2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Conceptualising Cyber Arms Races

Anthony Craig
Cardiff University
Cardiff, United Kingdom

Dr Brandon Valeriano
Cardiff University
Cardiff, United Kingdom

Abstract: This paper investigates the emergence of an arms race dynamic in the international cyber domain. The numerous claims made of an ongoing cyber arms race by the media and other analysts have not been backed up by careful empirical analysis. Characterised by the competitive and rapid mutual build-up of capabilities between pairs of states, arms races are a long standing aspect of study in international relations, with statistical evidence suggesting a relationship between these factors and war. Our work extends the tradition of arms race scholarship to the field of cyber security by providing a methodology for accounting for the build-up of cyber capabilities by nation states. We examine the concept of the cyber arms race and provide a plausibility probe for a macro study by examining the cases of the United States and Iran, and of North Korea and South Korea. We employ time series data on a number of indicators to measure each state's scale of increase in cyber capabilities, before investigating whether the states in question are directing their efforts against one another. Our findings suggest that these state dyads have indeed been engaged in cyber arms races, as defined by their competitive and above-normal mutual increase in cyber capabilities. This work furthers our understanding of state behaviour in the cyber domain, and our methodology helps to establish a pathway for the future extensive data collection of this new phenomenon.

Keywords: *cyber conflict, arms race, cyber capabilities*

1. INTRODUCTION

Cyberspace is now considered the fifth domain of warfare after land, sea, air, and space. Cyber conflict can be defined 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' (Valeriano and Maness, 2015, p.32). It consistently tops national threat assessments by policy figures, and in 2012 the US Defence Secretary warned of a 'cyber Pearl Harbor' that could devastate the country's critical infrastructure (Bumiller and Shanker, 2012). Regardless of the accuracy of these statements, there is a growing understanding that

such insecurities are driving countries to channel the ever increasing resources into their ability to defend themselves against cyber actions, and to launch offensive operations.

Media reports frequently use the term 'arms race' to describe the global proliferation of cyber warfare capabilities as states respond to their security concerns (Corera, 2015). For 57% of security experts and policy elites, the cyber arms race is a reality according to a 2012 survey (McAfee, 2012). Arms races traditionally refer to the rapid threat-driven and competitive build-up of military power between two countries, and have been criticised in the study of international relations due to their escalatory potential in bringing countries closer to the brink of war. Yet until now, the idea of a cyber arms race has not been subjected to proper empirical and academic analysis.

Here we conceptualise cyber arms races by applying traditional arms race theory to the cyber domain, thus gaining important insights into one of the most pressing and rapidly developing issues in world politics. First, the arms race and cyber literature is consulted before setting out our methods, and then two case studies of international rival state pairs are presented: the United States and Iran, and North and South Korea. We first measure their scale of arming, and judge whether it represents abnormal rates of increase. Then we investigate the extent to which these build-ups in cyber power occur in competition with one another specifically. We conclude by discussing the implications of our findings for interstate cyber relations, as well as their limitations, and explain how our research paves the way for future quantitative research on cyber capabilities.

2. WHAT IS AN ARMS RACE?

Arms races have been the subject of much research in the field of international relations as scholars have attempted to investigate their causes and consequences. In its traditional conceptualisation, an arms race results from mutual insecurity and the need to defend against an external threat. The build-up of arms is a core principle in realist theory, which tells us that the anarchical and self-help nature of the international system creates powerful incentives for countries to seek security through military strength and deter potential aggressors in an environment where they can never trust others' intentions.

Rather than promote stability, however, military build-ups can give rise to a security dilemma whereby 'many of the means by which a state tries to increase its security decrease the security of others' (Jervis, 1978). Security-seeking actions are often perceived as threatening and met with reactions in kind, causing interstate tensions to spiral out of control. Decades of peace science research has shown that arms races are associated with an increased likelihood of conflict, whereas very little evidence has been found in support of the opposing deterrence and balance of power theories (Leeds and Morgan, 2012, p.144).

Richardson (1960) made one of the first attempts at mathematically modelling this action-reaction dynamic, and in his set of equations each state's rate of arming increases in response to increases in its rival's military spending. This understanding of the arms race is one of mutual

fear, although Glaser (2004) notes how arms competition can occur when a status quo actor seeks to deter a power-seeking revisionist actor whose motivations are not those of insecurity. Psychology plays an important role in the arms racing process as policy makers do not always act rationally or with complete information (Jervis, 1976). Rather than react to actual threats, the decision to arm is often based on the 'subjective interpretations of the actions of others' (Hammond, 1993, p.47). The response to threats is therefore as much about perceptions as it is about reality.

