University of Glasgow

School of Social and Political Sciences

'Arms Racing in Cyberspace'

September 2015

0900425

Presented in partial fulfilment of the requirements for

the Degree of

Master of Research in International Relations

Acknowledgements

I thank my teacher and supervisor Dr Brandon Valeriano for sparking my interest in the study of International Relations, and for his ongoing support and encouragement of my research.

Abstract

Arms races, or threat driven mutual military build-ups, are traditionally associated with a dangerous escalation in interstate tensions. The heightened perception of threat in the cyber domain invites the question of how states are reacting to their security concerns in cyberspace. This paper adopts a mixed methods approach to first empirically establish the existence of a cyber-arms racing dynamic within the international system, and secondly to investigate, statistically, how a state's cybersecurity can be enhanced in a more positive, and less confrontational way. Case study methods are used on two rival state dyads: the United States – Iran, and North Korea – South Korea, to measure the rates of build-up in their cyber capabilities, and find evidence of external cyber threats, and competitive interaction. The results confirm that cyber arms racing in the international system is a reality, but that a focus on increasing defensive cyber infrastructure, as opposed to engaging in the militarisation of cyberspace, offers the best way forward for increased cybersecurity.

Table of Contents

List of Figures

1 INTRODUCTION

The highly interconnected digital age of the 21st century has given rise to new vulnerabilities, and a rapidly developing fear within the international political arena over a new form of interstate conflict. Cyber warfare, or the politically motivated hacking of enemy computer systems, is supposedly becoming the number one threat to national security. In 2012 for instance US Defence Secretary Leon Panetta warned of a "cyber-Pearl Harbour" from hackers who could inflict devastating damage on the United States critical infrastructure. (Bumiller and Shanker 2012) The threat from cyber-attacks consistently tops elite and public opinion polls as the greatest security concern, and there is a growing understanding that the "drumbeat of threat rhetoric" (Lindsay, 2013: 367), despite the evident restraint thus far in interstate cyber interactions (Valeriano and Maness 2015), is inspiring countries to channel ever increasing resources into their ability to defend themselves against cyber-attacks and, more worryingly, to prepare for offensive operations in cyberspace.

The media frequently uses the term 'arms race' to describe the current proliferation of cyber warfare capabilities in the international system (Corera 2015), and a 2012 survey found that 57% of security experts and policy elites believed there was an ongoing arms race in cyberspace. (McAfee 30 January 2012) What is clearly lacking however is the proper academic research and empirical evidence to support these claims. The term 'arms race' is traditionally used to describe the threat driven, and competitive build-up of military power between two rival countries (Richardson 1960), and has long been a major focus of international relations (IR) scholarship. What drives research on this topic, as well as efforts to control such behaviour, is the risk of military competition escalating out of control, causing deterioration in interstate relations, and bringing countries closer to the brink of war. Indeed, there is a wealth of IR research that demonstrates a link between arms races and the escalation of conflict. (Wallace 1979; Vasquez 1993; Sample 1997; Gibler et al 2005) Well known historical cases include the pre WWI Anglo-German naval competition and the Cold War nuclear build up between the USA and Soviet Union, and there is now an opportunity to apply this concept to the newly considered military domain of cyberspace.

Cyber security is clearly a burgeoning topic of interest for policy makers and academics, but we in fact know very little about the true nature of interstate interactions in cyberspace other than from the politicians, media, and the cyber security companies who often stand to gain from inflating the threat. Serious academic and empirically grounded research is therefore

urgently needed to bring measured analysis to the subject. It is only in very recent years that cyberspace has been considered an arena for interstate conflict, and this represents new and theoretically exciting territory for IR scholars who can bring their knowledge of international politics, and their older theoretical perspectives to bear on this new global security issue. Unfortunately, as Kello (2013: 13) points out, the IR community has "barely begun to apply their theoretical toolkits to explain, model, or predict competition in the cyber arena". Aside from the ground breaking work by Valeriano and Maness (2015) in coding interstate cyber incidents, there is indeed a lack of empirical research on the dynamics of the cyber domain, which is necessary for the IR discipline to retain its policy relevance. Taking another step towards rectifying this, the research here provides data and theory driven analysis to investigate a potential arms racing dynamic in cyberspace, thus gaining important insights into one of the most pressing and rapidly developing security issues in world politics.

An understanding of the patterns of state behaviour in the cyber domain, allows the researcher to inform the public policy dialogue in constructive ways, and is the first step in creating a more secure and cooperative environment. Investigating the nature and magnitude of cyber arms racing can inform the debate over the need to increase international cooperation in cyberspace, and reduce the arms race's escalatory potential. Knowing whether cyber build-ups are driven by external threats and security competition with other countries, as opposed to domestic factors is also important for giving direction to future policies to control cyber arms proliferation. Furthermore, it will also be helpful to know to what extent cyber arms races are driven by real as opposed to imagined threat. If driven purely by irrational fear, then we must warn of the dangers of fearmongering and encourage the development of cybersecurity policies that are more proportional to the actual cyber threat. Research like this is also beneficial to the progression of international relations theory as it applies to the cyber domain. The importing of old theories, like those pertaining to arms races, into a different domain, can help in evaluating their applicability and highlight the potential need for new theories to be developed in order to account for the unique character of the cyber domain.

The main methodological approach will be to conduct case studies of some of the key cyber actors in international politics. First, the research will be situated within the context of the cyber domain, before explaining the traditional theories of arms racing, and then discussing how a cyber-arms race can be identified. The next step will be to present data on the changing

cyber warfare capabilities of two rival state dyads, USA and Iran, and North and South Korea, measure the scale of their arming behaviour, and judge whether it represents abnormal rates of increase. Then more qualitative evidence will be examined to investigate the extent to which these build ups in cyber power are driven by external threats and in reaction to one another specifically.

If previous research on the consequences of arms races is anything to go by, then the militarisation of cyberspace and the escalation in offensive cyber weaponry is surely something to be scaled back. Political leaders are currently promoting the need to develop offensive capabilities to deter their enemies and increase security in the cyber domain. To test whether this is indeed increasing cybersecurity in a positive manner, statistical methods will be adopted in the latter part of this paper to show whether the move to militarise cyberspace is actually making countries' internet networks more secure, and whether there are more positive options available. This will provide evidence to allow a normative judgement to be made on the efficacy of engaging of the cyber arms race, and give policy guidance towards alternative methods of improving cyber security.

2 THE CYBER DOMAIN

Introducing the concept of cyber arms racing first requires an overview of the environment in which interstate cyber relations are played out. According to Choucri (2010: 228), the development of cyberspace has put states in an "unprecedented situation", characterised by high levels of uncertainty as they try to maintain control in the face of a changing global security environment. It also represents new theoretical territory in the study of international relations, and new opportunities for analysis on how states are responding to their insecurities. The purpose here is to review the key theoretical aspects of the cyber domain, and explain why the nature of cyberspace makes security competition likely, regardless of whether it is justified or not. In doing so, the scene is set for introducing the new concept, of the cyber arms race, to the cybersecurity literature.

Cyberspace has been defined by Nye (2011: 19) as the "internet of networked computers but also intranets, cellular technologies, fibre optic cables, and space based communications". It is also crucial to recognize its physical, as well as virtual, aspects since, as Clarke and Knake (2012: 70) put it, cyberspace not only refers to "all of the computer networks in the world"

but to “everything they connect and control.” This is especially important in discussions about the physical threat that cyber-attacks can pose to a nation’s infrastructure, which in the digital age is becoming increasingly dependent on computer network systems. One of the greatest fears in the US concerning the impact of cyberattacks for instance, is the damage they could inflict on the American “power grid, transportation system, financial networks, and government.” (Bumiller and Shanker 2012)

Cyberspace is now considered the “fifth domain” of warfare after land, sea, air, and space (The Economist 1 July 2010), with ‘cyber warfare’ defined as the use of “computer network attacks as a use of force to disrupt an opponent’s physical infrastructure for political gain”. (Lindsay 2013: 372) Clarke and Knake (2012: 31) declare it “the next threat to national security” and that “in anticipation of hostilities nations are already preparing the battlefield”. Thomas Rid (2013) on the other hand, by pointing to the fact that we have yet to witness a single death from a cyber-attack, argues that this is a misnomer, and an over exaggeration. Using instead the term cyber ‘conflict’, Valeriano and Maness (2015: 32) define it as “the use of computational technologies in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities.” They demonstrate empirically that despite the hype surrounding the cyber threat, the use of these tactics has actually been rather limited with only 16% of rival states having engaged in cyber conflict, which on average has occured at very low levels of severity. (Valeriano and Maness 2015: 89) One of the most prominent incidents was the ‘Stuxnet’ attack which resulted in the destruction of a fifth of Iran’s nuclear centrifuges, yet estimates vary widely on the extent to which this held back Iran’s nuclear programme. (2015: 153) Consequently, we should bear in mind that despite high levels of perceived threat, sources of actual cyber threats between countries have so far been rather limited.

Arms races require a build-up of arms, or weapons, which in the cyber conflict domain are defined by Rid and McBurney (2012: 6) as “computer codes that are used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.” Broadening this out, Valeriano and Maness (2015: 33) discuss the key methods of cyber-attack which include simple “website defacements or vandalism”, often used as a form of propaganda; Distributed Denial of Service (DDoS) whereby the targeted websites or servers are brought down by overloading the system with data requests; intrusions and infiltrations via the use of Trojans, backdoors and trapdoors,

logic bombs, worms, viruses, packet sniffers, and keystroke logging; and Advanced Persistent Threats which can involve the above methods but are especially stealthy and technologically sophisticated. Unlike the physical warfare domain, the virtual nature of cyber weapons makes it very difficult for states to gain an accurate picture of one another's capabilities, and states do not want to reveal what they can do for fear of their enemies replicating their technologies and methods. (Valeriano and Maness 2015: 58) The secrecy surrounding the cyber domain suggests that a threat driven cyber arms race would be influenced more by perceptions of what capabilities other states may possess, rather than being based on reliable information.

An important facet of cyber capabilities is that harnessing them can be much cheaper than building up conventional military strength. In 2009, the General of the US Air Force Cyber Command, William T Lord, remarked that in cyberspace "the price of admission is inexpensive…it's a laptop computer and a connection to the internet." (Derene 2009) Consequently, there is an understanding that cyber capabilities provide weaker states with an asymmetric advantage, and create a level playing field with more powerful states. Liff (2012: 410) explains that this asymmetric advantage is also a result of the fact that the most developed and technologically advanced countries are very network dependent and thus vulnerable, as well as the idea that there is no cost of force projection in a domain which lacks the constraints of geography. The implications for cyber arms racing is that most states, regardless of their conventional power, can participate, as the low cost makes it easier for states to increase their capabilities. The level of threat perceived by states is likely to be heightened also, with the awareness of multiple potential competitors in cyberspace. Weaker states may cannot necessarily reach parity in terms of cyber power however, as Lindsay (2013: 388) points out with regard to the American developed Stuxnet virus which he estimates to have cost around $300 million, and required the technological expertise only possessed by the most advanced states.

