rivalry with Ukraine. Similar behaviour can be observed by North Korea, with fluctuations in its perpetration of cyber operations over the two decades. Iran has demonstrated a progressively hostile position, with the majority of the state's activity occurring in the second decade against primarily the U.S. and its regional rival Saudi Arabia. China and Pakistan demonstrate the most consistent cyber behaviour, with Pakistan primarily targeting its regional rival India, and China maintaining a low-level yet constant stream of espionage operations.

The data on U.S. cyber operations cannot be consistent with reality. In 2018, U.S. Cyber Command launched its 'defend forward' cyber doctrine of 'persistent engagement' (Schneider 2022). This cyber strategy blurs offence and defence, a series of constant engagements with adversaries with the justification that it is better to consistently seek out and disrupt one's enemies before they attempt to pursue their own objectives (Moore 2022, 126). This anomaly highlights the limitations of the research as mentioned during the methodology chapter and incorporates into the discussion the concepts introduced concerning strategic attribution. Far more is known about cyber-attacks on American or Western targets than about those operations that successfully impact China or Russia, as is evident when there is a publicly established doctrine that emphasises constant engagement in cyberspace, yet minimal recorded state-perpetrated cyber incidents. This speaks to the idea of strategic attribution as it is evidently more advantageous for a state such as the U.S. to publicly acknowledge that it is the target of multiple cyber-attacks. It remains less advantageous for authoritarian states such as China and Russia to acknowledge either the occurrence or the success of an operation due to the objective of maintaining total control and projecting the strength of the regime.

3.2 Restraint Theory Applicability to DCID 2.0

Valeriano and Maness contend that states will conduct infrequent and low numbers of cyber operations against other states, terming this the 'normal relations range' for a rivalry (Valeriano and Maness 2014, 347). The target states will tolerate such attacks because they are low-level and

are not overly disruptive or destructive of critical infrastructure or national security apparatus. Conducting operations at this higher level would lead to armed or economic retaliation with subsequent collateral damage that could easily spiral out of control, forcing states to restrain their capabilities in cyberspace. The authors confirmed this theory using DCID 1.0, which highlighted the low intensity of interstate cyber conflict even between the most active rival dyads.

What the analysis of DCID 2.0 has shown is that there is no longer a 'minimal' number or low frequency of cyber incidents between rival states. While Valeriano and Maness did not directly define what 'escalation' stemming from more disruptive or destructive cyber incidents would specifically entail, this research's interpretation argues that escalation would materialise as an increasingly higher frequency and number of cyber incidents perpetrated by states against their rivals, with these operations of a more severe nature with a more devastating impact. This acceleration of interstate cyber operations would lead to physical consequences, such as armed retaliation and subsequent collateral damage. With evidence of an increase in the number and rate of cyber operations already demonstrated by the DCID 2.0 data, there should be evidence of consequences such as armed or economic retaliation as states intensify rivalries and move towards threatening the threshold for war. However, for example, when examining the top five most active rivalries that more often than not have more than one incident per year between 2012-2020, there appears to be no direct congruence between cyber operations and physical retaliation.

Valeriano and Maness' argument that states fear the consequences of escalation in cyberspace does not fit with the empirical evidence of increasing levels of offensive cyber activity with no clear retaliation stemming *directly* from such engagements. Taking the case of Russia and Ukraine as a dyad that experienced a sharp escalation of cyber activity in 2014, cyber operations were both frequent and high in number, being used as a force enhancer for Russia's conventional offensive. Sparked by the pro-European Maidan protests in Kyiv in late 2013, Russia began constant, low-level disruption campaigns against Ukraine (Jensen, Valeriano, and Maness 2019, 224). Conducted predominantly by state-linked hacktivist group Cyber Berkut, these operations primarily consisted of non-destructive operations such as denial of service attacks, website defacements, and disinformation campaigns linking the Ukrainian government to fascism and war crimes (ibid., 225). One of the most notable cyber incidents perpetrated by Russia in the later stages of the conflict with Ukraine was the 2017 NotPetya ransomware attack, which upon its disruption of hundreds of Ukrainian organisations and others globally, resulted in over $10 billion in economic losses (Bateman 2022, 21).

As the conflict continued, Russia found new ways of combining cyber effects with conventional military operations, for example using cyber espionage to isolate information objectives such as adjusting the location of artillery fire, jamming aerial drones through GPS, or re-routing Ukrainian mobile traders through Russian infrastructure. Furthermore, Russia employed cyber methods to degrade Ukrainian military capabilities such as using geolocation to locate artillery formations, and pre-emptively strike them (Jensen, Valeriano, and Maness 2019, 227). Cyber espionage was also used to degrade Ukrainian critical infrastructure, such as the 2014 Sandworm hacks that used BlackEnergy3 malware to gain access to Ukrainian power plants and temporarily take some of the systems offline (ibid.).

When considering the applicability of restraint theory to this surge in cyber engagement, it does not stand to reason that Russia maintained such low-level (non-destructive) operations because of the fear of consequences that might stem from more destructive incidents. Engaged in a conflict that was already causing destruction and subsequent collateral damage in the physical realm, Russia utilised cyberspace to execute information operations, causing Internet disruption, and exerting control over the information domain, showing no fear of escalation even when perpetrating more serious attacks such as NotPetya and the 2014 power grid attacks. The state, therefore, enhanced its conventional military campaign through the use of cyberspace. Hence, the higher number and frequency of Russian operations, as evidenced in DCID 2.0, did not threaten to directly cause escalation or armed retaliation nor indicate Russian restraint based on fear. Instead, the Russian state used this new domain of military power to enhance and consolidate its kinetic campaign, degrading the ability of the adversary to operate and comprehend that same environment.

Using an alternative example to assess restraint theory, the data from DCID 2.0 shows a clear incline in cyber engagement between the U.S. and Russia. As mentioned previously, the U.S. introduced its doctrine of 'persistent engagement' in 2018, a clear indication of the state's acceleration of cyber operations against its adversaries. As the data demonstrated, much less is known about the success of these operations not only because of their covert nature but because states such as Russia rarely publicly acknowledge successful cyber incidents against their critical infrastructure. Outside of regional conflict, Russia maintained a high tolerance for operational risk in cyberspace, continually launching offensive operations against the U.S. throughout the 2010s as reflected in DCID 2.0. The presidential election hack in 2016 stands out as a particular milestone in Russian cyber campaigns, with social media firm Facebook revealing in 2017 that targeted

Russian propaganda may have reached as many as 126 million users, with the purpose of "unleashing the protest potential of the population" (Jensen, Valeriano, and Maness 2019, 212; Gerasimov 2013, 212).