A distinction can also be made between the types of capabilities involved. Qualitative arms races refer to the competition over technological advances in weaponry, whereas a quantitative arms race is the competition over the sheer number of military forces (Huntington, 1958). 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 less cost (Valeriano, Sample, and Kang, 2013).

Gray (1971, p.40) provides a useful definition of the arms race as:

> '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'.

It seems that any form of 'race' in military capabilities should fundamentally feature abnormally high rates of arming by at least two states which are engaged in this behaviour with reference to, and in competition with, one another.

Identifying such a process requires a distinction be made between normal and abnormal rates of military increase. One method used frequently in large-N studies (Sample, 1997; Gibler et al., 2005) codes a rapid build-up if a state's annual growth in either military expenditure or personnel reaches 8% in each of three consecutive years. An alternative measure by Horn (1987) posits that a state is engaged in a rapid military build-up in a given year if its average growth rate in expenditure in the preceding five years is greater than that of the preceding ten years; and if this ten year average is greater than that of the entire time period under observation. Overall, the current lack of data in this relatively new and often secretive domain means that alternative methods for evaluating the magnitude of cyber build-ups will need to be used.

In these quantitative studies, the competitive aspect is also measured in various ways. Sample (1997) uses data on militarised interstate disputes (the threat, display, or use of force) to confirm an adversarial relationship. Gibler et al. (2005) code their arms races based on Thompson's (2001) dataset of ongoing rivalries. In qualitative studies such as this, however, a more in depth analysis of the dyadic relationship can help uncover an action-reaction dynamic.

3. THE CYBER DOMAIN

Cyberspace is defined by Nye (2011, p.19) as the 'Internet of networked computers but also intranets, cellular technologies, fibre optic cables, and space based communications'. Cyberspace refers to not only 'all of the computer networks in the world' but also to 'everything they connect and control' (Clarke and Knake 2010, p.70), highlighting the potential risk to a nation's infrastructure given the fact that these systems are often dependent on Internet networks.

According to Choucri (2010, p.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. Proponents of the 'cyber-revolution' hypothesis highlight the serious damage cyber conflict could inflict potentially, and in doing so elevate the threat to the top of the state's national security concerns (Clarke and Knake, 2010; Kello, 2013). Others argue to the contrary that the threat is inflated and disconnected from reality (Lindsay, 2013; Valeriano and Maness, 2015), and as we know from traditional arms racing, fear and perceptions can be just as powerful drivers of security competition as actual threats.

Several characteristics help to establish the perception of cyberspace as an inherently insecure environment. Cyber weapons are essentially 'computer codes' used to inflict harm (Rid and McBurney, 2012, p.6), meaning that unlike the physical warfare domain, the virtual nature of malware makes it very difficult for states to gain an accurate picture of one another's capabilities. The anonymity that cyber methods can provide the attacker and the resulting attribution problem add to this uncertainty. Cyber capabilities include the malicious code created as well as the units mobilised, and the hardware and software developed, to defend against such code. Since cyber technologies can be much cheaper than conventional weapons, weaker states can possibly gain asymmetric advantages by entering into the cyber arms arena and compete on a more even footing with traditionally powerful states. The sources of threat are therefore potentially more widespread.

The belief that the cyber conflict domain favours the offense also creates insecurity. The offense-defence balance theory postulates that if offensive military capabilities hold advantages over defensive capabilities, the security dilemma is more intense and the risk of arms races and war greater (Glaser and Kaufmann, 1998, p.47). Offensive cyber capabilities are assumed to be more cost effective and efficient, whereas defence is difficult given the immense challenge involved in securing every civilian and privately owned network and closing every vulnerability, many of which go undetected until an attack has pointed them out (Liff, 2012). The Internet's lack of geographical constraints further undermines the utility of defence. Offensive preparations may therefore become the dominant strategy, which can risk setting off the security dilemma.

Given the complexity of the cyber domain and its overall novelty, many make statements about the dynamics of cyber conflict without clear connections to more than a few cases, which may be outliers. This is why a macro and empirical perspective on cyber arms build-ups is an important task in the field. Exploring the concept of the cyber arms race is a theoretically appropriate

undertaking given the heightened perceptions of threat that characterise the international cyber domain, and will help shed light on how states are reacting to their cyber security concerns.

4. METHODOLOGY

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 in application. We conduct case study analyses of two rival state dyads; the United States and Iran, and North and South Korea. These four countries are among the major players in the cyber conflict arena, and are therefore of great interest to policy makers and academics alike.