The issue of cost also feeds into the idea that the cyber domain is geared heavily towards the development of offensive capabilities. Offence-defence balance theory postulates that if offensive military capabilities hold an advantage over defensive capabilities, the security dilemma is more intense and the risk of arms races and war greater. (Glaser and Kaufmann 1998: 47) In the cyber domain, offensive capabilities are indeed considered more cost effective and efficient to defence because of the immense challenge involved in securing

every civilian and privately owned network, and to close every vulnerability, many of which go undetected until an attack has pointed them out. (Liff 2012) Because cyber security costs almost ten times the amount of the malware that it defends against (Fahrenkrug 2012), the development of offensive capabilities is likely to be the prominent strategy. This understanding of offensive superiority is one of the reasons for the high levels of fear in the cyber domain and since offensive capabilities can inflict harm, they are more likely than defensive build-ups to kick off security dilemmas and fuel arms racing behaviour. There is little wonder then that some see the cyber domain as becoming increasingly militarised and securitised. (Hansen and Nissenbaum 2009l; Deibert 2011) This is supported by the United Nations Institute for Disarmament Research which finds that 47 governments worldwide are currently developing or have already developed, cyber warfare organisations, several of which have explicitly offensive doctrines. (UNIDIR 2013)

The heightened levels of threat perception inherent in the cyber domain are furthermore a result of the difficulty associated with tracing the origin and perpetrator of cyber-attacks. In contrast to the visible evidence of a physical attack, the nature of the internet and the anonymity it can provide creates this 'attribution' problem (Andres 2012), and makes cyber methods an attractive foreign policy choice for many states wishing to keep anonymity. A commonly used method of cyber-attack, for example, is for hackers to take remote control of computers, or botnets in other countries and launch attacks from them, making the actual location of the attacker difficult to trace. Valeriano and Maness (2015: 15) argue, however, that the attribution problem is overstated and that interstate cyber interactions tend to be tied up with pre-existing political issues between rival countries. Although there can be obvious clues as to which state was behind an attack, it nevertheless remains extremely difficult to prove, and so culprits retain plausible deniability and are less constrained from utilising cyber tactics if they believe they can act with impunity. (Liff 2012)

In treating cyberspace as a new warfare domain, many governments are reacting to their insecurities by applying the idea of deterrence, based on the Cold War nuclear strategy of Mutually Assured Destruction. In its 2011 'International Strategy for Cyberspace', the US government sets out its deterrence strategy of ensuring "that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits." (The White House 2011) Deterring cyber-attacks, according to Kugler (2009: 329), "is a matter of both assembling the physical capabilities for defending against them and of employing offensive

capabilities – cyber, diplomatic, economic, and military tools – for inflicting unacceptable damage in retaliation." The basic point is that the threat of retaliation is intended to make an enemy think twice about attacking in the first place, thereby preventing conflict. Applying the deterrence concept to cyberspace is nevertheless very problematic in practice. The attribution problem creates difficulty in knowing who to retaliate against, and the secrecy surrounding cyber capabilities means that offenders will not know the offensive capabilities of the defender to determine if an attack would be worthwhile. (Valeriano and Maness 2015: 58) Deterrence strategies, furthermore, may not bring the stability in interstate relations as hoped when considering the previous research demonstrating that meeting threats with counter threats only serves to escalate tensions between countries, and increase the likelihood of conflict. (Vasquez 1993)

There is a debate in the cyber field between those who warn of a cyber-revolution in military affairs, and those who argue that the threat is inflated, and disconnected from reality. (Lindsay and Kello 2014**)** By highlighting the serious damage cyber conflict could inflict potentially, Kello (2013) argues that the threat should be taken seriously. Yet, just because we can imagine such disastrous events, like the shutting off of the US electrical power grid, does not mean they will happen, or are even likely to happen. The empirical evidence brought to bear by those on the other side of the debate shows that there is little justification for such heightened levels of fear. Through the case of Stuxnet, considered by many to signal the beginning of the cyber war era, Lindsay (2013) shows that such technologically sophisticated weapons could only be developed only by the most advanced countries, and Valeriano and Maness (2015) show through an extensive analysis of cyber conflict that it has been a rarely used foreign policy tool, of low severity, and largely confined to world regions with pre-existing rivalries. There is therefore a significant disparity between perceptions and reality which may have negative implications. Dunn Cavelty (2012: 142) makes the constructivist argument that what states make of the cyber threat has an effect on the political reality, and that the "militarisation" of cyberspace has created an "unnecessary atmosphere of insecurity and tension in the international system based on misperceptions of the nature and level of cyber risk". The aim of this study is to measure how states have reacted to such fears.

Until now, IR scholars have yet to apply the arms race concept to the domain of cyberspace, which is evidently an international environment where threat and insecurity run high. The potential damage that cyber-attacks can inflict, the secrecy surrounding capabilities, the

asymmetric advantages provided to weaker states, the emphasis on offensive weaponry, the problem of attribution, and the developing strategies of cyber deterrence together make the domain ripe territory for a threat driven cyber arms race. Based on what we know about the cyber domain already, the cybersecurity field is ready for this further contribution to the literature, of investigating the nature and magnitude of the reaction to insecurity in terms of mutual increases in cyber warfare capabilities.

3 WHAT IS AN ARMS RACE?

Connecting arms races to the cyber domain requires that the traditional conceptualisation of the arms race be deconstructed, in order to gain a more detailed understanding of what it means in essence for states to be engaged in such behaviour. This literature review aims to define the arms race term, and discuss how they can be identified. The study can then proceed to the next step of establishing what a cyber-arms race represents, before measuring two of them through case study analysis.

The maintenance of a strong military force is a core principle in Realist IR theory which tells us that the anarchical, self-help international system creates powerful incentives for countries to seek security through military strength, and deter potential aggressors in an environment where they can never be certain of the intentions of others. (Mearsheimer 2006: 79) Deterrence theory states that countries can discourage attacks by maintaining a sufficient military capacity to retaliate, and by making clear their willingness to do so. (Cashman 1993: 219) It developed as a policy during the Cold War, as the U.S. and Soviet Union developed second strike nuclear capabilities and threatened retaliation with devastating consequences if attacked. Harnessing military capabilities is therefore seen as a fundamental tool of foreign policy in maintaining peace. Yet rather than having a stabilising influence on interstate relations, military build ups often give rise to a 'security dilemma'. A term coined by John Herz (1950), it describes the phenomenon whereby the actions one state takes to improve its security, such as a military build-up, is seen as a threatening by others, who react by taking similar steps to increase their security and so on, thus giving rise to an escalating military competition.

A "progressive, competitive peacetime increase in armaments by two states or coalitions of states resulting from conflicting purposes or mutual fears", or an arms race, as Huntington

(1958: 41) defined it, has been the subject of much case study, statistical, and formal modelling research in the field of international relations, as scholars have attempted to delineate the term, and investigate its causes and consequences. There is a wealth of statistical evidence showing that arms races contribute to the onset of war. (Wallace 1979; Sample 1997; Gibler et al 2005) Indeed, research has shown that the use of power politics strategies in general do not increase security but are likely to provoke more conflict and further deterioration in interstate relations. (Vasquez 1993) Arms races can be seen as part of the hard-to-break process of the conflict spiral whereby each step taken by a state to increase its security through confrontational policies, leads to similar reactions by the other side, and a greater chance of the situation eventually escalating to war. (Cashman and Robinson 2007: 14) This highlights the importance of developing strategies for preventing or controlling these rapid military build ups that are so detrimental to international security. The nature of the IR debate highlights the need to investigate arms racing in cyberspace, especially in light of the emphasis on offensive weaponry and deterrence strategies in the cyber domain.

Richardson (1960) conducted the first formal analysis of the action reaction arms racing dynamic using mathematical modelling techniques to represent state arming behaviour in terms of its most basic elements. In his equation the military expenditures of two countries are directly related. A country's rate of arming is a function of a rival country's military spending, and increases proportionally with it due to the threat it represents. The model also factors in, as constants, the economic cost of arming as a restraining influence on increased military spending, as well as the rates of arming that the states maintain due to ambitions or grievances, independent of the military expenditures of another state. The assumption that arms races are resource constrained is an important point to remember when applying this theory to the build-up of cheaper military technologies in cyberspace. What is notable in Richardson's equation is the potential, under certain conditions, for military spending to spiral upwards despite peaceful relations and purely defensive intent on both sides, suggesting that the reaction to another's military power is the key mechanism of the arms race process. (Hammond, 1993: 279) The naval arms race between Britain and Germany in the lead up to World War I is often seen as the epitome of the action reaction model. For example, Germany's action of increasing its numbers of battleships and cruisers led to British insecurity and a reaction by the admiralty of committing Britain to construct two new battleships for every one German ship built, and to maintain an overall 60% naval superiority. (Maurer, 1992: 288)

Although useful for getting at the heart of the action reaction dynamic, arming processes cannot be reduced down to one equation and arms races will likely display more complex characteristics in reality. Buzan and Herring (1998: 125) criticize Richardson for his assumption of "rational actors, perfect information, uncomplicated two party situations, and a set of actions and reactions that occur in a clear sequence of cause and effect." Taking the third point regarding the number of participants first, there indeed seems to be no reason why an arms race cannot involve more than two states where actors react to several threats rather than one designated rival, although there must be a minimum of two. In regard to the first couple of points, Jervis (1976) emphasises the important role psychology plays in the arms racing process and the fact that policy makers do not always act rationally, or with complete information. He notes that "once a person develops an image of the other – especially a hostile image of the other – ambiguous and even discrepant information will be assimilated to that image." (1976: 68) Rather than react to actual threats, arms racing "like other human interactions are based on subjective interpretations of the actions of others." (Hammond 1993: 47) Perceptions of threat can be just as important in driving an arms race as can possessing accurate information. This was evident in the so called 'missile gap' during the Cold War when the United States' intelligence greatly overestimated the number of ICBM's possessed by the Soviet Union, and subsequently escalated their own missile production in reaction. (Rathjens 1969) This links to the fourth point that the arms race may not follow an idealised pattern whereby one action is immediately met with a reaction and so on, which is especially true if military build ups are based on inaccurate information of the enemy's strength. It is for the aforementioned reasons that a more broad minded view should be taken of what constitutes an arms race when attempting to measure them.

Military build ups and arms races can also be motivated by a wider range of factors beyond the simple reaction to external threats. The traditional conceptualisation of the arms race emphasises mutual fear as the driving factor but, as Glaser (2000: 254) elaborates, a revisionist state may be involved in an arms race not out of insecurity but for the goal of gaining power over its rivals. Although there was evidently an action reaction mechanism operating within British-German relations, the initial German arming process can also be seen as an attempt at building a navy strong enough to challenge British supremacy and realise its overseas colonial ambitions. (Kennedy, 1980) Whether an arms racing state has offensive or defensive motivations has important implications for arms control. If states are only arms racing out of insecurity then a unilateral reduction in arms by one state could

reduce insecurity in the other and slow the military build-up. If, on the other hand, one state has aggressive intentions, then it will likely continue to arm itself regardless of the actions of the defensive state.

The externally driven, action-reaction explanation of arms races is in fact only one of two broad theoretical models. (Buzan and Herring 1998) An opposing explanation emphasises the factors internal to the state which motivates it to rapidly increase its arms which may include a military industrial complex, a dominant military research and development base, or the influence of bureaucratic politics. Scholars adapting and expanding Richardson's original model have often included many of these domestic level variables (Isard 1988), yet although other factors surely influence the nature and magnitude of the arms dynamic, it is hard to conceive of a 'race' that does not involve some element of competition between rivals. For this reason, and due to space constraints, it is the action-reaction model that is put to the test in this paper. Questions over the internal determinants of cyber build-ups nonetheless provide a path for future research.

There is also more to be said about the type of military capabilities being increased than simply military expenditures as is the focus of Richardson's model. Huntington (1958) makes the distinction for instance between quantitative and qualitative arms races. Qualitative arms races concern the competition over technological advances in weaponry, whereas a quantitative arms race is the competition over sheer numbers of military forces. Sorensen (1980) builds in the idea to his model that a state's arming levels will be influenced by the fear of its rival making a technological breakthrough. When measuring arms races using military expenditures it is important to note that a qualitative improvement in military capability will not necessarily be reflected in a state's military expenditure levels since new and improved weapons systems may be procured at cheaper costs. (Valeriano, Sample, and Kang, 2013) Hammond furthermore argues that the competition need not be in identical weapons systems, and developments such as a change in military doctrine could also signify a reaction to threat. (Hammond 1993: 86)

Gray's (1971: 40) arms race definition of "two or more parties perceiving themselves to be in an adversary relationship, who are increasing or improving their armaments at a rapid rate and structuring their respective military postures with a general attention to the past, current, and anticipated military and political behaviour of the other parties" is useful as it relaxes many of the strict assumptions of the original Richardson model, while retaining its most

important criteria. It seems that the two fundamental features of an arms race is that the states involved exhibit abnormally high rates of arming, and are engaged in this behaviour with reference to, and in competition with one another. The difficulty faced by scholars trying to identify cases of arms races is therefore twofold. First they must determine what rate of military acquisition constitutes a rapid build-up, considering that is considered normal behaviour for states to moderately increase their military budgets over time. Second, they must find evidence that mutual military build ups are not merely coincidental, but involve interaction with another state, or states.

One of the criteria set out by Hammond (1993) in his arms race case studies, is "an extraordinary and consistent increase in the level of defence effort in excess of 8 percent per annum of GNP". This seemingly arbitrary figure may well provide a reasonable threshold level for conventional arms races but may not be applicable to a study which looks into cheaper military technologies. The approach is also flawed in that an annual defence budget of 8% of GNP may not necessarily describe the 'consistent increase' that Hammond refers to. In theory it would be possible to observe an 8% figure in cases where a state's defence budget actually decreased in absolute terms from the previous year, depending on the changes in a state's GNP. Assuming that continual increases in expenditure are an important component of arms races, Hammond's method fails to capture such an idea.

Another measure frequently used in large N studies and originally developed by Diehl (1983) codes a rapid build-up if a state's annual growth in either military expenditures or personnel reaches 8% in each of three consecutive years. Unlike Hammond's approach, this measure builds in the idea, by using percentage increases, that a state's military spending is growing year on year. It does not, however, control for the possibility of variation in the average military spending patterns between states. (Valeriano, Sample, and Kang 2013) An 8% growth for example may be abnormally large for one country but not for another.