Reiterating this thesis' interpretation of restraint theory, such intense escalation of publicly attributed offensive activity in cyberspace could have threatened the threshold for war and therefore incurred some form of retaliation. However, U.S. responses to major hacks such as the presidential election campaign and the 2014 Yahoo attack that breached over 500 million email accounts were confined to the prosecution of Russian intelligence agents and economic sanctions (*Reuters* 2017b; Schmidt and Perlroth 2020). To a degree, this response adheres to restraint theory's position regarding economic retaliation. However, there was no indication that these attacks that were evident breaches of state sovereignty, targeting critical infrastructure, and that were publicly attributed, could or would result in physical retaliation. While the evidence doesn't disprove restraint theory, it gives reasonable doubt as to the applicability of the first hypothesis. This feeds into the research question by positing that the patterns of cyber conflict to a degree no longer reflect restraint based on fears of escalation. Rather, the evidence of escalation reflects the adoption and internalisation of cyber engagements between states as a new means of executing military-political goals.

When focusing on the idea that states will maintain a low rate and number of cyber operations due to restraint dynamics, it remains unclear as to how this framework can explain evidence of escalation within cyberspace with a lack of retaliation stemming directly from such conflict. There is evidence of restraint by states, seen by the frequent use of low-level and non-destructive cyber operations rather than 'total' offensive operations that are likely to reside in some states' cyber repertoires. However, this author finds that the use of restraint theory to explain state behaviour still leaves one reaching for explanations, hypothesising what could potentially occur rather than attempting to explain what has occurred and why. This is especially relevant considering evidence of a significant escalation in cyberspace, yet the continued use of non-destructive operations even within the context of conventional conflict. Hence, this author proposes an alternative theoretical framework that focuses on the strategic utility of cyber operations, a theory that can explain the observable changes in the patterns of cyber incidents.

2014 Hypothesis 1: *Due to restraint dynamics, the observed rate and number of cyber operations between rivals is likely to be minimal.*

2023 Hypothesis 1: *Due to the strategic utility of information control and network disruption, states will likely engage in low-level yet frequent cyber conflict with their rivals.*

When explaining the changes within rival state behaviour as seen in DCID 2.0, this author finds it useful to focus on the strategic utility of cyber operations. This theory emphasises that states use cyber operations in accordance with their optimal worth, that being information control and network disruption, in order to execute military-political objectives. To test this, the intent of the state and the subsequent use of cyber means will be reviewed. This use could include controlling situations in the information space, restricting the options of one's adversary, or preventing or degrading their own instruments of military power (Milevski 2016, 15). Hence, this leads to a new hypothesis, positing that due to the strategic utility of information control and network disruption, states will likely engage in low-level yet frequent cyber conflict with their rivals.

The case study of Russia is useful to demonstrate the applicability of strategic utility theory as a framework for explaining changes in state behaviour in cyberspace. When considering the primary use of offensive cyber operations, as reflected by the DCID 2.0 data, is information control and network disruption and disruption, Russia's intensification of its non-destructive information campaigns demonstrates state use of this means of warfare in accordance with its strategic value. While Russia may be the most clear-cut case of a state that has significantly escalated its operations in cyberspace over the past decade, the constraints of this thesis prevent the same framework from being applied in-depth to other cases such as China, Iran, and North Korea. This is, therefore, an opportunity this author welcomes further scholarship to take on.

The case of the 2008 Russo-Georgian War is one of the earliest examples of Russian aggression in cyberspace. Perpetrating an onslaught of defacements and DDoS attacks on government websites and routers supporting Internet traffic in and out of Georgia, these cyber incidents actively contributed to Georgia's inability to communicate both internally and externally (Betz and Stevens 2011, 30; Sheldon 2011, 103). While Georgia lost territory due to the terrestrial conventional campaign, this had little to do with cyber operations, with the 'clickskrieg' constrained to spreading disinformation and causing low-level disruption (Cornish 2010, 2). Richard Clarke concluded that this case indicated state restraint in cyberspace, suggesting that the Russian government was "saving [their cyber weapons] for when they really need them" (Clarke and Knake 2010, 21). This emphasises Russian intent and conscious decision-making not to employ 'total' operations not out

of fears of retaliation, but because such destructive means were not appropriate for the military-political ends in this context. Instead, lower-level operations were used to control and disrupt Georgian cyberspace, demonstrating how Russia used cyberpower to enhance conventional military power and influence or manipulate the information domain to their strategic advantage. In this context, exerting control over the information space was more strategically useful to the attacking state than it would have been to create another destructive front, emphasising Russia's use of information operations in accordance with their optimal value or worth.

In 2014, Russian military-strategic doctrine experienced a cyber turn. The disharmony and clash of principles that emerged in the late 2000s and early 2010s such as the Arab Spring, Russian Colour Revolutions, and the gradual expansion of NATO across Europe caused a reformation in Russian military thinking (Kari 2019, 73, 78). With the boundaries of war and peace becoming increasingly blurred, Russian thinkers such as General Valery Gerasimov attributed the changing character of war to the evolution of the 'coordinated use of military and non-military measures', going so far as to suggest the primacy of non-military measures over conventional military power (Lilly and Cheravitch 2020, 132; Kari 2019, 74). This recognition of the strategic value of characteristically non-violent methods such as cyber operations to military processes, as effective tools of both strategy (during wartime) and statecraft (during peacetime), was reflected in Russian strategic documents. The 2010 Russia Military Doctrine stated that integrated non-military and military means is a characteristic of modern military concepts, with the updated 2014 version reinforcing the utility of combining informational, economic, financial, and military power to state military-political strategy (Lilly and Cheravitch 2020, 131-132). Ultimately, this conceptual flip in Russian perception of modern warfare emphasised how information (cyber) operations could be used as a lower-risk alternative to conventional military force with the same purpose of achieving military-political goals.

The operational use of this cyber turn became evident with the information campaigns in Ukraine in 2014, and against the U.S. throughout the 2010s. As discussed previously, the Ukraine case demonstrates how Russia used cyber operations in accordance with their optimal strategic value of information control and network disruption. Not only did Russia enact a persistent campaign of low-level disruptive information operations against Ukrainian Internet services, but the state also was able to insert itself into and control Ukrainian military information as well as degrade Ukrainian military capabilities, all through non-destructive cyber campaigns. This shows the use of cyberpower, in accordance with Sheldon's definition of its strategic impetus, to manipulate

perceptions of the strategic environment to the advantage of Russia, while at the same time degrading the ability of the adversary to comprehend that environment, as completed through network disruption (Sheldon 2011, 95). These cyber operations were, therefore, able to have strategic effect through the achievement of the state's objectives of information control and network disruption, which was also a complementary capability to its conventional campaign, a similar force enhancer to those used in Georgia.