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. The two questions asked ensure that the essential arms race criteria are met:

1. Are both states engaged in a rapid build-up of cyber capabilities?
2. Are the states in competition with one another?

To answer the first question, time series data is presented to track changes in each state's cyber capabilities. Clearly it is not possible to quantify the actual cyber 'arms' or malware possessed by states, and we acknowledge this limitation. Instead, our approach is inspired by the Correlates of War Project (Singer, 1972) in its use of military expenditure and personnel data, which have often been used in previous arms race studies. Applying this to cyberspace, the data that is mainly sought here is government spending on cyber security and the number of cyber security specialists employed by governments. These should offer a direct indication of the effort that states are putting into developing their overall cyber strength. Other indicators are relied on if this data is not available. What we aim to indicate is at least whether a significant increase in the effort by states to boost their capabilities is occurring. To determine whether these cyber build-ups are out of line of normal state behaviour, various comparison techniques are used to place them in context.

To answer the second question, a qualitative approach is taken to identify a potential action-reaction and competitive dynamic between our state pairs. We look for a general indication that each state is developing its capabilities in response to the actions of, or the perceived threat posed by, the other. If these criteria are met, it would suggest that there is an arms racing dynamic in cyberspace. While the security portfolio of a state is quite diverse and a major power like the United States likely engages multiple threats, a cyber arms race as we conceptualise it is indicated by the existence of an adversarial relationship and does not demand that all monetary amounts be directed specifically towards the opposition state under examination. The methods we undertake here will allude to the opportunities and challenges in measuring cyber arms races, and our potential limitations are discussed in more depth in the concluding section.

5. THE UNITED STATES AND IRAN

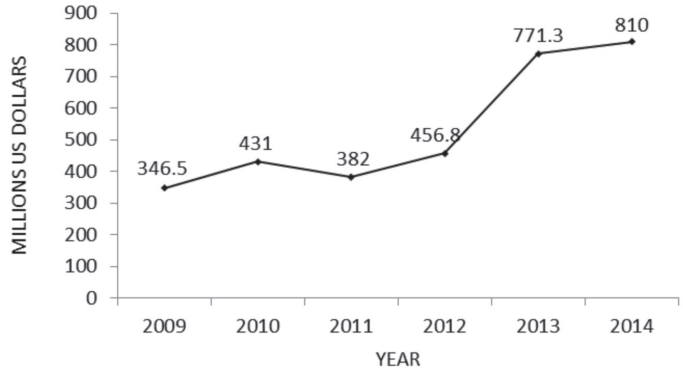
A. US cyber build-up

As a democratic and open society, the United States is relatively forthcoming about its investments in cyber security. The availability of data on two government departments, the Department of Homeland Security (DHS) and the Department of Defense (DOD), allows a rough distinction to be made between the changing defensive and offensive cyber capabilities of the United States.

The DHS is tasked with defending the country against a range of threats, and one of its five stated missions is to 'safeguard and secure cyberspace' by seeking to 'analyse and reduce cyber threats and vulnerabilities […and to…] distribute threat warnings […and…] coordinate the response to cyber incidents to ensure that computers, networks, and cyber systems remain safe' (DHS, 2015). Budget figures are available for the National Cyber Security Division (NCSD), which operates under the Directorate for National Protection and Programs and is home to the United States' Computer Emergency Response Team (CERT) team.

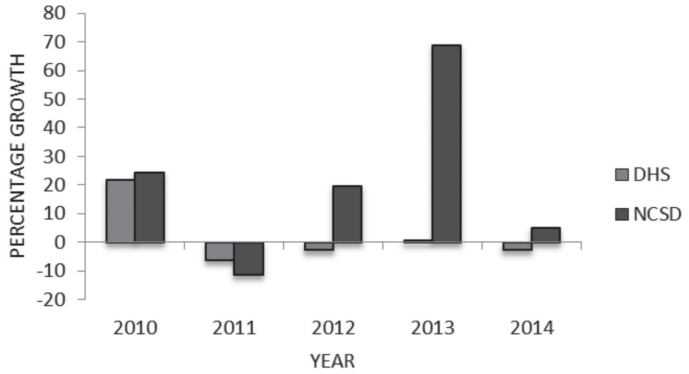
Figure 1 illustrates the changing NCSD budget in constant (2014) US Dollars. Although the unit was formed in 2003, the data is only available between 2009 and 2014.

FIGURE 1: NATIONAL CYBER SECURITY DIVISION BUDGET, 2009-2014 (CONGRESSIONAL RESEARCH SERVICE)



The government funding received by the Cyber Division increased from $346.5 million in 2009 to $810 million in 2014, representing a growth of 134%. The budget has grown in almost 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 growth in the NCSD budget to that of the DHS as a whole.