An alternative measure by Horn (1987) posits that a state is engaged in a rapid military build-up in a given year if first, the average growth rate in expenditures in the preceding ten years is greater than that of the entire time period under observation, and secondly if the average growth rate in the previous five years is greater than the ten year average. This measure builds in the idea of acceleration, whereby the rate of arming is increasing over time, and by taking into account the century average it measures the build-up with reference to the state's own 'normal' spending patterns. It offers a good indication that the military increase is

occurring at higher than normal rates, but one drawback of this method is that it relies on the availability of data over a long time period.

In terms of the evidence for competition and interaction, previous large N studies have often assumed the presence of an arms race between two rapidly arming states if they have been involved in militarised interstate disputes (Wallace 1979; Diehl 1983; Sample 1997), or if there has been a history of animosity and rivalry between them (Gibler et al 2005). One of the advantages of case study methods on the other hand is that the researcher can delve deeper into interstate relations and look for evidence of the action reaction dynamic in more detail. In investigating arms racing in cyberspace, the two fundamental aspects to look for are an abnormal build up in cyber capabilities, and evidence that this is occurring in reaction to the perceived threats posed by a rival state.

4 IDENTIFYING CYBER ARMS RACES

This research represents the first ever attempt in the field of international relations to apply arms race theory to the cyber domain. Cross national quantitative assessments of cyber capabilities have been made in the past like the 2011 Booz Allen Hamilton 'Cyber Power' index, and the 'Global Cyber Security Index', published in 2015 by the International Telecommunications Union. (Booz Allen Hamilton 2011; ITU April 2014) However, these past efforts have not taken an international security perspective, and rely on broad societal based indicators such as legal frameworks, or economic and social contexts, rather than focus on the direct resources that national governments channel into preparing for cyber conflict. These previous attempts, moreover, offer only a snapshot of capabilities, useful for comparing countries at a particular point in time, but not for tracking changes in cyber strength over time which is critical for investigating an arms racing process.

Clarke and Knake (2010) have focused more on the cyber conflict dimension, and attempt to compare some of the key actors in terms of cyber power which they break down into cyber offense, cyber defence, and cyber dependence. The latter refers to how 'plugged in' and therefore how vulnerable to attack a state is. For instance, Estonia receives a low dependence score because much of its infrastructure relies on internet networks, whereas North Korea, whose government has strict controls over internet usage, gets a high dependence score. However, again it is the process of developing capabilities that is of more interest here, rather

than the current balance of cyber power. It is the escalating arms race process, and the associated conflict spiral, that is considered a contributing factor in interstate war. Empirically confirming the presence of a cyber-arms racing dynamic is therefore a much needed task.

Since cyber-arms races are as yet an untested phenomenon, this study can be regarded as a "plausibility probe" (Eckstein 1975) to help decide whether the concept shows promise as a theory of state behaviour in the cyber domain that is applicable to a wider population of cases. The next section presents the case study analyses of two rival state dyads, the United States and Iran, and North Korea and South Korea. These four countries are among the major players in the cyber conflict arena and are each within the top ten countries in terms of most cyber incident involvement. (Valeriano and Maness 2015) Given the level attention received by these countries in the cyber conflict sphere, they are of great interest to policy makers and academic alike. The choice is also greatly limited due to the availability of cyber capability data, which is often kept secret by states.

The "structured and focused" case study design (George and Bennett 2005) is adopted here to identify the presence of cyber arms racing behaviour. This approach structures the analysis by asking similar questions of each case, and focuses on the key aspects of the dyadic relationship that will engage the research question. From the arms racing literature review, some fundamental criteria for a cyber-arms race can be identified. At a minimum, it should involve a mutual build-up of arms at a rapid rate, in response to external threats, whether real or perceived, and involve an element of interaction, or competition, between the countries involved. Since states often react to perceived threats, a perfect action reaction pattern is not necessarily expected. Cyber-attacks are also considered an action that may encourage reaction since they provide its rival with a clear indication of its cyber capabilities.

The questions asked of each dyad are as follows:

1. Are the states engaged in a rapid build-up of cyber capabilities?

2. Do the states have external cyber threats?

3. Are the states in interacting with one another?

To answer the first question, time series data will be presented graphically for each state to track the changes to its cyber capabilities using the available data. The approach here is inspired by the Correlates of War Project (Singer 1972), which partly uses the variables military expenditure and military personnel to construct its National Material Capabilities Index. These are also the variables used in previous arms race studies. Applying this to cyberspace, the data that is mainly sought here is government spending on cybersecurity, and on the number of hackers or cyber security experts employed by governments. This should offer the most direct indication of the effort states are putting in to develop their cyber strength. Ideally, to be consistent, both metrics should be used across all countries, and a clear distinction between what is offensive and what is defensive should be made, yet this is not always possible due to data limitations. In some cases, moreover, neither spending nor personnel data could be obtained so other indicators had to be relied on. A mutual build up is a necessary condition for an arms race and this should be observed at a rate which signifies behaviour that is out of the ordinary. If it is not greater than normal we would be witnessing a 'walk' as opposed to a 'race', which would be of less concern. To determine whether the cyber build-ups are out of line of normal state behaviour, various comparison techniques will be used to place them in context.

As the subject of study is the externally, as opposed to internally, driven arms race, the second question is in place to show that the states building up their cyber arms perceive some degree of threat from cyber-attacks, and/or have actual experience of cyber threats from other states. If not, then it would be difficult to see the cyber build ups as being a response to external threat. Addressing the second question will involve reviewing the cyber incidents involving these states generally, in order to establish that a justification for a cyber-build-up is present. The cyber incidents data set (Valeriano and Maness 2015) is used for this purpose, which can also help to give an idea of motivations, whether offensive or defensive.

The mere correlation between cyber build-ups and external threats cannot show that the increase in capabilities is a reaction to the external threat posed by a particular rival however, and without some evidence of competition and interaction it is difficult to call it a race. The third question therefore is asked in order to investigate whether each state regards the other as the reason for its build-up. A more qualitative approach is taken here to gain more detail into the potential action-reaction dynamic between the two rival states. It is not expected that there will be a very clear action reaction pattern however, but just a general indication that

states are developing their capabilities with the perceived behaviour or intentions of their rival in mind. Arms races, after all, are often driven by perceptions rather than concrete knowledge. If these three criteria are met, it would suggest that there is an arms racing dynamic in cyberspace. Analysing the interstate interactions will also help to determine to what degree the cyber build-ups are driven by the perception of threat from the rival, as opposed to actual cyber threats, thus representing an overreaction.

5 ARMS RACING IN CYBERSPACE

5.1 The United States and Iran

Tensions have been high between the United States and Iran since the 1979 Islamic revolution which broke the close Cold War ties between the two countries, and reconfigured Iran's foreign policy under the theocratic rule of the Ayatollah Khomeini who condemned the U.S. as the 'Great Satan' for its interventions in the region. After 9/11 Iran was one of the group of countries labelled by George W. Bush as the 'axis of evil' for its support of terrorist organisations in the Middle East. Relations have continued to deteriorate over Iran's nuclear development program, which has threatened America's close ally Israel, and has been met with a series of harsh economic sanctions. With the election of the more moderate President Rouhani in 2013 however, cooperation between the two has increased. This section will examine the cyber relations between the U.S. and Iran, and seek evidence of a cyber-arms race.

5.1.1 U.S. Cyber Build-up

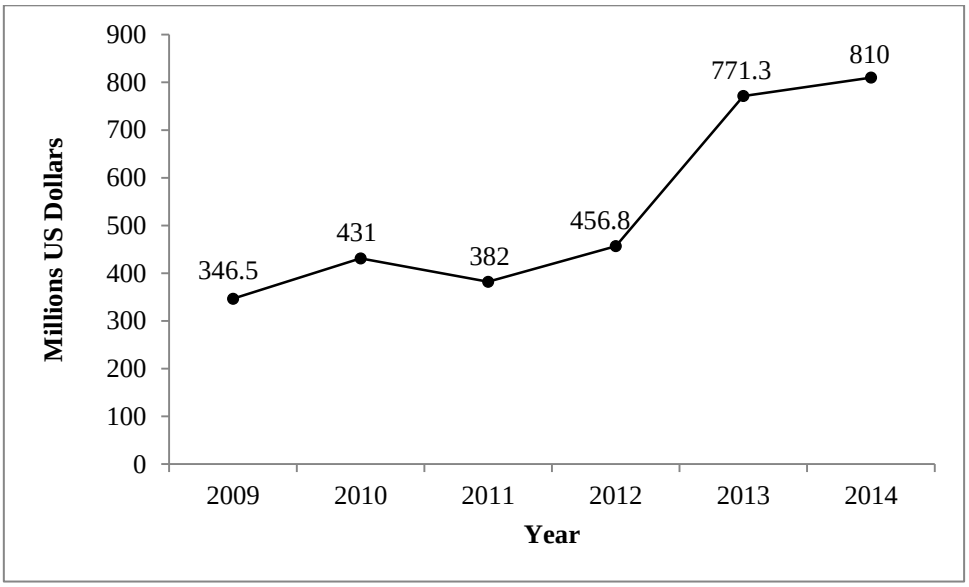
The United States is investing more in cybersecurity. A 2013 news report noted that the U.S. government was requesting "$9.3 billion through 2018 for information-assurance systems aimed at blocking hackers and preventing disruptions of information on Pentagon computers, and $8.9 billion for cyber-operations, which include both defensive and offensive capabilities." (Capaccio 2013) Uncovering time series data on cyber capabilities is generally difficult but out of all the countries covered in these case studies, the United States, as a democracy, is the most open about its efforts to secure cyberspace. In fact, the availability of

data on two government departments, the Department of Homeland Security, and the Department of Defence, allows a rough distinction to be made between the changing defensive and offensive cyber capabilities of the United States.

The Department of Homeland Security (DHS) was originally set up in response to 9/11 to defend the nation against terrorism, but has since taken on a broader role of protecting the civilian sphere against a range of threats including safeguarding the nation's cyber infrastructure. One of the DHS's five stated missions is to "safeguard and secure cyberspace", by aiming to "analyze and reduce cyber threats and vulnerabilities", "distribute threat warnings", and "coordinate the response to cyber incidents to ensure that computers, networks, and cyber systems remain safe". (DHS 6 August 2015) Although a state's cyber defensive capabilities cannot be reduced down to one department, this provides a good source for analysing the efforts of the U.S. government to build-up cyber defences. Budget figures are available for one particular organisation within the DHS, the 'National Cyber Security Division' (NCSD), which operates under the 'Directorate for National Protection and Programs', and is home to America's Computer Emergency Response Team (CERT) team.

Figure 1 below illustrates the changing NCSD budget converted to constant 2014 US Dollars. Although the NCSD was formed in 2003, the budget data is only available between 2009 and 2014, and over this period there has indeed been a definite increase in U.S. cyber security spending.

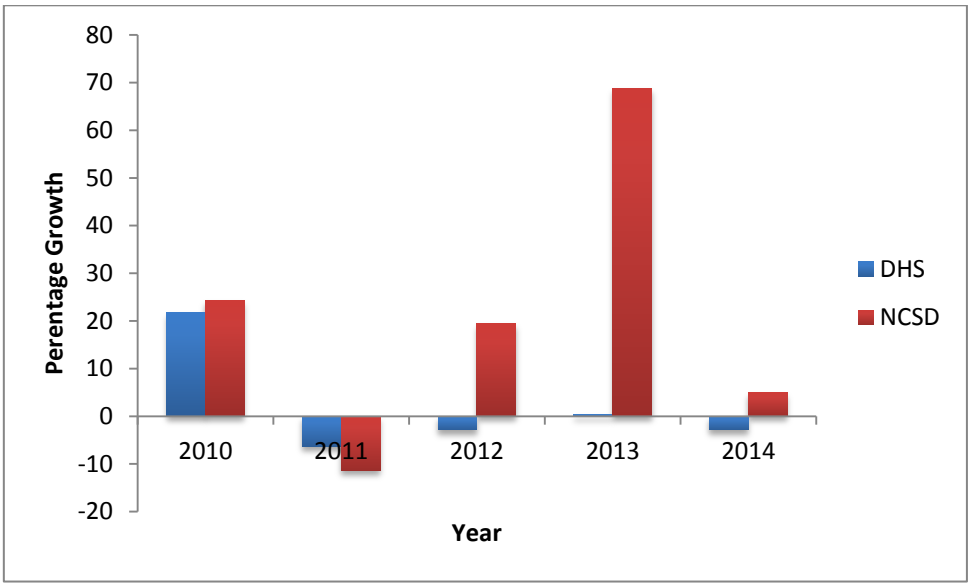
Figure 1: United States - National Cyber Security Division budget (2009-2014)



(Congressional Research Service)

The government funding received by the cyber division increased overall from $346.5 million in 2009, to $810 million in 2014, representing a growth of 134%. Despite a slight decrease in 2011 the budget has increased in every year with a particularly large jump in 2013. To put these increases in context and determine if it represents an abnormal increase, figure 2 compares the annual percentage growth in the NCSD budget to that of the DHS as a whole.