Russian information campaigns against the U.S. were also used to achieve political objectives such as undermining rival institutions and resolve, executed through non-harmful means that would not threaten the threshold of war. Taking the example of the 2016 presidential election hack again, the goal of this operation was to psychologically impact the domestic population of the target state while demonstrating to the Russian population the corruption of democratic institutions (Jensen, Valeriano, and Maness 2019, 220). The perceived strategic benefit of using espionage as a tool of manipulation was to instil chaos and fracture U.S. political alliances (ibid., 223). Cyber means were used to exert Russian influence within a sphere that otherwise would have lacked it, the political direction of the U.S. By conducting a non-destructive or harmful operation, Russia utilised the unique strategic worth of cyberpower in manipulating information to its advantage, cumulatively but covertly provoking unrest in a country. In doing so, the state used the most appropriate offensive means available by perpetrating a non-harmful operation that, therefore, incurred the least amount of risk while achieving its objectives of information manipulation that a more destructive campaign could not have accomplished. This demonstrates the applicability of the strategic utility theory, focusing on how states use cyber capabilities per their optimal strategic purpose.

In answer to the research question 'To what degree do patterns of cyber incidents between 2000-2020 reflect changes in rival state behaviour in cyberspace?' this chapter began with analysing the DCID 2.0 data, identifying the lack of congruence between patterns of cyber incidents from 2000-2011, and 2012-2020. What the data made clear was evidence of escalation in cyberspace in terms of the number and frequency of cyber operations conducted by states against their rivals. This thesis then went on to question whether this evidence of escalation congrued with restraint theory as an explanatory framework for state behaviour in cyberspace. Using Russia as the primary case study, it became evident that the escalation of cyber incidents as identified in the data provided reasonable doubt as to the continued operability of restraint theory due to the lack of substantial retaliation from an increasing intensity of attacks on critical infrastructure.

Instead, strategic utility theory was proposed as an alternative framework. This understanding emphasised how states consciously engage in low-level cyber conflict in accordance with the optimal capabilities of cyber operations being information control and network disruption. Using Russia again as a case study, it became clear that the observable escalation of cyber engagement with its rivals during the 2010s reflected a change in the state's behaviour in cyberspace, as it increasingly adopted and used cyber as non-harmful yet strategically effective means of military power to execute military-political objectives. By conducting a higher frequency of cyber conflict yet maintaining operations at a low level, the state incurred less risk while successfully executing military-political objectives. Therefore, so far, patterns of cyber incidents from 2000-2020 do actively reflect changes in state behaviour. Moving away from the fear of retaliation, states have increasingly engaged in conscious and calculated escalation while still maintaining conflict levels below the threshold of war. This indicates the increased adoption of the strategic utilisation of cyberspace as a new medium of offensive yet low-level engagement. To continue assessing the inoperability of restraint theory and the applicability of strategic utility theory, the next chapter will discuss the impact and severity of cyber incidents.

Chapter Four – Impact and Severity of Cyber Incidents

Hypothesis 2: *When cyber operations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics.*

Valeriano and Maness' second hypothesis reasons that due to restraint dynamics, that is the potential for 'devastating and unlimited' consequences of total offensive operations, cyber operations and incidents will be of 'minimal' *impact* and *severity*. This conclusion rested on the idea that although there is speculation as to states' abilities to destroy or disrupt state, military, financial, and economic infrastructure through cyberspace, such malicious and damaging tactics are not the norm due to the fear of retaliation. While the previous chapter demonstrated a clear lack of congruence between the data gathered in DCID 1.0 and that in 2.0, the findings concerning the impact and severity of cyber incidents are far more alike, with very subtle differences.

Briefly noting the methodology used during this chapter, the severity scale for DCID 1.0 only ranged from one to five and was expanded to one to ten in DCID 2.0. Therefore, only data from

DCID 2.0 will be used for consistency. Table 4.1 documents this severity scale. It is worth noting that although it ranges up to ten, no cyber incident has ever scored above a six. Those operations with a score of six were incidents such as Stuxnet and Shamoon that breached the networks of critical and national infrastructure, causing widespread destruction and the impairment of the stored information. A severity rating of five accounts for incidents such as Flame, TV5Monde, or the Kyiv power outages; breaches that cause damage yet leave the network intact in terms of recoverable loss and functionality (Valeriano *et al.* 2022).

Table 4.1. Severity Scale

1. Probing/packet sniffing without kinetic cyber
2. Harassment, propaganda, denial and disruption
3. Stealing targeted critical information from one network
4. Widespread government, economic, military, or critical private sector network intrusion, multiple networks
5. Single/multiple critical network infiltration and physical attempted destruction
6. Single/multiple critical network infiltration and widespread destruction
7. Minimal death as direct result of cyber incident
8. Critical national economic disruption as a result of cyber incident
9. Critical national infrastructure destruction as a result of cyber incident
10. Massive death as a direct result of cyber incident

Looking at the data from 2000-2011 that Valeriano and Maness would have covered (they started in 2001, however, for the purposes of encompassing the complete range of data, 2000 is included here), the most common severity score was two (harassment, propaganda, denial, and disruption), with 59 counts out of the total 107 recorded incidents. There were 27 counts with a score of three (stealing targeted critical information), and 15 counts with a severity score of four (widespread government, economic, military, or critical private sector intrusion). The most severe score of five and six only had two counts each, making up 3.8% of total cyber incidents. The most common target type was private or non-state (for example, financial sector or defence contractors), with 80 counts (75%). Regarding the objectives of cyber operations, there were 51 counts of disruption, 24 counts of short-term espionage, 19 counts of long-term espionage, and 14 counts of degradation (ibid.).

In accordance with the conclusions made by Valeriano and Maness in 2014, this data demonstrates that severe cyber incidents are few and far between, with the majority of operations of low impact and severity. Most operations aim to disrupt online services, spread disinformation, or are cases of cyber espionage. The most severe attacks are rare, in keeping with the authors' conclusion that when cyber incidents do occur, they will be of minimal impact and severity. They explained this behaviour through restraint theory, arguing that it was due to the fear of potential consequences from more impactful and severe operations (interpreted as those above level six that would cause either death or severe destruction and disruption), that motivated states to restrain their cyber capabilities (Valeriano and Maness 2014). It is the purpose of this chapter to determine whether this is still the case regarding the updated data.