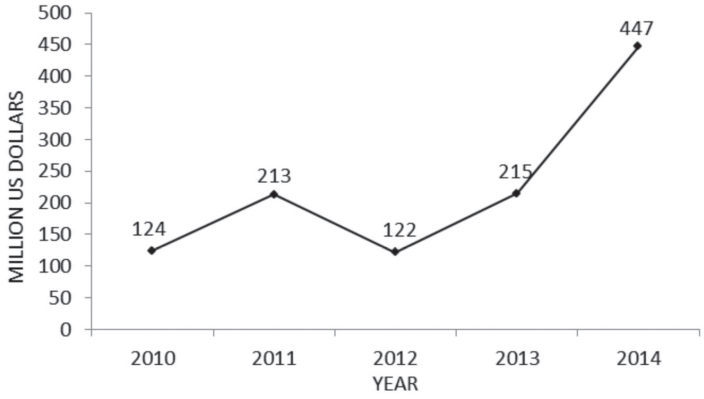
FIGURE 2: ANNUAL GROWTH IN DHS AND NCSD BUDGETS, 2010-2014 (CONGRESSIONAL RESEARCH SERVICE)



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 Division's budget grew by 69% from the previous year.

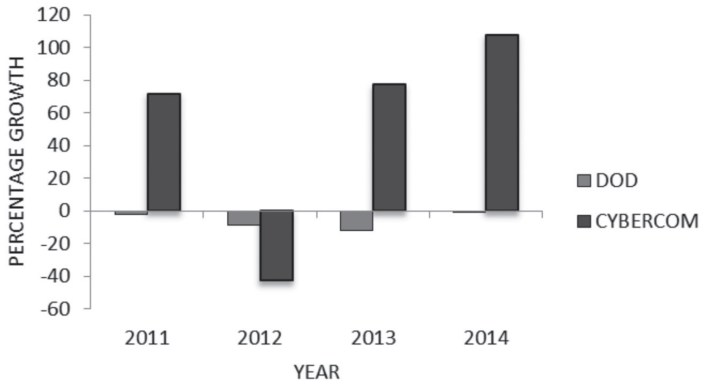
The build-up of offensive cyber capabilities is a more secretive and controversial development, but budget figures are available on the US Cyber Command unit, which reached full operational capacity in 2010. US Cyber Command falls under US Strategic Command, which is one of the 9 military command structures of the DOD. With its stated mission of carrying out the 'full spectrum military cyberspace operations [and to] ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries' (US Stratcom, 2015), the establishment 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 US dollars.

FIGURE 3: CYBER COMMAND BUDGET, 2010-2014 (FUNG, 2014)



The US government has evidently been channelling increasing resources into the Cyber Command budget, which has risen from $124 to $447 million since its inception. To give context to this spending pattern, the annual percentage growth in Cyber Command spending is compared in Figure 4 with that of the DOD; in other words, the entire military budget of the United States.

FIGURE 4: ANNUAL GROWTH IN DOD AND CYBER COMMAND BUDGETS, 2011-2014 (FUNG, 2014; SIPRI, 2015)

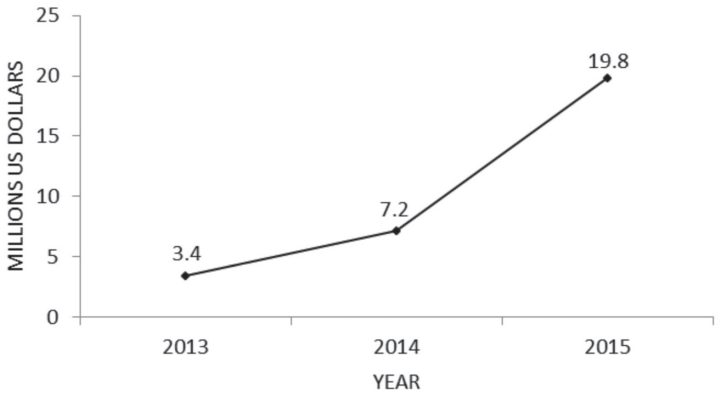


Despite decreases in each year to total defence spending, Cyber Command's budget has tended to grow, and more than doubled in 2014 from the previous year.