Figure 2: United States - annual growth in DHS and NCSD budgets (2010-2014)

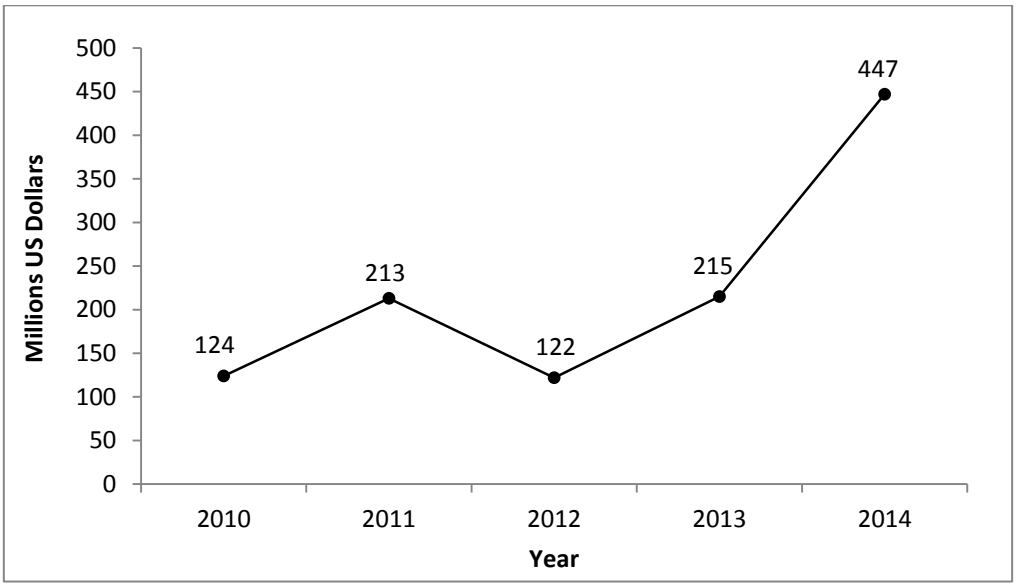


(Congressional Research Service)

On average, the budget of the NCSD grew at higher rates than its parent organisation. The biggest difference came in 2013 when, despite an increase of just 0.4% in the Homeland Security budget, the National Cybersecurity Division's budget grew by 69% from the previous year. This would suggest that cybersecurity spending has been out of line from normal budgetary increases and represents a significant effort to improve cyber defences.

The build-up of offensive cyber capabilities is a more secretive and controversial development but budget figures are available on the US Cyber Command unit which reached full operational capacity in 2010 at a cost of $7.1 Billion. (Sternstein 2015) U.S. Cyber Command falls under U.S. Strategic Command, which is one of the 9 military command structures of the Department of Defence. It is based at Fort Meade, Maryland, and is headed by Admiral Michael S. Rogers. With its stated mission of carrying out "full spectrum military cyberspace operations [and to] ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (U.S. Stratcom March 2015), the creation of Cyber Command can be seen as a move to militarise the cyber domain and develop offensive cyber warfare capabilities. Figure 3 shows the changing budget allocation for Cyber Command from 2010 to 2014 in constant dollars.

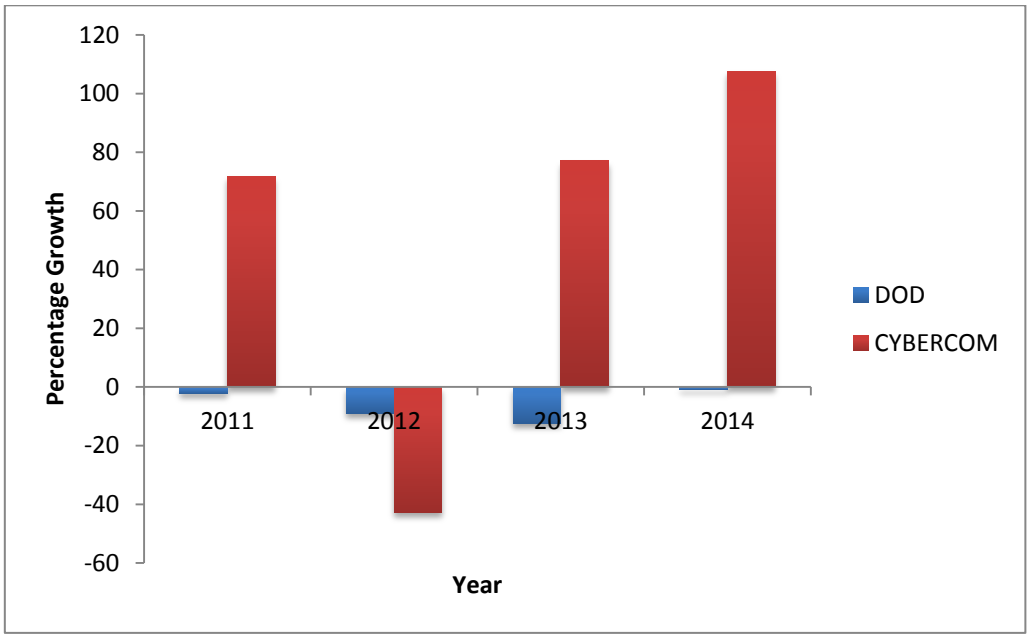
Figure 3: United States - Cyber Command budget (2010 – 2014)



(Fung 2014)

The US government has evidently been putting increasing resources into its cyber offence as well as cyber defence with an increase in budget from $124 to $447 million within the first four years of its inception. 2012 marked the point after which spending has been rising continuously. To give context to this spending pattern, the annual percentage growth in spending for cyber command is compared below in figure 4 with that of the Department of Defence, i.e the overall military budget of the United States.

Figure 4: United States - annual growth in DOD and Cyber Command budgets (2011-2014)



(Fung 2014; SIPRI 2015)

Despite decreases in each year to the DOD budget, Cyber Command's budget has tended to grow, and more than doubled in 2014 from the previous year. This data suggests that there has been a build-up in offensive capabilities against the backdrop of declining total military spending.

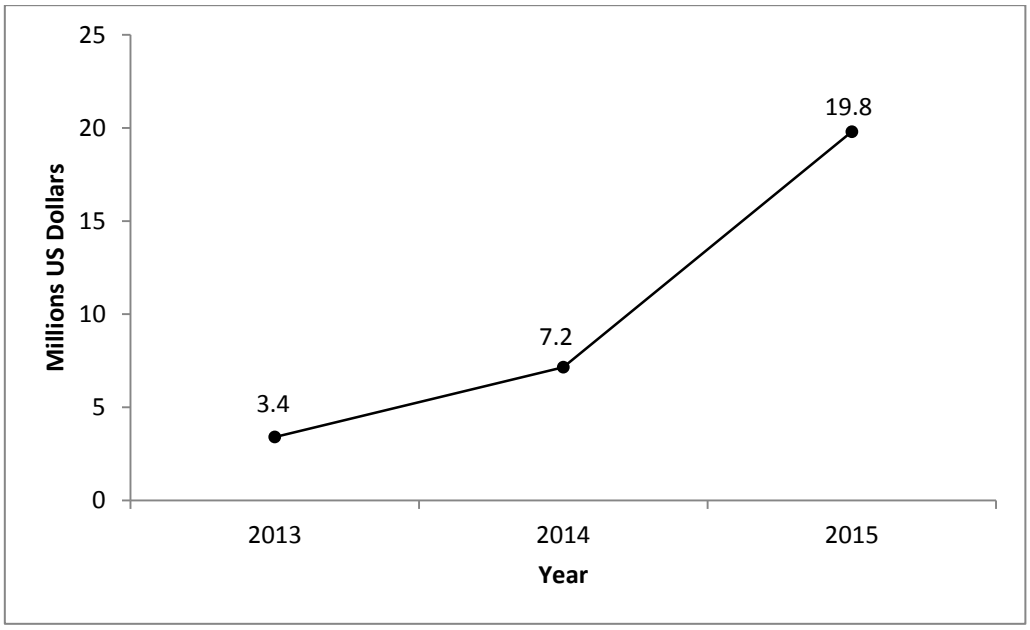
The numbers of cyber specialists, or 'troops', hired by the cyber warfare unit offers another quantifiable indicator of an offensive cyber build-up. From 937 in 2012 (IISS 2013: 54), the force size increased to 1,800 in 2014, and is expected to grow to around 6000 by 2016 (Nakashima 2014). If so, this would represent a greater than six fold increase in staff within 4 years. Therefore, the United States has evidently been engaged in a rapid build-up in terms of defensive and offensive cyber capabilities.

5.1.2 Iran Cyber Build-up

Like the US, Iran has also been building up its cyber capabilities. The Iranian Revolutionary Guard Corps has reportedly trained a cyber-army of 120,000 consisting of "university teachers, students, and clerics", which it claims to be the second largest in the world. (UNIDIR 2013: 32) In 2012 the Supreme Leader Ayatollah Khamenei established a new cyber unit titled the 'Supreme Council of Cyberspace' (SCC), with ultimate control over all

internet and cyber-related policies in Iran. The SCC's 2014 budget was $40 million, which ir receives from Iran's ICT budget. (Small Media 2014: 7) Since President Rouhani came to power, data has been released on Iran's cyber security spending which is illustrated in figure 6 below.

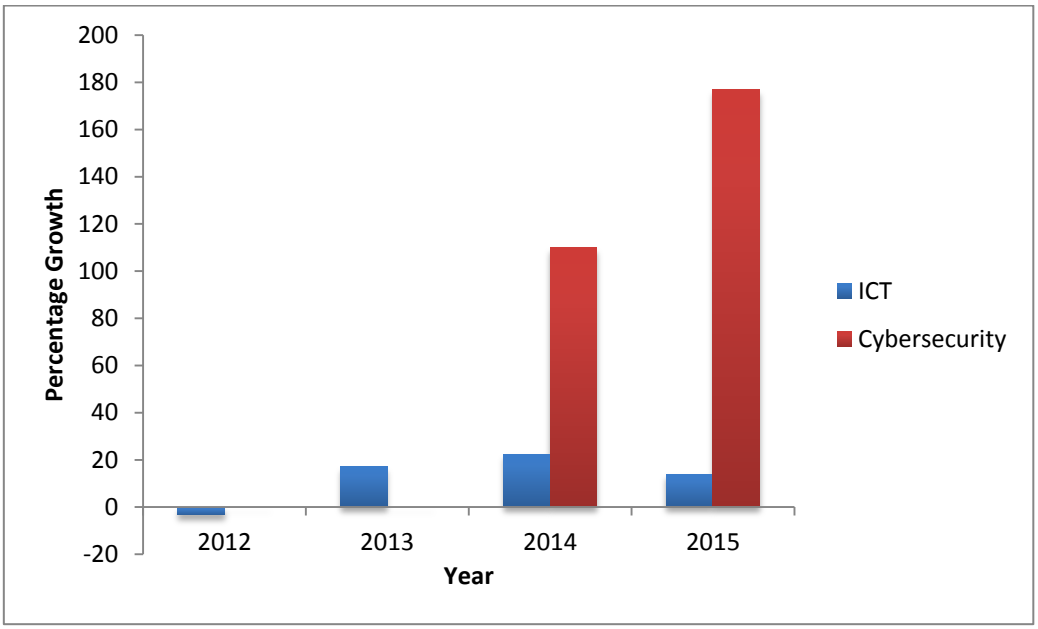
Figure 5: Iran - Cybersecurity budget (2013-2015)



(Small Media February 2015)

The cyber security budget increased from $3.4 million in 2013 to $19.8 million in 2015. It is unknown what exactly this money goes to, and there is a lack of similar data on Iran's build-up in offensive capabilities, but it clearly shows that Iran has at least been increasing its cybersecurity spending. To put this increase in context, Figure 4 compares the cybersecurity budget's annual percentage growth in 2014 and 2015 with that of Iran's ICT budget, using the available data.

Figure 6: Iran - annual growth in ICT and Cybersecurity budgets (2012-2015)



(Small Media January 2015; February 2015)

The ICT budget has also been increasing year on year since 2013 but not at such great a scale as the cyber security budget. This suggests significant efforts to build-up cyber defensive capabilities.