4.1 2012-2020 DCID 2.0 Analysis

Table 4.2 visualises the gradual increase in average severity score per year from 2000-2020. Disregarding 2002 as an anomaly caused by a lack of data rather than a lack of cyber operations, a steady increase can be observed over time. The highest average was in 2019, with a score of 3.6. Regarding the most common target type, it was still private or non-state with 157 counts (48% of the total 324 recorded incidents). The most common coercive objectives of cyber operations indicated an increase in severity, with long-term espionage as the most common (112), followed by short-term espionage (106), disruption (70), and finally degradation (36). This differs from the original findings where disruption took the lead, emphasising a move towards more impactful and severe operations over time. From 2012-2020, the most common severity score was three (stealing critical targeted information) with 131 counts, followed by 104 counts with a severity score of four (widespread intrusion). This can be contrasted to the original data covering 2000-2011, where the most common severity scores were two (harassment, propaganda, denial, and disruption), followed by three (stealing information) (Valeriano *et al.* 2022).

DCID 2.0 demonstrates changes in patterns of cyber conflict from 2000-2020, with an observable upwards trend in terms of states conducting more severe cyber operations that have more malicious and harmful impacts. However, this increase is still subtle, and the focus is still primarily on non-destructive cyber incidents with the most common objective being theft. Keeping in mind that the severity scale is out of ten, the average incident remains at a low level with a non-harmful (in terms of being overly disruptive or destructive) impact. This, therefore, displays a degree of

congruence with Valeriano and Maness' conclusion that when cyber incidents do occur, they will be of minimal impact and severity.

Alternatively, patterns of the *most severe* cyber incidents have witnessed a significant increase over time. Tables 4.3 and 4.4 document cyber incidents with either a five or six on the severity scale. From 2000-2011, there were only four incidents of this severity, whereas from 2012-2020, there were 19 recorded incidents, a 375% increase (Valeriano *et al.* 2022). This demonstrates a clear change in rival state behaviour; the growth of state-perpetrated cyber operations that intend to degrade or destroy, targeting national or critical infrastructure. The surge poses a direct challenge to Valeriano and Maness' contention that such operations with these targets would rarely occur due to the fear of uncontrollable consequences.

Table 4.2
Severity score averages per year 2000-2020

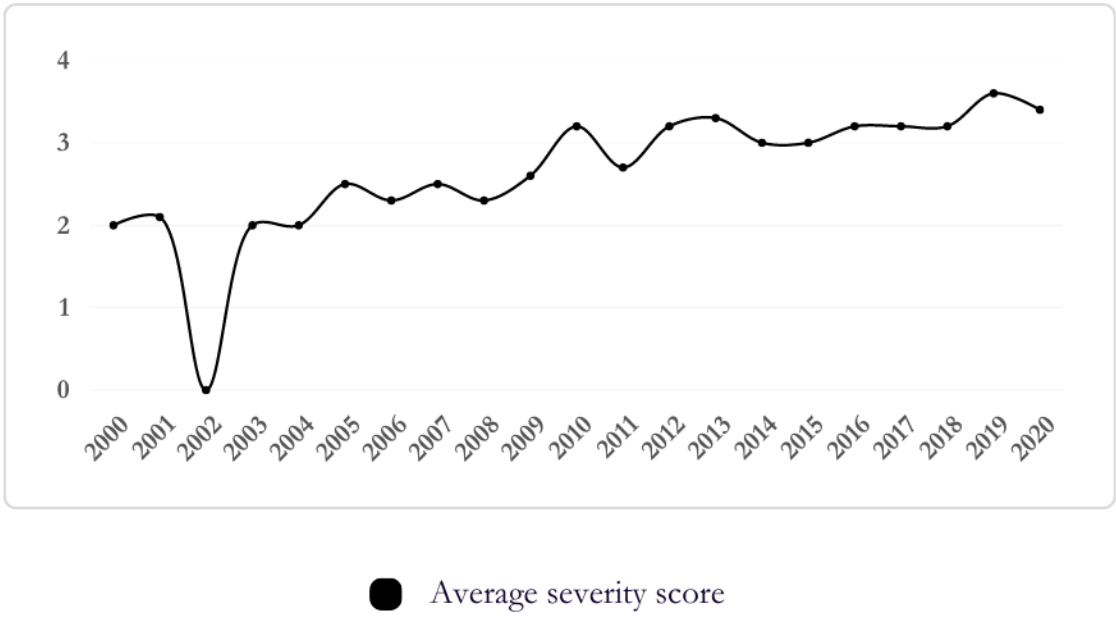


Table 4.3. 2000-2011 Cyber Incidents with a Severity Score of Five or Six

Incident	States involved	Method	Target	Initiator	Objective	Severity	Critical infrastructure
Cisco Raider	US China	Infiltration – keystroke login	Gov non-military	U.S.	Degrade	5	IT
NK Stuxnet	U.S. N. Korea	Infiltration – worm	Gov military	U.S.	Degrade	5	Nuclear
Stuxnet A	US Iran	Infiltration – worm	Gov military	U.S.	Degrade	6	Nuclear
Stuxnet B	Israel Iran	Infiltration – worm	Gov military	Israel	Degrade	6	Nuclear

Table 4.4. 2012-2020 Cyber Incidents with a Severity Score of Five or Six.

Incident	States involved	Method	Target	Initiator	Objective	Severity	Critical infrastructure
Wolf Creek	US Russia	Intrusion	Private/ Non-state	Russia	Degrade	5	Financial services
Grid Warning	US Russia	Intrusion	Gov non-military	U.S.	Disruption	5	Financial services
Iran Shipping Traffic Database	US Iran	Infiltration - worm	Gov military	U.S.	Degrade	5	Nuclear
Drone response	US Iran	Infiltration - worm	Gov military	U.S.	Degrade	5	IT
TV5Monde	France Russia	Infiltration - virus	Private	Russia	Degrade	5	Commercial facilities
German Steel Mill degrade	Germany Russia	Infiltration - virus	Private	Russia	Degrade	5	Critical manufacturing
Sandworm/ BlackEnergy	Russia Ukraine	Denial of service, DDoS, Botnets	Private	Russia	Degrade	5	Communications

DDoS							
Sandworm/ BlackEnergy Sabotage	Russia Ukraine	Infiltration - virus	Private	Russia	Degrade	5	Communications
Kyiv Power Outage A	Russia Ukraine	Infiltration - virus	Private	Russia	Degrade	5	Energy
Kyiv Power Outage B	Russia Ukraine	Infiltration - virus	Private	Russia	Degrade	5	Energy
NotPetya A	Russia Ukraine	Infiltration - worm	Private	Russia	Degrade	5	Financial services
Bad Rabbit (Bunny)	Russia Ukraine	Infiltration	Private	Russia	Degrade	5	Transportation
Israel Infrastructure Attack	Iran Israel	Infiltration - virus	Gov non-military	Iran	Degrade	5	Transportation
Shamoon 2.0	Iran S. Arabia	Infiltration – logic bomb	Gov non-military	Iran	Degrade	5	Energy
Shamoon 3.0 Saipem	Iran S. Arabia	Infiltration – logic bomb	Gov non-military	Iran	Degrade	5	Energy
Dustman Wipr	Iran S. Arabia	Infiltration – logic bomb	Gov non-military	Iran	Degrade	5	Energy
U.S. Left of Launch	U.S. N. Korea	Infiltration - worm	Gov military	US	Degrade	6	IT
Shamoon	Iran S. Arabia	Infiltration – logic bomb	Gov non-military	Iran	Degrade	6	Energy
RasGas Attack	Iran Qatar	Infiltration – logic bomb	Gov non-military	Iran	Degrade	6	Energy