B. Iran cyber build-up

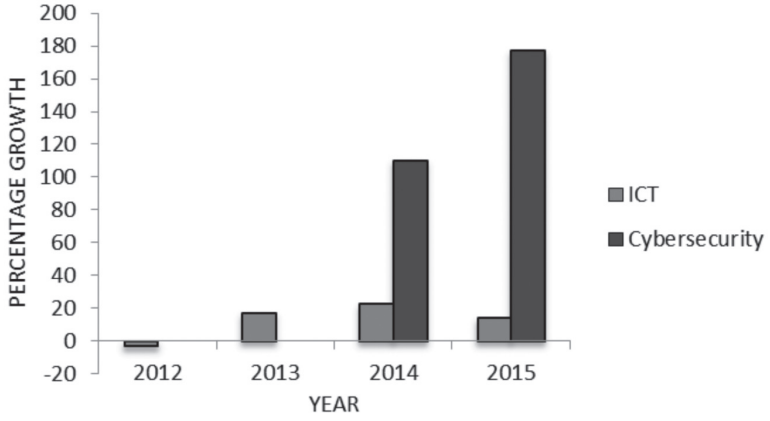
Like the US, Iran is also improving its cyber capabilities. The Iranian Revolutionary Guard Corps has reportedly trained a cyber-army of 120,000 consisting of 'university teachers, students, and clerics', which it claims to be the second largest in the world (UNIDIR, 2013, p.32). In 2012 the Supreme Leader Ayatollah Khamenei established a new cyber unit called the 'Supreme Council of Cyberspace' (SCC), which has ultimate control over all Internet and cyber-related policies in Iran. The SCC's 2014 budget was $40 million, which it receives from Iran's larger ICT budget (Small Media, 2014, p.7). Since President Rouhani came to power, data has been released on Iran's cyber security spending which is presented in figure 5.

FIGURE 5: IRAN'S CYBER SECURITY BUDGET, 2013-2015 (SMALL MEDIA, 2015)



The cyber security budget has increased markedly from $3.4 million in 2013 to $19.8 million in 2015. To put this increase in context, Figure 6 compares the cyber security budget's annual percentage growth in 2014 and 2015 with that of Iran's ICT budget.

FIGURE 6: ANNUAL GROWTH IN IRAN'S ICT AND CYBER SECURITY BUDGETS, 2012-2015 (SMALL MEDIA, 2014; 2015)



Iran's ICT budget has also been increasing year on year since 2013, but not on so great a scale as the cyber security budget. This suggests significant efforts by Iran to specifically improve its cyber capabilities.

C. Dyadic interaction

The United States and Iran have a history of cyber conflict with one another, and as is shown in Table 1, Iran clearly has had more to fear from the United States between 2001 and 2011.

TABLE 1: CYBER CONFLICT BETWEEN THE UNITED STATES AND IRAN, 2001-2011 (VALERIANO AND MANESS, 2014)

US Initiated	6
Iran Initiated	1
Total	7

Initially Iran did not factor much in US cyber strategy, and the sole documented incident carried out by Iran was the 2009 Twitter hack which involved mere website defacement. The competitive cyber relationship was sparked in June 2010 with the discovery of the highly sophisticated Stuxnet computer virus that had been used to target one of Iran's major nuclear enrichment plants in Natanz. The United States, in collaboration with Israel, is widely believed to have masterminded the attack as a means to curb Iran's nuclear ambitions. According to Sanger (2012b, p.205), the attack destroyed 984, or a fifth, of the facility's centrifuges.

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 Ayatollah Khamenei announced the creation of the Supreme Council of Cyberspace (SCC). Operating under the SCC is the National Centre for Cyberspace (NCC) which is tasked with protecting the country from cyber-attacks, and to help develop a national Internet that would reduce Iran's Internet dependency (Small Media, 2014, p.4).

Retaliation for Stuxnet, and a physical display of Iran's developing offensive cyber capabilities, came in the form of the 'Shamoon' attack, launched by Iran in August 2012 against the Saudi Aramco oil company. Valeriano and Maness (2015, p.157) judge the incident, which deleted data and removed the re-boot program from around 30,000 computers, to be an example 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 US feared that Iran was learning from the attack, with the head of Air Force Space Command, General William Shelton, reporting to the media in January 2013 that 'it's clear that the Natanz situation generated a reaction by them'. He identified Iran as 'a force to be reckoned with, with the potential capabilities that they will develop over the years and the potential threat that will represent to the United States'. He also called for increased cyber-security spending, and announced plans to increase the number of cyber personnel in his unit by 1,000 (Shalal-Esa, 2013).

That the US was developing a growing perception of threat from Iran is supported by a Snowdon-leaked NSA document from April 2013. It discussed how Iran had learned from

cyber-attacks launched against it, and had been behind several waves of DDoS attacks on US financial institutions, on top of the Saudi Aramco attack (Greenwald, 2015).

US officials undoubtedly began to see Iran as a source of cyber threat around this time. Speaking before the Senate Intelligence Committee in 2012, the 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 the Committee on Homeland Security in April 2012, it was reported 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).