5.1.3 External Threats

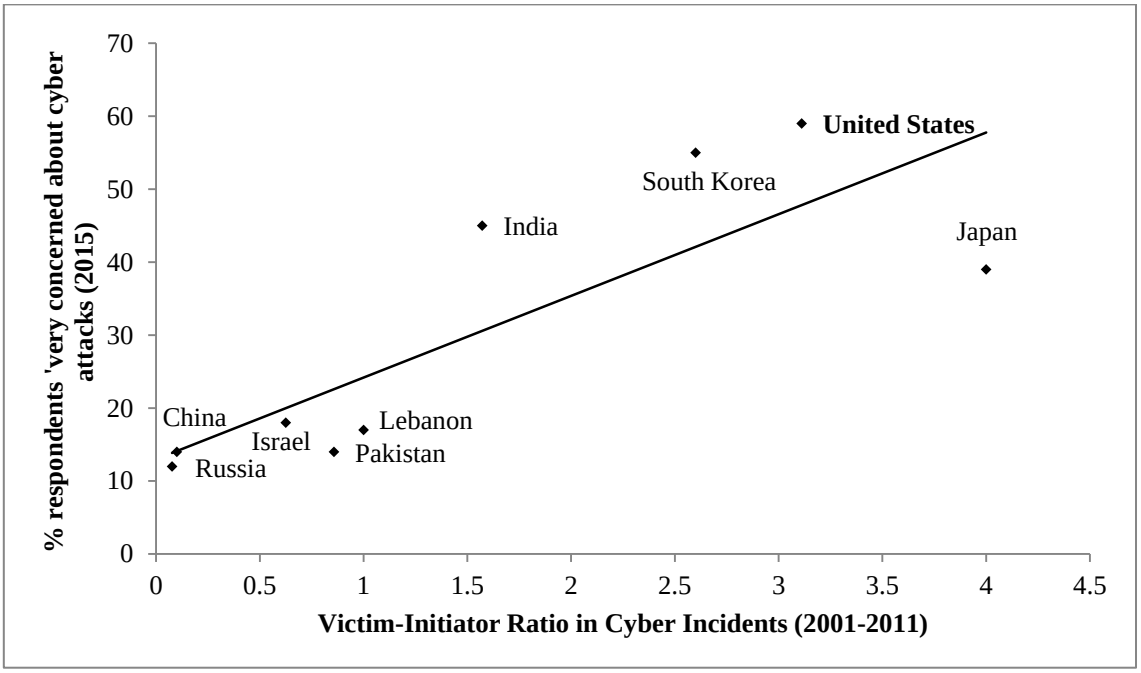
The United States' government clearly regards cyber conflict as a major threat. Between 2013 and 2015, cyber was consistently named as the top national security threat by the Director of National Intelligence James Clapper. (Taylor 2015) This threat perception is also reflected in public opinion. In a 2015 global threat survey conducted by Pew, the United States was found to have the highest perception of threat amongst the 40 countries surveyed, with 59% of the American public feeling 'very concerned', and 28% 'somewhat concerned' about the risk of cyberattacks on governments, banks or corporations. (Carle 2015)

It is also true that the United States has usually been a victim in interstate cyber interactions. Among rival states between 2001 and 2011 the United States has been involved in 37 cyber incidents, and has been the victim of nine of these attacks. (Valeriano and Maness, 2015: 88) China is perhaps America's biggest source of threat in cyberspace as it has for years been behind numerous cyber espionage attempts to steal sensitive military information, which including the theft of the F-35 joint strike fighter blueprints in 2009.

Iran too has experienced a number of real cyber threats. Out of a total of twelve cyber-incidents between 2001 and 2011, it has been the victim state in seven (58%) of them. (2015: 88) All of these attacks have come from the United States and Israel as they have sought to undermine Iran's nuclear development program.

To highlight how past experience of cyber-attacks may shape and the level of threat perception, the victim-initiator ratio and the percentage of respondents 'very concerned' about cyber-attacks is plotted against one another in figure 7 below.

Figure 7: Cyber incidents and threat perception



(Valeriano and Maness 2015; Carle 2015)

Although the sample size is too small to gain a measure of the statistical significance in this relationship, there appears to be a correlation between being more often the victim and a heightened perception of threat. This may suggest that fear of cyber-attacks have some basis in reality. Although there was no survey data on Iran, based on the data for other countries, it would seem likely that it would follow the same trend.

5.1.4 Dyadic Interaction

The United States and Iran have had a history of cyber conflict with one another, as shown in Table 1. Although America has tended to be a cyber-victim in general, its experience of actual cyber threats from Iran has been very limited. Iran has in fact had more to fear from the United States.

Table 1: Cyber interactions - United States and Iran (2001-2011)

Incidents	US Initiated	Iran Initiated
7	6	1

(Valeriano and Maness 2015)

In the U.S.-Iran dyad, out of a total of 7 incidents between 2001 and 2011, the United States has initiated all but one of them. The only attack by Iran against the U.S. was the 2009 Twitter hack which was no more than a simple website defacement; one of the most trivial of cyber-attack methods. Based on actual cyber threats therefore, up to 2011 at least, the U.S. has had little justification for fearing Iran.

Initially, Iran did not factor in much to America's cyber-strategy. In fact, despite the founding of Cyber Command in 2010, the U.S. government often appears vague on whom, or what it is developing its capabilities in response to. In a 2010 House Committee discussing the role of the newly created Cyber Command unit, its commander General Keith Alexander was questioned on the nature of the cyber threat facing the United States. On the topic of the international actors the U.S. must prepare itself against, Gen. Alexander stated that:

> *"I think there are a number of countries out there that are near peers to us in cyberspace, and you can just go around the world and pick—most of the modern nations have capabilities that I think many could argue are near to us and in some areas may exceed our capabilities."* (House of Representatives 2010: 13)

Uncertainty and vagueness about the cyber threat is evident, and there was clearly a lack of reference to explicit competition with any one designated rival like Iran. The U.S. was instead reacting to the perceived capabilities of other states. With regards to what he considered the greatest threat, Gen. Alexander replied that:

> *"What concerns me the most is destructive attacks that are coming. And we are concerned that those are the next things that we will see."* (2010: 7)

Rather than respond to actual threats that have occurred, the U.S. military's development of cyber warfare capabilities was based on imagined and perceived future threats, taking what Valeriano and Maness (2015: 7) call a "worst case scenario" policy approach.

A competitive relationship with Iran was sparked in June 2010 however with the discovery of the highly sophisticated Stuxnet computer virus that had been used to target one of Iran's major nuclear enrichment plants at Natanz. It is widely believed to have been developed by the United States, in collaboration with Israel, as a means to curb Iran's nuclear ambitions. According to Sanger (2012b: 205), the attack destroyed 984, or a fifth, of the facilities' centrifuges. Being the first attack of its kind to cause physical damage, it has been regarded as "a paradigm shift", and "a new class and dimension of warfare." (Kerr et al 2010: 6)

Iran's immediate response to Stuxnet was muted, perhaps not wanting to show weakness, yet it soon began developing its cyber capabilities and in March 2012 the Ayatollah Khamenei announced the creation of a new cyber command unit, the Supreme Council of Cyberspace, with full control over internet related policies. Operating under the SCC is the National Center for Cyberspace (NCC) which is tasked with protecting the country from cyber-attacks, and to help develop a national internet that will reduce Iran's internet dependency. (Small Media 2014: 4) Retaliation for Stuxnet, and a physical display of Iran's developing offensive capabilities in cyber warfare, came in the form of the 'Shamoon' cyber attack, launched by Iran in August 2012 against the Saudi Aramco oil company. Valeriano and Maness (2015: 157) judge the attack, which deleted data on, and removed the re-boot program on around

30,000 computers, to be an incidence of a "weak state attempting to damage a rival and harm, by proxy, its large state sponsor and greatest consumer of oil".

After Stuxnet, it became clear that the U.S. feared Iran was learning from the attack, with General William Shelton, the head of the U.S. Air Force Space Command, reporting to the media in January 2013 that "it's clear that the Natanz situation generated a reaction by them". He called for increased cyber-security spending, and announced plans to increase the number of personnel in his unit by 1000. (Shalal-Esa 2013) That the U.S. was developing a growing perception of threat from Iran is backed up by an Edward Snowdon-leaked NSA document from April 2013 which suggested that Iran had learned from cyber-attacks launched against it, and had been behind several waves of DDoS attacks on U.S. financial institutions, on top of the Saudi Aramco attack which was referred to as "the first such attack the NSA has observed from this adversary". (Greenwald 2015)

From 2012, The United States undoubtedly began to see Iran as a source of cyber threat. Speaking before the Senate Intelligence Committee, Director of National Intelligence James Clapper warned that:

> *"Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity."* (Shachtman 2012)

Similarly, in a committee on Homeland Security on April 26th, the issue was raised that Iran had invested over $1 Billion in expanding its cyber capabilities and had been carrying out cyber-attacks on media organisations to test its cyber strength. (House of Representatives 2012) Moreover, the head of the U.S. Air Force Space Command, reported to the media in 2013 that Iran's developing cyber capabilities will make it ''a force to be reckoned with". (Shalal-Esa 2013) This is a clear example of a state perceiving a threat from the developing capabilities of another, as the action-reaction model predicts. It is unsurprising therefore that the data presented in this paper on U.S. cyber-warfare spending, shows the largest increases after 2012, the year in which American officials apparently became more fearful of the threat from Iran. Both countries have therefore been shown here to have developed their capabilities in reaction to one another, and the criteria for an arms race appear to have been met in this case.

5.2. North Korea and South Korea

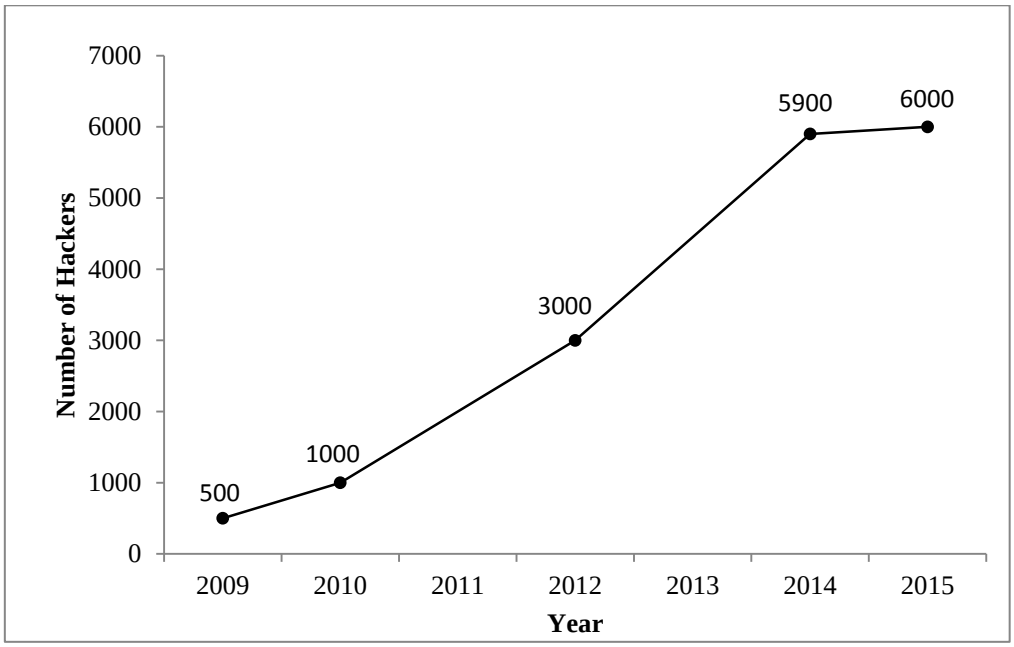
North and South Korea have been bitter rivals since they became independent states in 1948, after the Soviet Union and the United States captured the Korean peninsula from Japan at the end of World War II. They fought the Korean War against one another from 1950 to 1953, and their disputes and mutual animosity has endured into the 21st century, with neither state recognising the legitimacy of one another's governments. Tensions continue due to the South's close military alliance with the United States which imposes sanctions on North Korea in response to its nuclear program. This section will investigate whether this dyad has also been engaged in a cyber-arms race.

5.2.1 North Korea Cyber Build-up

The one-party communist state of North Korea is perhaps the most authoritarian and secretive country in the world so finding reliable data on its cyber capabilities is a particularly challenging endeavour. North Korea has been suspected of building up its cyber-attack capabilities, and is known to have a number of cyber warfare units that operate under the control of its armed forces. According to a report by security company Hewlett Packard, within the General Staff Department the Reconnaissance General Bureau runs two main cyber organisations, Unit 91, and Unit 121, both understood to be the source of offensive operations. There are in fact a total of 6 known cyber units, each with varying cyber warfare roles, including Unit 35 which is believed to be involved in training hackers. (Hewlett Packard 2014: 26)

Professor Huang Kwang, a defector from the North to the South estimates that between 10 to 20% of North Korea's military budget is spent on 'online operations' (Lee and Kwek 2015), yet despite this speculation, and the information on its cyber warfare units, there is very little quantitative data on the change in North Korea's cyber capabilities over time. Nonetheless, a number of defectors and South Korean news organisations have made various claims over the years about the size of North Korea's army of cyber hackers. In figure 5, these estimates are pieced together to highlight the growth of North Korea's offensive capabilities.