Several implications can be derived from the above data. The most common perpetrators of severe cyber incidents were Russia (nine), the U.S. (seven), and Iran (six). Those cyber incidents with a score of six, so single or multiple critical network infiltrations causing widespread destruction, were predominantly perpetrated by the U.S. (Stuxnet and Left of Launch), and Iran (Shamoon and RasGas). There was far more of an increase in cyber incidents with a rating of five (from two to 16) than there were those with a rating of six (two to three). Saudi Arabia and Ukraine were the most heavily targeted states by their regional rivals Iran and Russia. Regarding the objective, all bar one had the intention of degrading the target's network and system. This is a consistent conclusion from 2000-2020. The most common target was the energy sector (seven incidents), followed by the nuclear sector (four incidents) (Valeriano *et al.* 2022). This indicates a clean break from Valeriano and Maness' contention that it would be 'unlikely' for states to attack and destroy power networks, social services, or government organisations, challenged by the behaviour of states such as Iran who have consistently targeted Saudi Arabian critical infrastructure over the course of a decade (Valeriano and Maness 2014, 350).

4.2 Restraint Theory Applicability to DCID 2.0

Valeriano and Maness' argument rests on the idea that states will refrain from conducting severe cyber operations that have a significantly disruptive or destructive impact because of the fear that such operations could cause uncontrollable consequences. They, therefore, argue that the severity and impact of cyber operations will remain 'minimal', interpreted as predominantly scored under disruption or espionage on the severity scale (ibid.). While the findings from DCID 2.0 showed an incline in the average severity of cyber incidents, revealing the increasing commonality of operations with more detrimental impacts, the difference with the original data is marginal. To a degree, the congruence is based on the idea that cyber conflict is still predominantly conducted at a 'low' level. However, the evidence of escalation of the most severe cyber incidents leaves room for further analysis as to how this reflects changes in rival state behaviour; whether states are still operating with restraint, or whether there are other driving forces behind such actions.

The congruence between restraint theory and DCID 2.0 is based on the continuity of the majority of cyber operations being of low severity and impact. Most incidents were either cyber espionage or intrusions, types of cyber activity that have the primary purpose of theft, rather than disruption or destruction. In 2014, Valeriano and Maness stated that cyber conflict is the 'least harmful tactic' (ibid., 349). This feeds into the data, with only 5.5% of total incidents from 2000-2020 having a

severity score of five or six, those that cause significant disruption or destruction, and only 18.5% of methods being network infiltrations that have the capability of causing extensive network damage (the rest being non-harmful such as intrusions) (Valeriano *et al.* 2022). Consequently, the central conclusion made in 2014 that state behaviour is restrained in cyberspace is still applicable to the broad findings of the dataset, with indications that on average, cyber incidents maintain a low level of impact and severity. However, it should be kept in mind that there is still a discernible upwards trend with regard to the damaging impact of cyber incidents, and that the explanation of fears of retaliation remains in question.

Where the theory's applicability to the data wanes is the finding that the most severe cyber incidents, as recorded in Tables 4.3 and 4.4, all target critical infrastructure with the malicious intent to degrade. Whereas Valeriano and Maness based their conclusion that these operations are 'unlikely' on only four recorded incidents, from 2012-2020 this type of cyber engagement increased exponentially in comparison. While these types of incidents remain rare, they do pose a challenge to the central tenets of restraint theory. Not only does this increase in willingness to damage or degrade a rival's national security apparatus directly contradict restraint theory's position of the unlikelihood of such operations that threaten the threshold for war, but akin to the increased number and rate of cyber operations discussed in the previous chapter, there is little evidence of retaliation stemming directly from these incidents despite their severe nature and significant target.

The Iran-Saudi Arabia dyad demonstrates that while the most severe cyber incidents remain rare, such incidents are certainly *not unlikely* to target critical infrastructure. In fact, evidence of Iranian behaviour in cyberspace indicates a lack of restraint or fear of retaliation when conducting its cyber operations. A rivalry that can be traced back to the 1979 Iranian Revolution, Saudi Arabia is now bearing the brunt of the development of Iranian offensive cyber capabilities. One of the most notable examples of a severe cyber incident with a severity score of six is the 2012 Shamoon operation. Attributed to government-sanctioned Iranian actors, the wiper malware targeted Saudi Aramco, one of the world's largest oil producers, erasing data on three-quarters of its computers (Cyberlaw 2021). This forced the company to shut down its internal network and disable all Internet and email services, however, according to Aramco, it did not impact oil production and exploration (ibid.). Subsequent statements suggested that the attack could have been an act of retaliation against the al-Saud regime for their links to the crimes occurring in the Middle East, or in response to the regime's connection with the U.S. (ibid.). The Saudi Interior Ministry stated that "The August cyber-attack on Aramco's computer network targeted not just the company but the

Kingdom's economy as a whole" (Dehlawi and Abokhodair 2013, 74). Similar attacks continued into the 2010s, in the form of Shamoon 2.0 and 3.0, as well as the notably severe Dustman Wipr Attack (Valeriano *et al.* 2022). However, despite this lengthy onslaught of severe and impactful operations against the state's critical infrastructure, there has been little retaliation from the Saudi Arabian regime bar public attribution of the incident to Iran and advocation for the strengthening of the nation's cyber defences (Reuters 2017a).

The Iranian-Saudi dyad demonstrates that the most severe cyber-attacks lack congruence with restraint theory. Not only do these destructive cyber operations target national infrastructure that is critical to the survival of the target state's regime, but there is also a lack of evidence of any form of substantial retaliation to such operations. While acknowledging that these cyber incidents remain a rarity in the grand scheme of interstate cyber conflict and that stat restraint is still evident on the whole, the increase in the number and frequency of such impactful operations does not correlate with the second hypothesis. Therefore, it acts as a weak framework for explaining the observable changes in the patterns of cyber conflict over the past two decades.

Whether the maintenance of low-level conflict is due to the fear of retaliation or not, this thesis would contend that the lack of evidence of any high-level retaliation in responses to severe and impactful operations targeting critical infrastructure provides reasonable doubt as to this conclusion. This questions the validity of the argument that states would act out of fear of something that has never occurred, nor been significantly threatened. This, therefore, still leaves space for the argument of the more appropriate operability of the theory of strategic utility, which explains both the increase in more severe cyber operations and the maintenance of most operations at a low level of severity and impact.