This is a clear example of a state perceiving a threat from the developing capabilities of another, as the action-reaction model predicts. Although a firm connection cannot be proven, it is unsurprising that the data presented on US cyber-warfare spending shows the largest increases after 2012, the year in which the United States apparently became more fearful of the threat from Iran as it responded to Stuxnet. The evidence suggests that both countries developed their capabilities in reaction to one another. Therefore, the competitive aspect of an arms race appears to be present here, as well as the rapid and mutual increase in cyber capabilities.

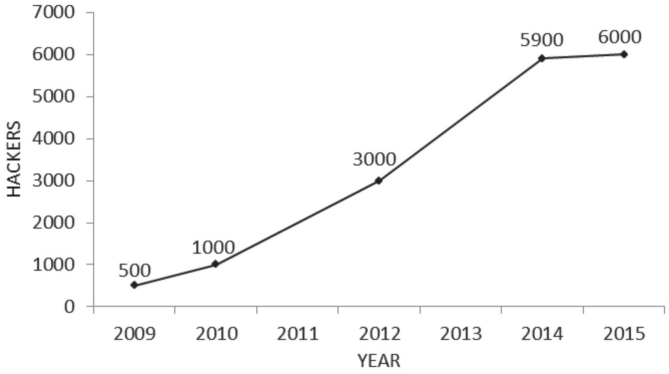
6. NORTH KOREA AND SOUTH KOREA

A. North Korean cyber build-up

The one-party Communist state of North Korea is strongly suspected to be building up its offensive cyber capabilities and is known to have a number of cyber warfare units. Acquiring reliable data on perhaps the most secretive country in the world is particularly challenging. 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 a total of six known cyber units, each with varying cyber warfare roles, including Unit 35 that is believed to be involved in training hackers (Hewlett Packard, 2014, p.26).

A defector to South Korea estimated that between 10 and 20% of North Korea's military budget is spent on 'online operations' (Lee and Kwek, 2015), and a number of defectors as well as South Korean news organisations have made various claims over time regarding the size of North Korea's army of cyber hackers. In figure 7, these estimates are pieced together to highlight the growth of North Korea's offensive capabilities.

FIGURE 7: NORTH KOREA'S 'CYBER ARMY',
2009-2015 (HEWLETT PACKARD, 2014; MULRINE, 2015; LEE AND KWEK, 2015)



If accurate, the data would suggest that the number of North Korean hackers has increased twelvefold since 2009. There is reason to believe such estimates due to the repeated nature of the information, yet the figures are potentially biased since defectors to the south are likely to support heightened concern for North Korean activities.

B. South Korean cyber build-up

South Korea has also been developing its cyber capabilities and in 2010 a cyber-warfare unit was created, staffed by approximately 200 personnel (UNIDIR, 2013, p.41). The 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 web servers that use encryption technology in Internet transactions, thus somewhat gauging a country's cyber defences. It has certain weaknesses as an indicator of cyber power, but nevertheless appears to show a reaction from South Korea. The change in secure servers from 2003 to 2014 is plotted in Figure 8, and is compared with other groups of countries to put South Korea's cyber build-up into context.

FIGURE 8: SOUTH KOREA'S SECURE SERVERS, 2003-2014 (WORLD BANK, NETCRAFT)

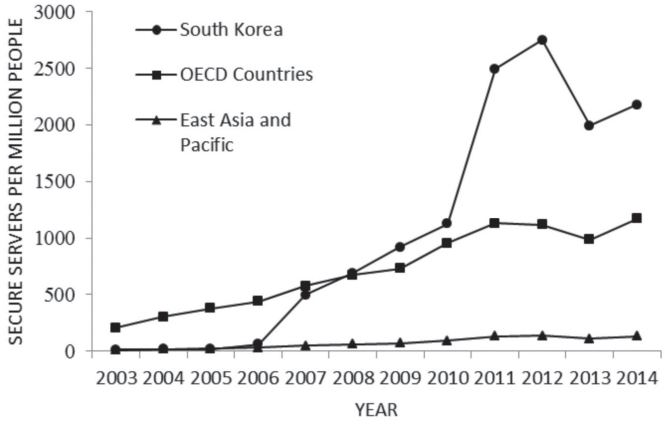


Figure 6 shows a remarkable increase in the number of South Korea's cyber defences. Secure servers grew from just 14 per million people in 2003, to 2,178 per million people in 2014. There was a particularly accelerated period of growth from 2010 when the number of secure servers more than doubled within a year. Furthermore, South Korea's improvements to its cyber capabilities have evidently been on a much greater scale than that of its neighbours in the region, as well as among other economically advanced OECD member states.