Figure 8: North Korea - cyber 'army'



(Hewlett Packard 2014; Mulrine 2015; BBC 2015)

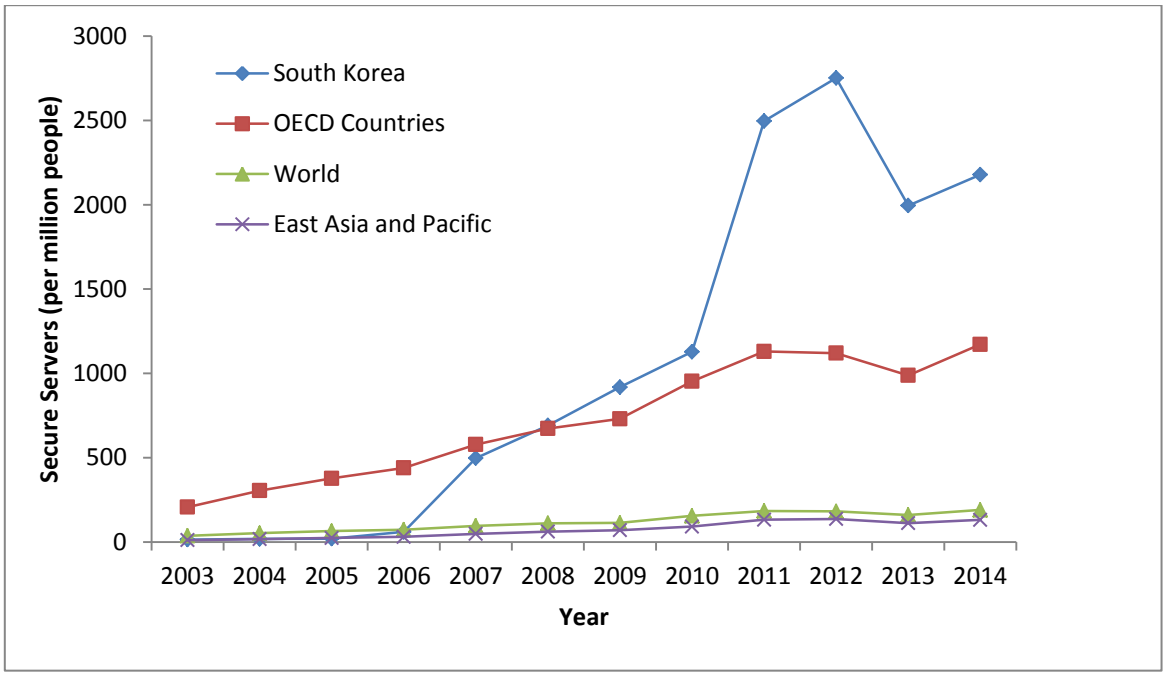
If accurate, the data would suggest the number of North Korean hackers has grown by 1100% since 2009. There is reason to believe such estimates due to the inside knowledge of the defectors who provided the data, yet since they are South Korean sources, the figures may be biased and deliberately inflated in order to raise awareness of their security concerns, and paint their Northern rivals as a threat.

5.2.2 South Korea Cyber Build-up

South Korea has also been developing its cyber capabilities and in 2010 a cyber-warfare unit was created, taking on an offensive as well as defensive role, and staffed by approximately 200 cyber security personnel. (UNIDIR 2013: 41) The time series data used here to measure South Korea's cyber build-up is the number of secure servers per million of the population. Secure Servers are servers that use encryption technology in internet transactions (World Bank/Netcraft 2015), thus providing a measure of a country's cyber defences. It should be noted however that secure servers do not represent weapons and therefore a growth in them is not a development that would be feared or reacted against. It is the only relevant time series

data available for the country, but nevertheless measures the reaction from South Korea. The change in secure servers from 2003 to 2014 is plotted in figure 6 below, and is compared with other groups of countries to put South Korea's cyber build-up into context.

Figure 9: South Korea – secure servers



(Source: World Bank/Netcraft)

Figure 6 shows there has been a remarkable increase in South Korea's cyber defences. Secure servers grew from 14 per million people in 2003 to 2178 per million people in 2014. There was a particularly accelerated period of growth from 2010 when secure servers more than doubled in the space of a year. South Korea's improvements to its cyber defences have evidently been on a much greater scale than the world average, as well as among its neighbours in the East Asia and Pacific region. South Korea has furthermore increased its cybersecurity at a higher rate than the other economically developed, democratic, and free market oriented OECD countries. Such a deviation from the norm, suggests that South Korea has put deliberate effort into strengthening its nationwide cyber defences.

5.2.3 External Threats

South Korea is comparably much more vulnerable to cyber-attacks than North Korea, with 41 million internet users and an internet penetration rate of 84% of the population, and like the United States, South Korea is very concerned about the threat of cyber-attacks. In the Pew global threat survey, South Korea came second, after the United States, in terms of most heightened cyber threat perception. 55% of the population were 'very concerned', and 33% 'somewhat concerned', about the threat of cyber-attacks on governments, banks, or corporations. (Carle 2015) Out of the 18 cyber incidents it has been involved in between 2001 and 2011, it has been the victim in 13 (72%) of them, which have involved either North Korea or Japan.

In contrast, North Korea has been much more offense oriented in the cyber domain, and has fewer cyber threats. It has been involved in a total of 15 cyber incidents and has initiated 14 (93%) of them. Its targets in cyberspace include South Korea, the United States, and Japan. Pyongyang keeps strict controls over internet access, with the vast majority of the population denied its use. North Korea's main advantage in cyberspace comes from this lack of cyber dependence, as its critical infrastructure is less controlled by internet networks. North Korea considers cyber warfare an opportunity to challenge its rivals on an equal cyber footing despite its asymmetrical conventional capabilities. North Korea's military spending is just $825 million compared to South Korea's $36.6 billion (SIPIR 2015), and considering the South's military alliance with the USA, North Korea is at a significant disadvantage when engaging with South militarily.

5.2.4 Dyadic Interaction

There have been several known cases of cyber conflict between North and South Korea, and Table 2 shows a total of 11 incidents from 2001 to 2011, with North Korea initiating all but one of them.

Table 2: Cyber Interactions – North Korea and South Korea

Incidents	North Korea Initiated	South Korea Initiated
11	10	1

(Valeriano and Maness 2015)

North Korea is most definitely the more offensive state in the dyadic relationship, reflected in the fact that its main hacking centre, Unit 121, was established in 1998, several years earlier than the similar developments of other countries. (Carroll 2007) According to the data set, these 10 cyber incidents initiated by the North against the South all took place in the short space of 3 years between 2008 and 2011, giving South Korea the motivation to increase its cyber capabilities.

The cyber relations between these countries have mainly followed the pattern whereby attacks from the North are followed by reaction in the South. For example, in 2009, a DDoS attack suspected to be from North Korea, hit the networks of several South Korean government departments and banks including that of the Defense Ministry, the National Assembly, and the Korean Exchange bank. (Weaver 2009) In response, South Korea created a Cyber Command unit in 2010, headed by an army general, with the defence ministry explicitly referencing the threat from North Korea as the justification for the development. (Yonhap News Agency 8 October 2010)

South Korea was again targeted by the North in 2011, in an attack which brought down 26 government, military, and banking websites. (BBC News 4 March 2011) In the same year South Korea launched its cyber security strategy, now treating the cyber domain as part of the military sphere in the same way as land, sea, or air. Also included in the strategy was a requirement that public and private sectors take measures to encrypt and back up data. (Schweber 2011) The huge increase in South Korean secure servers from 2010 to 2011, as shown in figure 6, is perhaps directly linked to this policy. In August 2012, moreover, the South called for the number of cyber security personnel in its cyber warfare unit to be

increased to 1000 from the 200 initially operating there, to help cope with the North Korean threat. (Korea JoonGang Daily 30 August 2012)

Another attack in 2013, not covered by the incidents dataset, shut down the South Korean banking system and several television stations. This attack was somewhat more sophisticated than before as it used malware, as opposed to the DDoS methods which simply overloads a system with requests. (Sang-Hun 2013) This hinted at the growing offensive capabilities of North Korea. In reaction, South Korea announced another build up in manpower revealing its intention to train an extra 5000 cyber troops to defend against North Korean cyber-attacks. (Hewlett Packard 2014: 4) If this was indeed a reaction to the developing capabilities of the North, it gives reason to believe in the accuracy of the data on North Korea's cyber army, and shows the South Koreans trying to compete with the similar developments of the North.

North Korea is by far the more aggressive state in the dyad, yet the relationship was not completely one sided and the North had blamed the South for an attack on its own websites only days before the 2013 attack on South Korea. North Korean State Television had referred to the "intensive and persistent virus attacks [that] are being made every day on internet servers operated by the DPRK" (Nam 2013), and warning that they "will never remain a passive onlooker to the enemies' cyberattacks". (Sang-Hun 2013)

5.3 Discussion

The analysis suggests that both dyads have been engaged in cyber-arms races. The U.S.-Iran case provides a good example of cyber-arms competition being driven by mutual insecurity. From 2012, the United States evidently started to put increasing resources into its defensive and offensive cyber capabilities as shown in the NCSD and Cyber Command budgets, as well as the increase in cyber personnel numbers. The limited data on Iran also shows extraordinary increases to its cyber security budget from at least 2013. This evidence, as well as the creation of the Iranian cyber-warfare command structure in 2010, shows a mutual build-up of cyber capabilities between these countries. Equally important, is the strong evidence of competition in their relationship. America's plan to undermine Iran's nuclear development program with the Stuxnet attack appears to have kicked off the security dilemma and action-reaction pattern. The attack was met with a response from Iran in terms of increasing capabilities and the use of cyber-attack methods, which then created a heightened perception

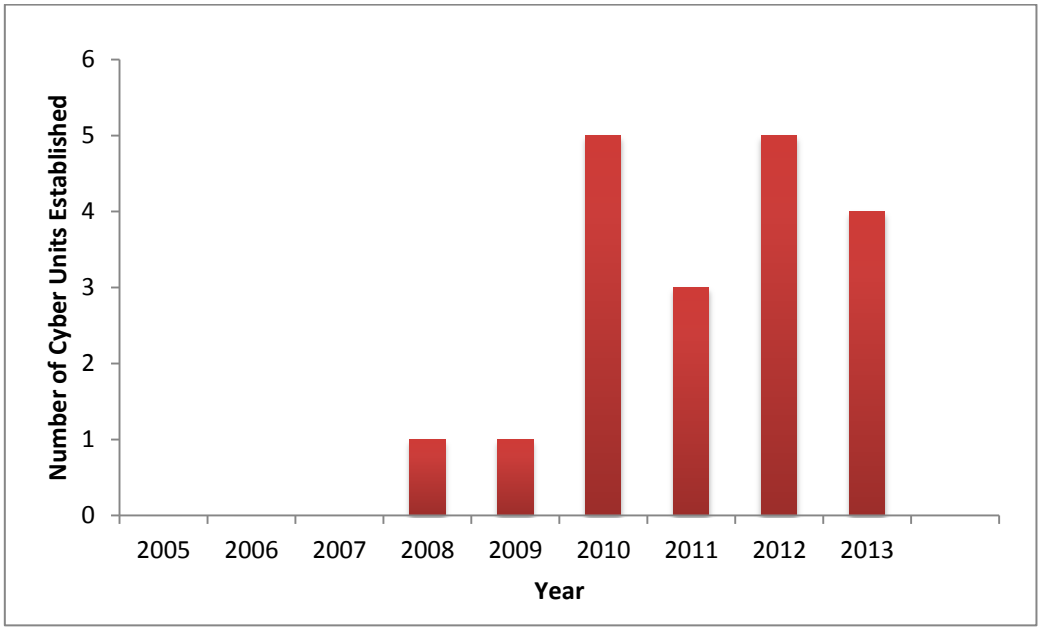
of threat in the United States over Iran's growing cyber capabilities. The fact that these U.S. security concerns began around the same time as the rapid increases to its cyber security spending suggests they were linked and that a U.S.-Iran cyber arms race was initiated around 2012. Perceptions of threat are a major driving factor of this arms race, especially on the U.S. side which experienced very few cyber-attacks from Iran and instead reacted to the perceived increase in Iran's offensive capabilities. More recently, however, these countries have come to agreement over the nuclear issue, yet whether this has slowed the cyber competition is not clear with the available data. If uncertainty and defensive motivations are indeed at the heart of this cyber arms race then there is hope for an end to its escalation, if trust and cooperation can be achieved. Although the arms race was driven by mutual threat, it also began as a result of American aggression, at a time when Iran's cyber-aggression was very limited. The case study highlights the negative impact that the use of offensive cyber tactics can have in escalating competition and further cyber conflict.

The evidence would suggest that there has also been a cyber-arms race between North and South Korea. Reports on the size of North Korea's hacking army show that the country has been continually increasing its cyber offensive capabilities since 2009, and by using secure server data, it has been shown that South Korea has been putting huge effort into improving its cyber defences in comparison with other countries. Interaction is also evident between the two states, in that continual attacks from North Korea were met with a progressive development in South Korean cyber-capabilities, including the creation of a cyber-warfare unit and the build-up of personnel to match that of the North. However, unlike the U.S.-Iran dyad, the insecurity that characterises this arms race has been very one sided. One the one hand, South Korea is certainly building capabilities in response to the North Korean threat, considering the continual attacks, and reference to North Korean capabilities and actions. North Korea on the other hand is motivated more by aggressive intent rather than fear, given the fact that the North initiated all but one of the cyber incidents between it and South Korea between 2001 and 2011. Although there is some indication that North Korea perceived a threat from South Korea, the North is mostly motivated by the desire to cause a nuisance to its long-term rival. This is an example of an arms race where one state has mainly defensive motives, whereas the other has offensive motives, and this creates a difficulty in finding a solution to the escalating competition. North Korea is unlikely to give up on its offensive ambitions regardless of levels of threat, which leaves South Korea little choice but to continue to build-up its capabilities in reaction.

6 IMPROVING CYBERSECURITY

The build-up of cyber warfare capabilities is not something confined to a few country cases and many countries are engaged in the militarisation of cyberspace, which according to Deibert (2011: 2) "refers to the growing pressures on governments and their armed forces to develop the capacity to fight and win wars in this [cyber] domain." In 2013 for example, Russia created a new cyber warfare unit and has spent $500 million building a "cyber army". (Gerden 2014) Similarly China admitted in 2015 for the first time to having "specialized military network warfare forces" for offensive as well as defensive purposes. (Green 2015) One of the main symptoms of the militarisation of cyberspace has been the recent phenomenon whereby states create cyber warfare units as part of their military command structures. We have seen this trend within the previous case studies, and according to the UNIDIR (2013: 1), there are around 47 states engaged in a similar practice. Using the available data on the years in which units were established, Figure 7 highlights the rate at which this phenomenon has taken place.

Figure 10: Creation of Cyber Warfare Units in the International System (2005-2013)



(UNIDIR 2013)

The rate of the creation of cyber units has increased within a similar time frame as the two cyber arms races identified in the case studies, and it would not be unreasonable to suggest that these other states are engaged in similar processes as they seek to increase security through deterrence strategies. By creating cyber warfare units, states are following the old realist dictum that "if you want peace, prepare for war" (Diehl 1983 205), yet a large body of statistical studies show that seeking security through military strength and deterrence strategies in fact fuels insecurity and reaction, and the arms races that follow increase the likelihood of conflict. (Wallace 1977, Sample 1997, Gibler et al 2005, Vasquez 1993)

Rather than build up cyber warfare capabilities, states should seek non-confrontational methods of improving their cyber security, like increasing their cyber security infrastructure. Such strategies can only be seen as a positive thing in that they presumably make networks more difficult to penetrate by hackers, and are unlikely to contribute to the escalation of the cyber arms race, since they cannot be used for offensive purposes, or conceivably be seen as a security threat by other countries. To show that increasing cyber security in this way is beneficial, a statistical analysis is conducted here to show the relationship between secure servers and a country's malware infection rate.

A country year cross sectional data set was constructed using Microsoft Excel, and an Ordinary Least Squares regression was run using STATA statistical software. The dependent variable is a country's malware infection rate, which is a measure of how many instances of malware-infected computers are cleaned for every 1,000 computers scanned with Microsoft's Malicious Software Removal Tool. (Rains 2014) It serves as a good indicator of a country's cyber-attack threats since Microsoft has such a large share of the software market, but is by no means a comprehensive measure. The basic summary statistics of the dependent variable are shown below in table 3, to get an idea of the distribution of the data.

Table 3: Summary Statistics: Malware Infection Rates

No. Observations	Mean	Standard Deviation	Min	Max
114	11.1	5.6	1.5	30.9

(Rains 2014)

The range in this data sample, of the numbers of cleaned malware infected computers per 1000 scanned, runs from a minimum of 1.5 to a maximum of 30.9, with an average infection rate of 11.1.

Four independent variables are included in the model. The main variable of interest is the country's number of secure servers, used as a measure of a purely defensive improvement to cybersecurity. A secure server is a computer server using encryption technology in internet transactions, and the data comes from the World Bank/Netcraft. The variable is measured in terms of 1000's of secure servers per million of the population. Also included is a variable accounting for the countries that are known to have developed or are developing cyber warfare organisations, doctrines, or strategies. The assumption is made that this development is one of the main symptoms of the cyber arms race, as states respond to international cyber threats, and prepare for military engagement in the cyber domain. This data comes from the UNIDIR cyber index and the variable is coded as '1' if it is one of the 47 countries found to have "cyber security programmes that give some role to the armed forces". (2013: 1) With these two variables their relative impact on a country's cybersecurity can be quantified and compared.

Two other variables, also taken from the World Bank, are added as controls. The number of internet users per 100 people, and the GDP per capita in 1000's of US (current) dollars, are included as they are expected to be correlated with the numbers of secure servers. Countries that are more economically developed, and have more internet users will logically have improved internet infrastructure and technology, and these factors may also influence the level of malware intrusions. Without their inclusion therefore, a spurious relationship could be found between secure servers and the malware infection rate. The sample size is 114

countries, which is limited by the availability of the malware data. The data for all variables is taken from 2014

Table 4: OLS regression on malware infection rate (2014)

Variable	Coefficient	Std. Error
Constant	15.08***	1.24
Secure Servers	-3.74***	1.07
Cyber-militarisation	-0.84	1.01
GDP per capita	-0.05	0.04
Internet users	-0.05*	0.03
r^2 = .29		
N = 114		

*, **, *** indicates significance at the 90%, 95%, and 99% level respectively

The regression model makes a prediction, based on the data for the 114 countries, of the effect that each independent variable has on the dependent variable, while controlling for effect of the others. The r-squared value shows that these variables together explain 29% of the variance in the dependent variable. Internet usage is a significant predictor, yet only at the .1 level. The coefficient predicts a weak negative relationship between the number of internet users and malware infection rate. This may be explained by the likelihood that a country with more internet users has higher levels of computer technology, and thus better cyber security measures. Although the regression predicts that cyber militarisation was associated with decreased malware intrusions, it is not a statistically significant explanatory variable. Having cyber warfare organisations which seek to deter cyber-attacks therefore has no actual bearing on the level of malware intrusions.

The number of secure servers, on the other hand, is a statistically significant predictor of malware infection rate, at the .01 level. The coefficient suggests that on average, an increase in 1000 secure servers per million of the population, while controlling for the other factors, is

associated with a 3.47 reduction in the number of computers cleaned of malware for every 1000 computers scanned, suggesting that more secure servers is likely to improve cyber security against cyber-attacks. Although this is a very small reduction in malware infection rate, it should be remembered that the mean removal rate is just 11 as shown previously in table 3. This measure of cyber intrusions moreover, is based on only one type of cyber protection software, and one type of cyber-attack method. Regardless, the important conclusion to draw here is that increasing secure servers has a positive impact on cyber security.

7 CONCLUSION

One of the fundamental goals of IR research has always been to study the interaction between nation states in order to discover how competition and conflict can be minimised, in an international system that remains essentially anarchical and characterised by its inherently insecure nature. This same purpose should apply to the study of the cyber domain. We do not want to see an increase in the frequency or severity of cyber-attacks, and we want to steer policy makers away from using such tactics. In contributing to this goal, what this dissertation has shown is that, regardless of whether or not cyber conflict represents a growing danger to national security, perceptions of threat run extremely high in cyberspace, and this is causing a major reaction from states, evident in their build-up of cyber capabilities and preparations for cyber warfare. The central debate in the field is whether cyber is going to become a serious form of warfare, but the fact is that although it certainly poses a potential threat, we have yet to see anything on the scale of the 'cyber Pearl Harbour' predicted by some of those at the very top of policy making. Despite this political reality, governments worldwide are nevertheless engaged in the process of drawing up offensive cyber strategies, developing cyber weapons, establishing cyber warfare organisations, employing hackers, and increasing their spending. They are doing so because they believe it will deter attacks and make them more secure in cyberspace. The great irony, however, is that if cyber conflict does increase, it is the use of such confrontational policies that may be to blame. Realism's greatest flaw is the failure of power politics to enhance security; in fact it makes conflict more likely. The escalation of the cyber arms race must therefore be slowed, and different policies pursued.

Reacting to threats in this way is not the only option for states. The statistical analysis conducted in this paper shows that these militarised cyber policies do not actually reduce the level of intrusions coming in. Therefore, it can be concluded that the move to militarise cyberspace through the creation of cyber warfare organisations and strategies, in an attempt to increase national security, does not help in improving the nation's cybersecurity. What does improve cybersecurity on the other hand, are the preventative measures of securing one's internet servers that importantly, do not represent a threatening weapon of cyber warfare to other states. This research has thus not only measured a new phenomenon in international relations, but has been able to give clear policy guidance as to the strategies states should adopt, as well as avoid, to become more secure in cyberspace, and to discourage interstate cyber rivalries. In response to perceived threats, states should refrain from acquiring offensive capabilities which only set off security dilemmas, and focus instead on the prevention of attacks through improved cyber defence measures.

8 LIMITATIONS AND FUTURE RESEARCH

This has been an exploratory analysis to determine if the concept of an arms race could be applied to the cyber domain and in this respect the research aims have been met. Overall, the concept fits well into an international environment characterised by heightened threat perceptions, and the dyad cases presented here certainly exhibit the essential characteristic of an arms race, that is, of escalated competition. In many ways, however, an arms race is a theoretical construct as opposed to a real, identifiable phenomenon. Unlike the decision to go to war for example, policy makers do not make a conscious choice to end their normal behaviour and enter into an 'arms race', but are rather just conducting their foreign policies in relation to the international pressures that confront them. Where the line is drawn between normal and abnormal military competition will always be arbitrary and depend on the scholar's own judgement. To label specific events as arms races, and specific dyads as arms racing, is perhaps misleading, and it therefore may be more accurate to describe the arms dynamic on a continuum. Nevertheless, in empirical, and especially statistical, studies, dividing lines have to be drawn in order for variables to be operationalised, and for the analysis to be conducted. Treating arms races as distinct phenomena can be seen as a methodological tool that helps researchers identify, and thus investigate the motivations and

implications of some of the most serious instances of militarised competition in the international system.

This study only marks the beginning of a more ambitious research project to extensively quantify cyber capabilities in the international system, and this endeavour will requires a lot more data. The availability of time-series data has been the greatest constraint on the scope of this research project, and rather than carefully selecting representative cases for analysis, these case studies have admittedly been chosen largely because data could be found on them. Although they have been of interest for the cybersecurity discourse, other major players in the cyber conflict domain like China or Russia have been left out due to lack of information. Future research will therefore need to consider alternative metrics of cyber capabilities. These could include for example, the number cyber units in each country, the presence of cyber doctrines or strategies, and levels of computer education. The ultimate aim would be to collect these various types of data and create a capability index for each country in a similar vein to the Correlates of War project's National Material Capabilities Index. Such a data set would serve to promote the evidence based study of cyber politics that is a much needed development for countering the hyperbolic nature of the cyber domain.

In the analysis of the causes of cyber build-ups, more explanatory variables must also be considered. This has been an investigation of an action-reaction dynamic in international cyber relations, and in explaining the rapid build-up of cyber capabilities observed here, this paper has only considered one explanatory variable, that is, the presence of external cyber threats from rival states. A correlation between external threats and cyber build-ups has been found in these case studies, as well as evidence of a degree of interaction and competition between rivals. But military build-ups can also be motivated by a host of internal factors such as civil unrest, electoral politics, bureaucratic politics, a military-industrial complex, or by technological factors. Translating this to the cyber domain, the next step in investigating the causes of cyber build-ups is to look at domestic factors. For instance, cyber threats not only come from outside the state, but from hacker groups or individuals within the state. The role of cyber security companies in inflating the threat and creating a cyber-military industrial complex must also be studied, as well as the military bureaucracies that have an interest in promoting the acquisition of offensive capabilities. Even if external threats are still present, these domestic actors may be very influential in affecting the scale of the cyber build-up.

A final, and critical point, concerns the emphasis made throughout this paper that military competition is destabilising and likely to lead to further conflict, the assumption of which has served as the main justification for conducting this study. The previous IR research on the issue has been rather unequivocal, but nevertheless, since cybersecurity is a relatively new field of study, we do not yet know whether the same applies in the cyber domain. It has been beyond the scope of this research to properly investigate whether cyber arms races increase the chances that cyber tactics will be used, but this will be one of the next stages of research. The cyber arms race dynamic has been found to exist in international politics, and now the path has been cleared for more to be identified, and for their implications for international cyber security to be analysed.

References

Andres, Richard. 2012. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence", In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, ed. Derek Reveron, (Washington, DC: Georgetown University Press)

Booz Allen Hamilton, 2011. Cyber Power Index, http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

Bumiller, Elizabeth, and Thom Shanker. 2012. *"Panetta Warns of Dire Threat of Cyberattack on U.S"*, The New York Times, 11 October 2012, Available from: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Buzan, Barry, and Eric Herring. 1998. The Arms Dynamic in World Politics, (London: Lynne Reinner)

Cavelty, Myriam Dunn. 2012. *"The Militarisation of Cyberspace: Why Less May Be Better"*, NATO Cooperative Cyber Defence Centre of Excellence, 4th International Conference on Cyber Conflict, eds. C. Czosseck, R. Ottis, K. Ziolkowski.

Capaccio, Anthony. 2013. "Pentagon 5-year Cybersecurity Plan Seeks $23 Billion", Bloomberg Business, 10 June 2013, Available from: http://www.bloomberg.com/news/articles/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion

Carle, Jill. 2015. *"Climate Change Seen as Top Global Threat"*, Pew Research Center, 14 July 2015, Available from: http://www.pewglobal.org/files/2015/07/Pew-Research-Center-Global-Threats-Report-FINAL-July-14-2015.pdf

Carroll, Ward. 2007. *"Inside DPRK's Unit 121"*, DefenseTech, 24 December 2007, Available from: http://defensetech.org/2007/12/24/inside-dprks-unit-121/

Cashman, Greg, and Leonard C. Robinson. 2007. An Introduction to the Causes of War: Patterns of Interstate Conflict from World War I to Iraq, (Plymouth: Rowman and Littlefield)

Cashman, Greg. 1993. What Causes War? An Introduction to Theories of International Conflict, (New York: Lexington)

Choucri, Nazli. 2012. Cyber Politics in International Relations, (Cambridge: MIT Press)

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

Corera, Gordon. 2015. *"Rapid escalation of the cyber-arms race"*, BBC News, 29 April 2015, Available from: http://www.bbc.co.uk/news/uk-32493516

Deibert, Ronald. 2011. "Tracking the emerging arms race in cyberspace", Bulletin of the Atomic Scientists, 67(1): 1-8.

Derene, Glenn. 2009. *"The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back"*, Popular Mechanics, 30 September 2009, Available from: http://www.popularmechanics.com/military/a12667/4277463/

Diehl, Paul F. 1983. "Arms Races and Escalation: A Closer Look", Journal of Peace Research, 20(3): 205-212.

Eckstein, Harry. 1975. "Case Study and Theory in Political Science", in The Handbook of Political Science, eds. F. I. Greenstein and N. W. Polsby, (Reading: Addison-Wesley).

Fahrenkrug, David T. 2012. "Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy", Presented at the 4th International Conference on Cyber Conflict, ed. C. Czosseck, R. Ottis, K. Ziolkowski, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, June 5-8, 2012.

Fung, Brian. 2014. *"Cyber Command's exploding budget in 1 chart"*, The Washington Post, 15 January 2014, Available from: https://www.washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/

George, Alexander L. and Andrew Bennett. 2005. Case Studies and Theory Development in the Social Sciences, (Cambridge: MIT Press)

Gerden, Eugene. 2014. "$500 million for new Russian cyber army", SC Magazine, 6 November 2014, Available from: http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720

Gibler, Doug, Toby J. Rider, and Michael Hutchison. 2005. "Taking Arms Against a Sea of Troubles: Conventional Arms Races During Periods of Rivalry", Journal of Peace Research, 24(2): 251-276.

Glaser, Charles L. 2000. 'The Causes and Consequences of Arms Races', Annual Review of Political Science, 3: 251-276.

Glaser, Charles L. and Chaim Kaufmann. 1998. "What is the Offense-Defense Balance and Can we Measure it?", International Security, 22 (4): 44-82.

Gray, Colin S. 1971a. "The Arms Race Phenomenon", World Politics, 24(1): 39-79.

Green, Marcel A. 2015. "China's Growing Cyberwar Capabilities", The Diplomat, 13 April 2015, Available from: http://thediplomat.com/2015/04/chinas-growing-cyberwar-capabilities

Greenwald, Glen. 2015. "NSA Claims Iran Learned from Western Cyberattacks", The Intercept, 10 February 2015, Available from: https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

Hammond, Grant T. 1992. Plowshares into Swords: Arms Races in International Politics, 1840-1991, (Columbia: South Carolina Press)

Hansen, Lene, and Helen Nissenbaum. 2009. *"Digital Disaster, Cyber Security, and the Copenhagen School",* International Studies Quarterly, 53: 1155-1175.

Herz, John H. 1950. 'Idealist Internationalism and the Security Dilemma', World Politics, 2(2): 157-180.

Hewlett Packard. 2014. "Profiling an enigma: The mystery of North Korea's cyber threat landscape", HP Security Briefing Episode 16, August 2014, Available from: http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

Horn, Michael Dean, 1987. "Arms Races and the International System", PhD diss., (Rochester, NY: Department of Political Science, University of Rochester)

House of Representatives. 2010. "U.S. Cyber Command: Organizing for Cyberspace Operations", Committee on Armed Services, 23 September 2010, Available from: http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62397/pdf/CHRG-111hhrg62397.pdf

House of Representatives. 2012. "Iranian Cyber Threat to the U.S Homeland", Joint Hearing before the Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, 26 April 2012, Available from: http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm

Huntington, Samuel P. 1958. 'Arms Races: Prerequisites and Results', Public Policy, 8: 1-87.

International Telecommunications Union. 2015. Global Cyber Security Index and Cyberwellness Profiles, July 2015, Available from: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Isard, Walter. 1988. Arms Races, Arms Control, and Conflict Analysis: Contributions from Peace Science and Peace Economics, (New York: Cambridge University Press)

Jervis, Robert. 1976. Perception and Misperception in International Politics, (Princeton, Princeton University Press)
Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security, 38(2): 7-40.
Kennedy, Paul M. 1980. The Rise of the Anglo-German Antagonism, 1860-1914, (London: Allen and Unwin)
Kerr, P. K., J. Rollins, and C. A. Theohary. 2010, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," CRS Report for Congress R41524 (Washington, DC: Congressional Research Service, December 9, 2010), Available from: http://www.fas.org/sgp/crs/natsec/R41524.pdf
Kugler, Richard L. 2009. "Deterrence of Cyber Attacks", In Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Washington DC: Potomac Books), 309-342.
Lee, Dave, and Nick Kwek. 2015. "North Korean hackers 'could kill', warns key defector", BBC News, 29 May 2015, Available from: http://www.bbc.co.uk/news/technology-32925495
Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyebrwarfare Capabilities and Interstate War", Journal of Strategic Studies, 35(3): 401-428.
Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare", Security Studies, 22 (3): 365-404.
Lindsay, Jon R. and Lucas Kello. 2014. "Correspondence: A Cyber Disagreement", International Security, 39(2): 181-192.
Maurer, John H. 1992. 'The Anglo-German Naval Rivalry and Informal Arms Control, 1912-1914', The Journal of Conflict Resolution, 36(2): 284-308.
Mearsheimer, John J. 2010. 'Structural Realism', in International Relations: Discipline and Diversity (2nd Edition), ed. Tim Dunne, Milja Kurki, and Steve Smith, (New York: Oxford University Press) 78-94.
Mulrine, Anna. 2015. *"How North Korea built up a cadre of code warriors prepared for cyberwar"*, Christian Science Monitor, 6 February 2015, Available from: http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar
Nakashima, Ellen. 2014. *"Alexander: Promote Cyber Command to ful unified command status"*, The Washington Post, 12 March 2014, Available: https://www.washingtonpost.com/news/the-switch/wp/2014/03/12/alexander-promote-cyber-command-to-full-unified-command-status/
Nam, In-Soo. 2013. "North Korea Complains of Cyberattacks", The Wall Street Journal, 15 March 2013, Available from: http://blogs.wsj.com/korearealtime/2013/03/15/north-korea-complains-of-cyberattacks
Nye, Joseph. 2011. The Future of Power, (New York: Public Affairs)
Rains, Tim. 2014. *"United States' Malware Infection Rate More than Doubles in the First Half of 2013"*, Microsoft Cyber Trust Blog, 31 March 2014, Available from: http://blogs.microsoft.com/cybertrust/2014/03/31/united-states-malware-infection-rate-more-than-doubles-in-the-first-half-of-2013/
Rathjens, George W. 1969. 'The Dynamic of the Arms Race', Scientific American, 220: 15-25.
Richardson, Lewis F. 1960. Arms and Insecurity: A Mathematical Study of the Causes and Origins of War, ed. Nicolas Rashevsky and Ernesto Trucco, (Pittsburgh: The Boxwood Press) 17.
Rid, Thomas, and Peter McBurney. 2012. "Cyber-Weapons", The RUSI Journal, 157(1): 6-13.
Rid, Thomas. 2013. Cyber War Will Not Take Place, (C Hurst & Co Publishers Ltd)

Saltzman, Ilai. 2013 "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, 34 (1): 40-63.
Sample, Susan. 1997. "Arms Races and Dispute Escalation: Resolving the Debate", Journal of Peace Research, 34(1): 7-22.
Sanger, David E. 2012b. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Random House).
Sang-Hun, Choe. 2013. "Computer Networks in South Korea Are Paralyzed in Cyberattacks", The New York Times, 20 March 2013, Available from: http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html
Schweber, Aerianna. 2011. "South Korea Develops National Cyber Security Strategy", Intelligence, 28 August 2011, Available from: http://blogs.absolute.com/blog/south-korea-develops-cyber-security-strategy/
Shachtman, Noah. 2012. *"Iran Now a 'Top Threat' to U.S. Networks, Spy Chief Claims"*, Wired, 31 January 2012, Available from: http://www.wired.com/2012/01/iran-now-a-top-threat-to-u-s-networks-spy-chief-says/
Shalal-Esa, Andrea. 2013. "Iran strengthened cyber capabilities after Stuxnet: US General", Reuters, 17 January 2013, Available from: http://www.reuters.com/article/2013/01/18/us-iran-usa-cyber-idUSBRE90G1C420130118
Singer, J. David. 1972. *"The 'Correlates of War' Project: Interim Report and Rationale"*, World Politics, 24(2): 243-270.
Small Media. 2014. Iranian Internet and Infrastructure Policy Report, February 2014, Available from: http://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf
Small Media. 2015a. Iranian Internet Infrastructure and Policy Report, Special Edition, The Rouhani Review (2013-15), February 2015, Available from: http://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf
Small Media. 2015b. Iranian Internet Infrastructure and Policy Report, January 2015, Available from: http://smallmedia.org.uk/sites/default/files/u8/200215_InternetInfrastructure%20(1).pdf
Sorensen, D. S. 1980. *"Modelling the Nuclear Arms Race: A Search for Stability"*, Journal of Peace Science, 4: 169-185.
Sternstein, Aliya. 2015. 'Federal Cybersecurity Spending is Big Bucks. Why doesn't it Stop Hackers', Nextgov, 6 January 2015, Available from: http://www.nextgov.com/cybersecurity/2015/01/has-spending-nearly-60-billion-federal-cybersecurity-stopped-hackers/102534/
Stockholm International Peace Research Institute. 2015. SIPRI Military Expenditure Database, Available from: http://www.sipri.org/research/armaments/milex/milex_database
Taylor, Guy. 2015. *"James Clapper, intel chief: Cyber ranks highest on worldwide threats to U.S."*, The Washington Times, 26 February 2015, Available from: http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all
The Department of Homeland Security. 2015. "Safeguard and Secure Cyberspace", 6 August 2015, Available from: http://www.dhs.gov/safeguard-and-secure-cyberspace
The International Institute for Strategic Studies. 2014. The Military Balance 2014: The Annual Assessment of Global Military Capabilities and Defence Economics, 5 February 2014, (Routledge)
The White House. 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, Available from:

https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
United Nations Institute for Disarmament Research. 2013. The Cyber Index: International Security Trends and Realities, March 2013, Available from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
Valeriano, Brandon, and Ryan C. Maness. 2015. Cyber War versus Cyber Realities, (New York: Oxford University Press)
Valeriano, Brandon, Susan Sample, Choong-Nam Kang. 2013. "Conceptualizing and Measuring Rapid Military Buildups in the International System", Presented at Eurasian Peace Science Conference, Istanbul, Turkey, May 24-25 2013.
Vasquez, John A. 1993. The War Puzzle, (Cambridge: Cambridge University Press)
Wallace, Michael D. 1979. "Arms races and escalation: some new evidence", Journal of Conflict Resolution, 24(2): 289-292.
Weaver, Matthew. 2009. "Cyber attackers target South Korea and US", The Guardian, 8 July 2009, Available from: http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack
World Bank Group. 2015. Data Indicators, Available from: http://data.worldbank.org/indicator