2014 Hypothesis 2: *When cyber operations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics.*

2023 Hypothesis 2: *When cyber incidents do occur, they are likely to be employed based on their optimal strategic utility of information control and network disruption, resulting in largely minimal impact and severity.*

When explaining how the patterns of cyber conflict reflect changes in state behaviour in terms of the dominant use of low-impact and non-harmful cyber operations, this author finds it useful to focus on the strategic utility of such capabilities. This approach focuses on the military-political

objectives of the perpetrating state, and how cyber means are used in accordance with their optimal strategic purpose, usually information control and network disruption, to achieve these goals. Using this framework, it stands to reason that the majority of cyber incidents are non-harmful or non-destructive in their impact due to the primary use of cyberspace by states as facilitating espionage and disruption, methods reflected in the DCID 2.0. Hence, the new hypothesis claims that when cyber incidents do occur, they are *likely* to be employed based on their optimal strategic utility for information control and network disruption, resulting in their predominantly minimal impact and severity.

The same framework can be applied in the few cases of severe cyber incidents that come under the 'unlikely' umbrella of state use. When considering that the objective of the incidents recorded above was the degradation of the enemy's systems, it is logical to conclude that states continued to use the most appropriate and strategically sound means of warfare for that operation, one that otherwise could not have been achieved through conventional means. These higher-level cyber operations also maximised some of the unique characteristics of cyber operations such as its favourable advantage to the offence, its covert nature, and the inexpensiveness of use (Sheldon 2011, 101).

Using the case study of Iran and Saudi Arabia again for comparison, strategic utility theory highlights the connection between the political objectives of the state and the increased adoption and use of cyber means as appropriate methods of achieving these goals. Since developing the capabilities to do so, Iran has incorporated cyberspace into its arsenal of perceived deterrence against rival states that often have both technological and conventional superiority, thus using cyber capabilities not so much as malevolent weapons of destruction, but more so as a method of continuously projecting power (Moore 2022, 204). Aspiring to this "deterrence through asymmetry", Iran has increasingly targeted critical and civilian assets through the medium of cyberspace in order to reduce the need for direct military friction between conventional forces (ibid., 202). When compared to the DCID 2.0 data in Table 3.5, the change in cyber behaviour is evident. Iran increasingly adopted cyber operations not as a means of persecuting war, but rather as a newly revealed medium of executing the military-political objectives of the state such as the projection of power.

Moore contends that Iranian cyber behaviour cannot be analysed in separation from its geopolitics. A deeply ideological state, events such as the 1953 coup d'état, the forced re-installation of the

Western-backed Shah, and the 1979 Revolution all contributed to the anti-Western sentiment that runs deeply as a driving force behind much of Iran's foreign policy (ibid., 204). Moore argues that in the absence of being able to provide a credible conventional threat to its stronger adversaries such as the U.S., Iran employs cyber operations as a way of replacing the missing technological and operational superiority with aggressiveness (ibid.). While this could be interpreted as Iran restraining its cyber capabilities from 'total' operations that would threaten conventional warfare, the evidence of patterns of escalation in cyberspace devalues restraint theory, instead emphasising the usefulness of examining the roots, purpose, and intent of Iranian military-strategic behaviour as an explanatory framework.

While Shamoon was one of the first demonstrations of Iranian offensive capability in cyberspace, the operation did not even *attempt* to target Saudi Aramco's industrial control networks that govern oil production and exploration. Instead, it was a 'crude' wiper malware that ran through Aramco's computer systems without discrimination and with no evidence of intent to do targeted or substantial damage (ibid., 203). This highlights the lack of intended destruction, instead emphasising the use of this lower-level operation as a means of projecting power against its rival through the very public targeting of one of its key financial resources.

A further supporting point stems from the evidence of the escalation (evident in DCID 2.0) of Iranian cyber activity after 2010 and the discovery of the Stuxnet worm. In an alleged joint U.S.-Israeli operation, the malware infiltrated the Natanz nuclear enrichment facility in Iran and attempted to destroy its centrifuges, thus undermining the nuclear program (Rid 2012; Denning 2012). Considering the subsequent escalation of Iranian cyber activity against the U.S., Israel, and Western-connected Saudi Arabia, it stands to reason that Iran recognised the offensive potential of cyber capabilities, and weaponised this new domain to exploit its asymmetric advantages, in turn projecting power and maintaining perceived deterrence.

Therefore, by analysing the intent behind such cyber behaviour, it becomes evident that the patterns of cyber incidents identified within the DCID 2.0 do reflect changes in rival state behaviour, not indicating restraint in cyberspace but rather the increase of strategic employment of cyber operations in accordance with the military-political goals of the attacking state. Not only did Iran continually utilise an inexpensive means of warfare that favours the offence, but it exploited its primarily non-destructive nature to conduct mid-range cyber operations against its regional rivals to project power against asymmetrically capable rivals.

To reiterate this conclusion, the DCID 2.0 data on China shows that the state has not partaken in any severe cyber operations despite being technologically advanced. Whereas Valeriano and Maness posited in their article that "if a state is endowed with the ability to infiltrate its adversary in cyberspace, it will do so" China focuses on conducting extensive espionage operations against the target's infrastructure to gain access to critical technologies and collect information on the intentions of its rivals (Valeriano and Maness 2014, 349). Adhering to the approach of 'active defence', China's cyberspace strategy consists of three layers: a revision of the U.S.-led international system to give China more prominence in great power relations; the control of the domestic flow of information; and its techno-nationalist industrial policy that aims to break from a dependency on the West (Bey 2018, 32-33). By considering these factors as driving forces behind the military-strategic objectives of the state, it makes sense that China would use cyber means such as espionage and network intrusions, rather than higher severity operations. These methods enable the gathering of information that is so crucial to the above objectives, while not threatening the global flow of trade, information, and interconnectivity that fundamentally underpins China's economy (ibid., 32).

China is a case where, upon analysis of the data, changes in the patterns of cyber incidents are marginal, as are changes within its cyber behaviour. However, the data still reflects the action. By conducting these 'low-level' operations, there are no indications that China is restrained by fears of escalation. Instead, the state maximises the strategic utility of cyber weapons to execute its objectives.

To answer the research question 'To what degree do patterns of cyber incidents between 2000-2020 reflect changes in rival state behaviour in cyberspace?', this chapter has addressed the second hypothesis of restraint theory which contended that cyber operations will be of minimal impact and severity due to restraint dynamics. Analysis of the DCID 2.0 showed that cyber incidents have gradually increased in severity and impact, indicating the increasing commonality of more harmful cyber operations. Acknowledging the maintenance of state restraint in terms of the continued low-level nature of the majority of cyber conflict, the increase in more severe operations as well as the maintenance of majority low-level engagement does not reflect restraint based on fears of escalation, but rather the strategically driven behaviour of states in cyberspace. The case studies of Iran and China portray states maximising the worth of cyber capabilities in different ways, whether that be power projection or espionage, in accordance with the state's individual military-political

goals. This calculated employment of cyberpower to perpetuate rival relationships while realising individual objectives moves explanations of state behaviour away from the dynamics of restraint, and towards the strategic utilisation of cyber operations as military means of executing political goals.

Conclusion

This thesis has answered the research question 'To what degree do patterns of cyber incidents between 2000-2020 reflect changes in rival state behaviour'. By using the *Dyadic Cyber Incident Dataset*, the rate, number, impact, and severity of cyber operations perpetrated by states from 2000-2020 was evaluated, identifying deviations from Valeriano and Maness' original conclusions made in 2014. What the findings showed was that there was a lack of congruence between the rate and number of cyber incidents from 2000-2011 and 2012-2020, also when considering the number of the most severe cyber incidents. This, therefore, indicated clear changes in the patterns of cyber conflict over the two decades, with evidence of escalation in cyberspace. However, there was minimal difference identified in the average severity, meaning that although cyber conflict has become much more common as an offensive tool within state rivalries, it has predominantly remained at a low level.

When ascertaining how the observable patterns of cyber conflict from 2000-2020 reflected changes in state behaviour in cyberspace, this thesis first operationalised Valeriano and Maness' theory of state restraint in cyberspace against the evidence of escalation. While there were indications of restraint, or states not using their full offensive capabilities in cyberspace, escalatory behaviour against critical infrastructure with a lack of retaliation indicated that the theory lacked continued operability, especially when considering overtly aggressive states such as Russia and Iran.

With the literature review highlighting the omission from restraint theory being the strategic employment of cyberpower by states, the theoretical framework of strategic utility was presented as an alternative explanation for changes in state behaviour in cyberspace. Reflecting on the patterns of cyber conflict, this new theory highlighted that restraint was being conducted by states not out of fears of retaliation, but in accordance with the optimal purpose or the worth of cyber operations predominantly being information control or network disruption; 'low-level' operations. Accounting for the more severe incidents, it still stood to reason those states deliberately employed

mid-range operations, utilising the unique strategic features such as the covert or offensively favourable nature of cyber operations to execute specific objectives without creating unnecessary risk. Case studies were used in order to reiterate both the reasonable doubt around the continued operability of restraint theory, and the subsequent appropriateness of strategic utility theory as a framework for understanding the changes in patterns of state behaviour.

Betts concluded that states engage in strategic behaviour that maximises the value of the operation by choosing the most appropriate means and minimising the risk involved (Betts 2000, 9-10, 50). Strategic utility follows the same line of thinking: information technology is utilised as the most appropriate means of executing the military strategy; the value of cyber operations is often maximised with the objective of information control and network disruption; and the risk is minimised as these incidents will predominantly be of low impact and severity to both target and attacker. The strategic effect of such incidents comes from the discussed ability of cyberpower to control situations, restrict or prevent the adversary's options in the same domain, or degrade the adversary's instruments of military power, all outcomes and consequences that have been shown to be possible through the calculated and premeditated use of cyber operations (Milevski 2016, 14-15).

Hence, patterns of cyber conflict, as observed through the DCID 1.0 and 2.0, reflected changes in rival state behaviour in terms of the degradation of the dynamics of restraint, and the increased adoption and utilisation of cyberpower as a strategically sound military means of executing policy goals.

In terms of further research stemming from this thesis, the first step would be to apply strategic utility theory to the case studies not analysed in-depth so far, that being states such as the U.S., and North Korea, as well as other dyads such as India and Pakistan that have been engaged in long-term cyber conflict. The Russian invasion of Ukraine in 2022 also offers a new case study of nation-state use of cyber operations as wartime military instruments and a force multiplier for conventional offensives, with information on these offensives being uploaded to the DCID at the time of writing (Jensen *et al.* 2022). Furthermore, an approach that was considered for this research but not carried out was the use of strategic culture theory. Given how little has been published on cyberspace using this framework of analysis that focuses on how factors such as history, geography, and economics influence national styles of strategy, it could be an interesting offshoot of this research to further investigate the drivers behind state behaviour in cyberspace.

This research has primarily contributed to the fields of cybersecurity studies and strategic studies. Regarding the practical implications of this research for policymakers, understanding the cyber-threat landscape from nation-states has never been more important, with Microsoft reporting in 2022 that the proportion of cyber-attacks perpetrated by states targeting critical infrastructure has risen from 20 to 40%, partially due to the Russian invasion of Ukraine (Microsoft Digital Defence Report 2022). By understanding how and why states conduct cyber operations through identifying patterns and trends in cyberspace, this research has contributed to the ability of policymakers to recognise future turning points and significant events that could indicate the intensification of cyber aggression, as well as inform appropriate responses to such incidents.

Bibliography

Alperovitch, Dmitri. 2011. 'Towards Establishment of Cyberspace Deterrence Strategy'. *3rd International Conference on Cyber Conflict*, Tallinn, Estonia: 1-8.

Arquilla, John, and David Ronfeldt. 1999. 'The Advent of Netwar: Analytic Background'. *Studies in Conflict & Terrorism* 22 (3): 193–206.

Barrass, Gordon, and Nigel Inkster. 2018. 'Xi Jinping: The Strategist Behind the Dream'. *Survival* 60 (1): 41–68.

Bateman, Jon. 2022. 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications'. *Carnegie Endowment for International Peace*. December 16, 2022. https://policycommons.net/artifacts/3348853/russias-wartime-cyber-operations-in-ukraine/4147737/.

Betts, Richard. 2000. 'Is Strategy an Illusion?' *International Security - INT SECURITY* 25 (October): 5–50.

Betz, David. 2012. 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed'. *Journal of Strategic Studies* 35 (5): 689–711.

Betz, David, and Tim Stevens. 2011. *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1st edition. London, U.K: Routledge.

Bey, Matthew. 2018. 'Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition. *The Cyber Defense Review*, December 18, 2018.

Brenner, Susan W. 2007. '"At Light Speed": Attribution and Response to Cybercrime/ Terrorism/Warfare'. *The Journal of Criminal Law and Criminology (1973-)* 97 (2): 379–475.

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

Cornish, Paul, David Livingstone, David Clemente, Claire York. 2010. *On Cyber Warfare*. Chatham House.

Dehlawi, Zakariya, and Norah Abokhodair. 2013. 'Saudi Arabia's Response to Cyber Conflict: A Case Study of the Shamoon Malware Incident'. *IEEE International Conference on Intelligence and Security Informatics*: 73–75.

Denning, Dorothy. 2012. 'Stuxnet: What Has Changed?' *Future Internet* 4 (December): 672–87.

Egloff, Florian J., and Max Smeets. 2021. 'Publicly Attributing Cyber Attacks: A Framework'. *Journal of Strategic Studies* (0): 1–32.

Farwell, James P., and Rafal Rohozinski. 2012. 'The New Reality of Cyber War'. *Survival* 54 (4): 107–20.

Gartzke, Erik. 2013. 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth'. *International Security* 38 (2): 41–73.

Gerasimov, Valery. 2013. 'The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations'. *Military-Industrial Kurier*, February.

Gray, Colin. 2009. 'Understanding Airpower: Bonfire of the Fallacies'. Air University, Air Force Research Institute.

———. 1999. *Modern Strategy*. 1st edition. New York: Oxford University Press.

Gustafsson, Karl, and Linus Hagström. 2018. 'What Is the Point? Teaching Graduate Students How to Construct Political Science Research Puzzles'. *European Political Science* 17 (4): 634–48.

Hare, Forrest. 2012. 'The Significance of Attribution to Cyberspace Coercion: A Political Perspective'. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–15.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. 2019. 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist'. *Journal of Strategic Studies* 42 (2): 212–34.

Jensen, Ryan C. Maness, Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias, Benjamin. 2022. 'Tracking Competition in Cyberspace: Announcing the Dyadic Cyber Incident Dataset Version 2.0'. Modern War Institute. 14 October 2022. https://mwi.usma.edu/tracking-competition-in-cyberspace-announcing-the-dyadic-cyber-incident-dataset-version-2-0/.

Jervis, Robert. 1979. 'Deterrence Theory Revisited'. Edited by Alexander George and Richard Smoke. *World Politics* 31 (2): 289–324.

Jinghua, Lyu. 2019 'What Are China's Cyber Capabilities and Intentions?' *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

Johnston, Alastair Iain. 1995. 'Thinking about Strategic Culture'. *International Security* 19 (4): 32–64.

Kari, Martti J. 2019. 'Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats'. *JYU Dissertations*.

Kari, Martti J., and Katri Pynnöniemi. 2023. 'Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception'. *Journal of Strategic Studies* 46 (1): 56–84.

Klein, James P., Gary Goertz, and Paul F. Diehl. 2006. 'The New Rivalry Dataset: Procedures and Patterns'. *Journal of Peace Research* 43 (3): 331–48.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?' *Journal of Conflict Resolution* 63 (2): 317–47.

Kukkola, Juha. 2020. 'The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry'. NATO CCDCOE Publications: 9-30.

Lee, Robert M, and Thomas Rid. 2014. 'OMG Cyber!' *The RUSI Journal* 159 (5): 4–12.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation.

Lilly, Bilyana, and Joe Cheravitch. 2020. 'The Past, Present, and Future of Russia's Cyber Strategy and Forces'. NATO CCDCOE Publications, Tallinn. 129–55.

Maness, Ryan C, Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen, and Jose M. Macias. 2022. 'Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 2.0'.

'Microsoft Digital Defense Report 2022 | Microsoft Security'. n.d. Accessed 26 May 2023. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

Milevski, Lukas. 2020. 'Enunciating Strategy: How to Talk about Strategy Effectively'. *Military Strategy Magazine* 7 (1): 18–25.

———. 2016. 'Making Sense of Strategy's Relational Nature'. *New Strategist* 1 (May): 9–19.

Moore, Daniel. 2022. *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press.

National Research Council. 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies Press.

Nye, Joseph S. 2011. 'Nuclear Lessons for Cyber Security?' *Strategic Studies Quarterly* 5 (4): 18–38.

Raud, Mikk. 2016. *China and Cyber: Attitudes, Strategies, Organisation*. NATO Cooperative Cyber Defence Centre of Excellence.

Reuters. 2017a. 'Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces', 23 January 2017, sec. Internet News. https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

———. 2017b. 'U.S. Authorities Charge Russian Spies, Hackers in Huge Yahoo Hack', 16 March 2017, sec. Media and Telecoms. https://www.reuters.com/article/us-yahoo-hack-indictments-fsb-idUSKBN16N0CO.

Rid, Thomas. 2012a. 'Cyber War Will Not Take Place'. *Journal of Strategic Studies* 35 (1): 5–32.

———. 2013. 'Cyberwar and Peace: Hacking Can Reduce Real-World Violence'. *Foreign Affairs* 92 (6): 77–87.

Rid, Thomas, and Ben Buchanan. 2015. 'Attributing Cyber Attacks'. *Journal of Strategic Studies* 38 (1–2): 4–37.

Rid, Thomas, and Peter McBurney. 2012. 'Cyber-Weapons'. *The RUSI Journal* 157 (1): 6–13.

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

Schmidt, Michael S., and Nicole Perlroth. 2020. 'U.S. Charges Russian Intelligence Officers in Major Cyberattacks'. *The New York Times*, 19 October 2020, sec. U.S. https://www.nytimes.com/2020/10/19/us/politics/russian-intelligence-cyberattacks.html.

Schmitt, Michael. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press.

Schneider, Jacquelyn. 2022. 'A World Without Trust', 15 February 2022. https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust.

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. 1st edition. Public Affairs.

'Shamoon (2012)'. 2021. International Cyber Law: Interactive Toolkit. 17 September 2021. https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012).

Sheldon, John. n.d. 2011. 'Deciphering Cyberpower: Strategic Purpose in Peace and War'. *Strategic Studies Quarterly* 5 (Summer): 95–112.

Shires, James. 2022. *The Politics of Cybersecurity in the Middle East*. Oxford University Press.

Steed, Danny. 2021. *The Politics and Technology of Cyberspace*. 1st edition. Routledge.

Thompson, William R. 2001. 'Identifying Rivals and Rivalries in World Politics'. *International Studies Quarterly* 45 (4): 557–86.

Valeriano, Brandon, and Ryan C Maness. 2014. 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11'. *Journal of Peace Research* 51 (3): 347–60.

Valeriano, Brandon, Ryan C Maness, Kathryn Hedgecock, Benjamin M. Jensen, and Jose M. Macias. 2022. 'Dyadic Cyber Incident Dataset v 2.0'. Harvard Dataverse. https://doi.org/10.7910/DVN/CQOMYV.

Wilde, Gavin. 2022. 'Cyber Operations in Ukraine: Russia's Unmet Expectations', December. *Carnegie Endowment for International Peace.* https://policycommons.net/artifacts/3336743/cyber-operations-in-ukraine/4135603/.