C. Dyadic interaction

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

TABLE 2: CYBER CONFLICT BETWEEN NORTH AND SOUTH KOREA, 2001-2011 (VALERIANO AND MANESS, 2014)

North Korea Initiated	10
South Korea Initiated	1
Total	11

According to the data set, these 10 cyber incidents initiated by the North against the South all took place in the short space of three years between 2008 and 2011, thus giving South Korea a motive for increasing its cyber defences. The process of interaction here has typically been action by the North followed by reaction by the South. For example, in 2009 a DDoS attack hit the networks of several South Korean government organisations and banks (Weaver, 2009). In response, South Korea created a cyber command unit in 2010, with the defence ministry explicitly referencing the threat from North Korea as the justification for the development (Yonhap News Agency, 2010).

South Korea was again targeted by the North in 2011, in an attack that brought down 26 government, military, and banking websites (BBC News, 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 the 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 shown in Figure 6 is perhaps directly linked to this policy. In August 2012, the South called for the number of cyber security personnel in its cyber warfare unit to be increased to 1,000 from the 200 initially working there, to help cope with the North Korean threat (Korea JoonGang Daily, 2012).

Another incident in 2013 shut down the South Korean banking system and several television stations. This attack was somewhat more sophisticated in that malware was used, as opposed to the DDoS method, 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 5,000 cyber troops to defend against North Korean cyber-attacks (Hewlett Packard, 2014, p.4). If this was indeed a reaction to the developing capabilities of the North, it gives reason to believe the data

on North Korea's cyber army as it shows South Korea trying to compete with the developments of its rival.

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

The presence of a mutual cyber build-up, and the fact that both countries were targeting or responding to one another, is suggestive of an arms racing relationship between North and South Korea also.

7. CONCLUSION AND LIMITATIONS

Both cases appear to meet the criteria for a cyber-arms race which, when applied according to the standards of the international relations research community, is confirmed as a suitable framework for use in the cyber domain. The US-Iran case provides a novel example of cyber competition being driven by mutual insecurity, despite a vast difference in conventional power between them. The actual threat that Stuxnet posed sparked the cyber build-up by Iran, which in turn was perceived as a threat by the United States. The fact that these US security concerns began around the same time as the rapid increases to its cyber security spending suggests they were linked, and that a US-Iran cyber arms race was initiated around 2012. If uncertainty and defensive motivations are indeed at the heart of this cyber arms race, then, given the progress being made on the nuclear issue, there may be hope for an end to its escalation if confidence building measures can be put in place.

The relationship between North and South Korea is somewhat different. Unlike the US-Iran dyad, the insecurity that characterises this arms race has been very one sided since North Korea is motivated in its build-up more by aggressive intent rather than fear. 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 case 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. In a situation somewhat akin to that of a revisionist power, 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 response.

This research has demonstrated that there is much the cyber security community can learn from international relations scholarship on arms races. It provides the basis for an understanding of the motivations behind the proliferation of cyber warfare capabilities currently observed in the international system by placing it within the context of interstate competition. Conceptualising this dynamic in cyberspace is an important step in working towards a more secure and

cooperative environment. Given the escalatory nature of arms races, our findings highlight the urgent need for policy makers to understand how their cyber security policies can lead to reactions and create instability as tensions spiral.

Our methodological limitations must be addressed, however. A likely criticism relates to whether we have been able to demonstrate that these cyber build-ups are explained purely by dyadic competition. For instance, surely US cyber spending is motivated just as much, and perhaps more, by its other competitors such as Russia or China. This could very well be true, and we have not tried to argue that its spending is wholly a function of Iranian threat. This is not a necessary criteria for arms races generally, as states must consider all potential threats in the system. Nevertheless, it is clear from our case study evidence that the US perceived a significant threat from Iran and vice versa, which correlates with notable developments in their cyber capabilities.

Since cyber might be an asymmetric domain (Liff, 2012, p.409), we should not dismiss the idea that a traditionally weaker power like Iran plays an important role in US cyber strategy. An extensive report by security firm Cylance even places the Iranian threat on a par with Russia and China (Cylance, 2014). Our analysis leads us to suggest that the term arms race is a reasonable description of the relationship, based on our review of the case. We accept that we cannot demonstrate a causal link between patterns of cyber-build up and the actions or behaviour of another state. To establish such would be difficult without direct statements from the leadership, a condition rare in history. In any study of arms races, it is not possible to calculate just what proportion of spending is accounted for by one particular state, or what threat drives which weapons system. Moreover, factors internal to the state (political, economic, and technological) can have a major effect on military spending patterns, and how this idea relates to the cyber domain is a critical area for future research.

This endeavour is only the beginning of a more systematic investigation of cyber build-ups in international politics. Our method of focusing on single state pairs represents a manageable first step in this particular area, and follows decades of research in the international relations field. At a minimum, we believe we have been able to show that external threats from other states, whether perceived or real, are an important variable in shaping a state's national cyber security policies. We aim to build on what we have begun here and continue to identify the wider range of factors accounting for the acquisition of cyber capabilities.

The next step will include expanding the number of cases, collecting data on a wider range of indicators, and developing a methodology for accurately judging cyber power. Despite the secrecy that pervades the domain, the collection and analysis of data relating to cyber security is possible, although difficult and time consuming. It is nevertheless a much needed task if we are to ground the study of cyber conflict within empirical research frameworks.

REFERENCES

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

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

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

Congressional Research Service Reports on Homeland Security, last updated December 15, 2015, http://www.fas.org/sgp/crs/homesec/

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

Cylance, 'Operation Cleaver', December 2014, https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

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)

Fung, Brian,'Cyber Command's exploding budget in 1 chart', The Washington Post, 15 January 2014, 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)

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

Greenwald, Glen, 'NSA Claims Iran Learned from Western Cyberattacks', The Intercept, 10 February 2015, 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)

Hewlett Packard, 'Profiling an enigma: The mystery of North Korea's cyber threat landscape', HP Security Briefing Episode 16, August 2014, 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, '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

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

Jervis, Robert. 1976. Perception and Misperception in International Politics, (Princeton, Princeton University Press)

Jervis, Robert. 1978. 'Cooperation Under the Security Dilemma', World Politics, 30(2): 167-214

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

Lee, Dave, and Nick Kwek, 'North Korean hackers 'could kill', warns key defector', BBC News, 29 May 2015, http://www.bbc.co.uk/news/technology-32925495

Leeds, Brett A. and T. Clifton Morgan. 2012. 'The Quest for Security: Alliances and Arms', in Guide to the Scientific Study of International Processes, Ed. Sarah McLaughlin Mitchell, Paul F. Diehl, and James D. Morrow, (Wiley-Blackwell)

Liff, Adam P. 2012. 'Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare 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

Mulrine, Anna, 'How North Korea built up a cadre of code warriors prepared for cyberwar', Christian Science Monitor, 6 February 2015, http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar

Nam, In-Soo, 'North Korea Complains of Cyberattacks', The Wall Street Journal, 15 March 2013, http://blogs.wsj.com/korearealtime/2013/03/15/north-korea-complains-of-cyberattacks

Nye, Joseph. 2011. The Future of Power, (New York: Public Affairs)

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)

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

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, 'Computer Networks in South Korea Are Paralyzed in Cyberattacks', The New York Times, 20 March 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

Schweber, Aerianna, 'South Korea Develops National Cyber Security Strategy', Intelligence, 28 August 2011, http://blogs.absolute.com/blog/south-korea-develops-cyber-security-strategy

Shachtman, Noah, 'Iran Now a 'Top Threat' to US Networks, Spy Chief Claims', Wired, 31 January 2012, http://www.wired.com/2012/01/iran-now-a-top-threat-to-u-s-networks-spy-chief-says/

Shalal-Esa, Andrea, 'Iran strengthened cyber capabilities after Stuxnet: US General', Reuters, 17 January 2013, 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, Iranian Internet and Infrastructure Policy Report, February 2014, http://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf

Small Media, Iranian Internet Infrastructure and Policy Report, January 2015, http://smallmedia.org.uk/sites/default/files/u8/200215_InternetInfrastructure%20(1).pdf

SIPRI, Military Expenditure Database, last updated November 2015, http://www.sipri.org/research/armaments/milex/milex_database

Thompson, William R. 2001. 'Identifying Rivalry and Rivalries in International Politics', International Studies Quarterly, 45(4): 557-586

UNIDIR, The Cyber Index: International Security Trends and Realities, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Valeriano, Brandon, and Ryan C. Maness. 2014. 'The dynamics of cyber conflict between rival antagonists, 2001-11', Journal of Peace Research

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. 'Conceptualising and Measuring Rapid Military Buildups in the International System', Presented at Eurasian Peace Science Conference, Istanbul, Turkey, May 24-25 2013

World Bank/Netcraft, Secure Internet Servers (per 1 million people), last accessed December 2015, http://data.worldbank.org/indicator/IT.NET.SECR.P6

Weaver, Matthew, 'Cyber attackers target South Korea and US', The Guardian, 8 July 2009, http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack