Reacting to Cyber Threats: Protection and Security in the Digital Age

Anthony Craig [A] & Brandon Valeriano[B]

The cyber threat is now a major source of concern in contemporary security affairs and for many governments worldwide cyberspace now represents a new warfighting domain. Given these heightened levels of fear, it is important to ask what steps are being taken by states in response to the threat. A worrying development is the supposed cyber arms race in offensive capabilities given the propensity of these processes to escalate already high levels of tensions between rivals. At the same time, there are suggestions that proper defensive measures have not being given the utmost priority that they arguably should be. Despite speculation, these questions have not been subjected to empirical and data-driven analysis. This article investigates the reaction to the cyber threat by first examining the relationship between threat perception and the presence of offensive capabilities, and then engages the question of whether states are improving their nationwide defensive infrastructure in response to fear. Our results suggest that the heightened perception of threat is indeed linked to the possession of offensive capabilities, but we find little evidence to show that the cyber fear is motivating states to improve their basic cyber hygiene through the use of encrypted server technologies.

Key words: *cyber security, threat, offense, defense*

Introduction

In this highly interconnected digital era, cyber threats now represent one of the most urgent national security concerns. This has prompted governments worldwide to reconfigure their military strategies to prepare for battle in cyberspace, now considered a domain of warfare alongside land, sea, air, and space.[1] Cyber has become a particularly critical issue within US political discourse with the Director of National Intelligence James Clapper consistently naming it as the top security concern over the past few years.[2] This heightened level of fear is also reflected in American society at large

[A] Cardiff University

[B] Cardiff University and Donald Bren Chair of Armed Conflict, Marine Corps University

[1] *"War in the fifth domain,"* The Economist, July 1, 2010, http://www.economist.com/node/16478792

[2] G. Taylor, *"James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S.,"* Washington Times, Feb 26, 2015, http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all

doi: 10.18278/gsis.1.2.3

as is evident in a 2015 global threat survey which found that 59% of the US public felt "very concerned" about the "risk of cyber attacks on governments, banks, or corporations".[3] The cyber threat is ranked up there with and often supersedes other pressing security threats like ISIS, a rising China, or a resurgent Russia, as commentators warn of a "Cyber Pearl Harbor" suggesting a devastating cyber incident against the state's critical infrastructure is inevitable.[4] Fear clearly runs high in the cyber domain and a key question to address is what kind of reaction these heightened levels of threat perception are provoking.

An ongoing debate within the cyber security field centers on the issue of whether this level of perceived threat is justified, and if the prospect of cyber conflict represents a revolution in how states should think about their national security, or whether the risk is instead largely exaggerated by the military bureaucracies, security firms, and the media outlets who often stand to gain from threat inflation. Empirical studies suggest that the threat is hyped to a large extent (Lindsay 2013; Valeriano and Maness 2015), yet the critical query skipped thus far in the debate regards the nature of the reaction. It is important to pay close attention to how states react to their perceived fears because we should be concerned with encouraging policy responses that are proportional to the reality of the dangers in the international system and effective in increasing security.

One way in which states can react to the threat is through offensive cyber technologies that are wielded as an assumed deterrent against potential aggressors in cyberspace. Many countries appear to be seeking to enhance their cyber warfare capabilities by establishing cyber command units and hiring teams of professional hackers, and these actions may be symptomatic of what is increasingly being referred to as the "cyber" arms race (Craig and Valeriano 2016; Diebert 2011). While it is urgent we pay attention to these offensive developments, we should also ask how states are responding in terms of their defensive and protective infrastructure. This is arguably the sensible first step governments should take in response to their security fears, in contrast to the build-up of offensive capabilities which risks setting off security dilemmas and escalating levels of tension and conflict.

Our research question is particularly critical in light of suggestions that proper defensive measures are not being given priority (Rid 2013). The US Department of Homeland Security for example is charged with protecting the nation-state against incoming attacks, yet an internal audit reported numerous fatal flaws in security systems as well as a lack of training among cyber security professionals.[5] The hack of the Office of Personnel Management (OPM) in June 2015 resulted in 22.5 million sensitive records being stolen, but this breach did not occur due to the skill of the attacker but rather

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

[4] While these threats may overlap, public opinion surveys ask the question in such a way as to make these threats different.

[5] A. Carman, *"DHS Websites Vulnerable to Exploits Amid Lacking Cyber Security Training,"* SC Magazine, September 17, 2015, http://www.scmagazine.com/oig-issues-department-of-homeland-security-report/article/439025/?utm_content=bufferc11a1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

the incompetence of the systems administrators and the connections with external contractors.[6] Rather than upgrade their systems to prepare for the increasing online threats, the US Navy even continues to pay Microsoft to support the outdated and vulnerable Windows XP platform.[7] And despite the Department of Homeland Security's attempts to secure government networks through the deployment of the EINSTEIN intrusion detection system, it has been reported that these systems fail to detect 94% of the most common types of vulnerabilities.[8] These examples suggest that there is room for improvement in the state's basic cyber hygiene practices that should be given at least as much, if not more, consideration than offensive cyber posturing.

This article investigates reactions to the cyber threat and particular attention is paid to whether states are responding by improving their cyber security infrastructure. In doing so this article continues the rise of the social science perspective in this new area of security studies by using data and evidence to engage critical cyber security questions. While examples and case studies can be illustrative and illuminating, they fail to provide us with a macro picture of state behavior in the international cyber domain. One can tell a harrowing story of the Stuxnet cyber attack and its impacts as if it was a James Bond story rewritten for modern times, but these illustrations have little connection to the general trends in the field. Our approach is to provide a statistical analysis of the issue using the available data to uncover global patterns in cyber security practices in the international system.

Cyber Threats and Their Reactions

Concerns over politically motivated, destructive attacks from other states or terrorists groups are what motivated the "cyber Pearl Harbor" warning by the then US Defense Secretary Leon Panetta in 2012. This type of threat can be described as sabotage or cyber conflict 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). These types of actions can be launched against a nation's critical infrastructure, much of which is connected to and operated by internet networks. Such an attack, in theory, has the potential to shut down electricity grids or financial systems and create chaos within society, although an incident on such a destructive scale has yet to take place. In these attacks, there is clear coercive intent.

[6] A. Elkus, *"No Patch For Incompetence,"* War on the Rocks, June 23, 2015, http://warontherocks.com/2015/06/no-patch-for-incompetence-our-cybersecurity-problem-has-nothing-to-do-with-cybersecurity/

[7] R. Hackett, *"Why the U.S. Navy is Still Paying Microsoft Millions for Windows XP,"* Fortune, June 24, 2015, http://fortune.com/2015/06/24/navy-microsoft-windows-xp/

[8] A. Sternstein, *"US Homeland Security's $6B Firewall Has More Than a Few Frightening Blind Spots,"* Defense One, January 29, 2016, http://www.defenseone.com/technology/2016/01/us-homeland-securitys-6b-firewall-has-more-few-frightening-blind-spots/125528/?oref=DefenseOneFB

Much more widespread is the activity of cyber espionage, or the "attempt to penetrate an adversarial computer network or system for the purpose of extracting sensitive or protected information" (Rid 2013). Cyber espionage is a form of computer network attack (CNA) that can also come in the form of coercive attempts and disruption events (Jensen, Maness, and Valeriano. 2016). The 2009 theft of the F-35 fighter designs from the US military by Chinese hackers is one of the most high-profile cases of cyber espionage. Cybercrime is another threat that applies to society more generally. It involves the financially motivated theft of information and tends to be carried out by non-state actors or individuals lacking political motivations.

Scholars working on these issues are split on the level of risk they represent. Some see the rapid technological change in the information age as causing the greatest revolution in military affairs of our time (Clarke and Knake 2010; Kello 2013). This is known as the cyber revolution hypothesis, whose proponents argue that the unique characteristics of the cyber domain, such as the lack of geographical constraints, the problem of attribution, the involvement of non-state actors, and the low cost of offensive cyber tools in relation to defense, make the cyber threat difficult to counter and thus represents a new and serious risk to the security of the nation-state. Others are more moderate about the reality of the danger facing us and argue against the overhyping of threat. Rid (2013) for one rejects the use of the term cyber warfare, raising the point that it has yet to result in a single casualty. In an analysis of the 2011 Stuxnet attack against Iran's nuclear program, Lindsay (2013) shows that such a sophisticated computer virus costs hundreds of millions of dollars to develop and could only have been created by a technological superpower like the United States. Providing a broad picture of the cyber threat landscape, Valeriano and Maness (2015) collect data on cyber incidents between rival states and find that only 16% have engaged in cyber conflict and the incidents that do occur generally exhibit low levels of severity.

Yet regardless of the actual danger cyber conflict represents, the perception of threat is undoubtedly very high. International Relations scholarship has long emphasized the role perceptions play in shaping the state's reaction to threat through the process of the security dilemma (Jervis 1978). A state's decision to build-up armaments is often based, as Hammond (1993) notes, "on the subjective interpretations of the actions of others" rather than on accurate information and real events. The role that psychology plays is especially important to factor into the study of the cyber domain given the fact that we have yet to witness a catastrophic computer network attack. The threats are clearly constructed as much by perceptions as by reality, and these perceptions alone are able to dramatically alter the strategic landscape (Dunn Cavelty 2012). We can therefore expect perceptions of threat to impact national security policies and the development of a state's cyber capabilities.

This research taps into the broader issue regarding the appropriate type of response to cyber security threats. The hack of the OPM in 2014, widely believed to have been carried out by China, has added fuel to the debate over how exactly the United States should respond to such acts of cyber aggression. The White House did not publicly blame China for the attack and the American response has been restrained as it seeks to avoid escalation, but at the Aspen Security Forum Senator John McCain criticized the lack of reaction and clear policy.[9] The question is whether the focus ought to be on prevention and defense or, as McCain himself advocates, hacks like that of the OPM should be considered an act of war, best met with retaliation to allow the United States to demonstrate its superior capabilities and resolve in dissuading further intrusions into its networks. There have been many calls for a firmer policy of deterrence in cyberspace, yet much less has been said about what the government can do to bolster its own defenses and to reinforce greater cyber hygiene nationwide.

The distinction between offense and defense is regularly made when discussing cyber capabilities, and much attention has been paid to the notion that the cyber domain favors the former. Offensive cyber weaponry is considered more cost effective with one military official claiming that it costs 10 times as much to defend against malware as it does to mount an offensive operation (Fahrenkrug 2012). Defensive measures on the other hand are considered to be less efficient 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).

If the domain is indeed offense oriented, it raises a challenge for the future of international security. In the traditional International Relations discourse, offense–defense balance theory predicts 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). Although there is little statistical evidence that either the perceived or actual offense–defense balance in the international system predicts militarized disputes and war (Gortzak, Haftel, and Sweeney 2005), its impact on interstate competition and arms races may nevertheless be substantial. If this is true of the cyber domain, we may unfortunately witness a greater development of offensive capabilities at the expensive of the defense, and an escalation of fear and tension within the international system. There are already signs that this proposition is becoming a reality with several media sources making claims of a "cyber" arms race[10]. Moreover, research by the United Nations Institute for Disarmament Research finds that 47 countries worldwide have begun to integrate cyber warfare units, strategies, and doctrines into their military organizational structures.[11]

The rationale behind the development of offensive capabilities as a national security policy is to send a clear message to potential aggressors of one's willingness and capacity to retaliate in the hope of deterring attacks in the first place (Huth and Russett 1990). Analysts often use this framework of deterrence theory in discussions about the use of cyber weaponry, forgetting however that the secrecy states keep over their cyber capabilities makes deterrence a problematic strategy if the goal is to make clear

[9] D. Verton, *"U.S. Cyber Policy Struggles to Keep up with Events,"* Fedscoop, July 27, 2015, http://fedscoop.com/u-s-cyber-policy-struggling-to-keep-up-with-events

[10] G. Corera, *"Rapid Escalation of the Cyber-Arms Race,"* BBC News, April 29, 2015, http://www.bbc.co.uk/news/uk-32493516

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

one's capacity to retaliate (Valeriano and Maness 2016). Furthermore, the large body of International Relations research demonstrating a link between military build-ups and the escalation of disputes (Gibler, Rider, and Hutchison 2005; Sample 1997; Vasquez 1993; Wallace 1979) suggests that confrontational policies in cyberspace will only serve to intensify cyber conflict.

There are other paths forward in improving state security, and if the fault of the Sony hack, the OPM hack, and countless other violations lies with those who run the security apparatus within states and private companies, might the first task rationally be to prepare the defenses and establish a resilient cyber industry that meets future challenges? There is a clear need in the cyber domain, no matter what perspective one has of the threat, to bolster defensive and resiliency strategies.

The benefit of cyber defensive measures, such as through the encryption of data or improved methods of threat sharing and detection, is that they cannot be seen as threatening weapons to other states, unlike the creation of explicitly attack oriented cyber warfare units. Developing offensive weapons is sure to activate the traditional security dilemma suggesting that defensive measures instead should be encouraged. The cyber security field has not adequately investigated the nature of cyber defenses in the macro-political context. The central aim of this article is to examine how states are reacting to the cyber threat both offensively and, but more importantly, in terms of defensive cyber infrastructure improvements by using the specific indicator of encrypted web servers.

Research Design

Our data analysis includes a number of techniques ranging from identifying simple bivariate associations to multivariate regression modeling. Cyber threats represent our explanatory variable in this analysis, and our aim is to measure the reaction to such fears. To gauge the level of cyber threat experienced by states we use survey data from the 2015 Pew Research Center study which asks the public their views on a range of global security issues. Alongside the other contemporary issues of climate change, economic instability, the terrorist threat from ISIS, the risk of Iran acquiring nuclear weapons, as well as the tensions regarding Russia and China and their neighbors, a sample of respondents in each of 39 countries worldwide were asked about their level of concern about the risks of "cyber attacks on government, banks, or corporations."[12] We create our threat perception variable by combining the percentage responses of those "very concerned" with those "somewhat concerned" about the cyber threat. This gauges the level of priority given to cyber threats in the population's national security concerns. The survey covers a geographically and economically varied range of countries, with the threat perception ranging from a low of 18% (Ukraine) to a high of 88% (South Korea), with a mean of 60%. Later on in our investigation, we utilize data on actual cyber incidents which allows us to make use of a larger dataset and build a regression model.

[12] Pew Research Center, Global Threats Report, July 14, 2015, http://www.pewglobal.org/files/2015/07/Pew-Research-Center-Global-Threats-Report-TOPLINE-FOR-RELEASE-July-14-2015.pdf

The offensive reaction is measured using information on which states are suspected of possessing offensive cyber capabilities. Unfortunately, because governments are highly secretive of their cyber weaponry, this is an area where data is most scarce. Some headway has been made however into documenting the cyber military organizations that governments worldwide are establishing as they prepare for engagement in the cyber warfare domain. We use the findings from one report published by the Wall Street Journal, which identifies 29 such states with "formal military or intelligence units dedicated to offensive cyber efforts."[13] Because the information comes from a media source there may be issues regarding its reliability including a potential omitted data bias if there are excluded states with offensive, albeit unknown, capabilities. This variable consequently represents only a small part of our analysis.

We are also limited to what data we can use for the analysis of levels of cyber defenses but data is available from the World Bank/Netcraft[14] on one particular indicator, that is, the numbers of web servers utilizing encryption methods in each country. The acquisition of secure internet servers is a standard cyber security measure which involves the use of Secure Socket Layer (SSL) technologies to encrypt the data being communicated between a web server and a client, which would otherwise be sent as plain text. Encryption of data adds a layer of security and makes it more difficult for sensitive information to be stolen. SSL's are therefore a service that private firms and banks as well as governments and military organizations have an interest in purchasing to improve their cyber defense against hackers.

If states are concerned about the risk of cyber attacks one way in which they may respond is to encrypt their data, but we are well aware that is only one method of cyber security and our analysis cannot shed light on the many other approaches. Good cyber hygiene practices in one area may or may not spill over to others areas but we are limited by the availability of data indicators in the cyber field and so this question remains unresolved. We are also aware that changes in the secure server variable do not necessarily signify a direct government policy as the private sector plays a major role in securing a country's networks. In this regard we are not solely testing government reaction but also of businesses nationwide. This in fact better reflects the reality of cyber incidents which are often targeted against private firms. The secure server indicator therefore also connects well with the threat perception variable which gauges the fear among the population as a whole, not just from the government.

[13] D. Paletta, et al., *"Cyberwar Ignites a New Arms Race."* Wall Street Journal, October 11, 2015, http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

[14] World bank/netcraft, Secure Servers per 1 million people, November 1, 2015, http://data.worldbank.org/indicator/IT.NET.SECR.P6

Perceptions versus the Reality of Cyber Threats

Before turning to the key question of the reaction to threat levels, we first examine the extent to which this fear is based in the reality of actual cyber incidents. Figure 1 graphs each country's victim–initiator ratio in their cyber incidents using the incidents dataset for rival states between 2001 and 2011 (Valeriano and Maness 2014) by their perception of cyber threat. This shows whether the frequency of actual cyber actions on the country has a bearing on the levels of concern about the issue.

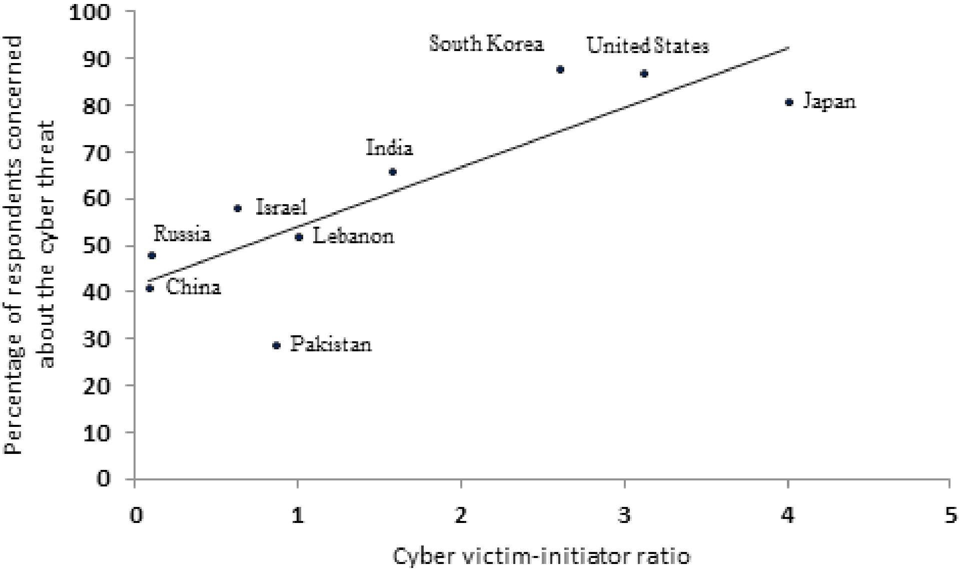

Figure 1: Cyber incidents and threat perception

There is evidently a rough correlation and positive relationship between the two variables. States like China, Russia, and Israel, which tend to be the initiator of cyber actions, have the lowest levels of threat perception, while Japan, South Korea, and the United States have more frequently been victims and consequently have greater concern about cyber actions. This would suggest that fear in the cyber domain is to at least some extent based in the reality of actual cyber incidents.

Of course, the data does not follow a perfectly linear pattern because of the other factors to consider in accounting for heightened fear. The frequent media coverage of cyber incidents for one likely serves to inflate the threat but this is a question that cannot be addressed further here. As we now go forward in investigating the reaction, we know that threat perception likely has some basis in real events with the potential to affect government and/or private sector cyber security policy.

The Perceptions and the Offensive Reaction

A worrying trend observed currently in the international system is that of states developing their offensive cyber capabilities as a means to deter cyber aggression. In its 2011 national cyber strategy, the United States sets out its goal of ensuring "that the risks associated with attacking or exploiting [their] networks vastly outweighs the potential benefits."[15] But as we know from decades of IR research, engaging in power politics as a means of deterrence is only likely to lead to counter reactions, security dilemmas, and the escalation of hostilities (Vasquez 1993). Indeed, Craig and Valeriano (2016) provide evidence that certain states are engaged in competitive cyber relationships based on action–reaction dynamics, these sorts of relationships often escalate in the conventional sphere.

Here we test whether greater cyber fear is more likely among offensively capable states as identified by the Wall Street Journal. If these developments are a reaction to the cyber threat, a correlation would be expected between threat perception and the presence of these offensive capabilities. Table 1 compares the mean level of threat perception between two groups: states that reportedly have offensive cyber capabilities and states where there is no evidence of such developments. The data sample is limited to the 49 countries included in the survey. To determine if the difference is statistically significant, a *t* test is run which tests the null hypothesis that there is no statistically significant difference in means between the two groups.

Table 1: Comparison of mean threat perception between offensive/non-offensive states

	States without offensive capabilities (*N* = 22)	States with offensive capabilities (*N* = 17)
Mean percentage of respondents concerned about cyber threat	55.6	65.7
	t = 2.16, degrees of freedom = 37, *p* = .037	

Perceptions of the cyber threat were on average 10.1 percentage points greater in the countries with offensive cyber capabilities, with a mean level of threat perception of 65.7%. The average percentage of people concerned about the cyber threat in countries that did not possess offensive capabilities was 55.6%. The *t* test gives a significant result with a *p*-value of 0.037 meaning the null hypothesis can be rejected and we can confirm that the states with offensive capabilities are statistically more likely to have higher levels of threat perception. This finding is consistent with the proposition that states are

[15] The White House, International Strategy for Cyberspace, May 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

reacting to increased threat through offensive strategies. The correlation also fits within traditional IR theory which sees military build-ups as resulting from external threats, whether perceived or real (Richardson 1960).

Nevertheless, bivariate tests like this cannot establish a causal link between the two variables, and there is always the possibility of intervening factors or a reverse causal mechanism which better explains the correlation. Neither do we know if these findings can be generalized to the entire population of states in the system due to the limited sample. Yet because the evidence fits with theory and expectations it is not unreasonable to suggest that increased levels of threat are motivating the build-up of offensive cyber capabilities. Clearly there is room for further research in this area.

The Perceptions and the Defensive Reaction

The problem comes when offensive solutions are advanced before basic defensive improvements. While the quip that the best defense is a good offense has become conventional wisdom at this point, the veracity of this statement in the world of cyber security is dubious. If states are indeed reacting to the threat by preparing for cyber warfare through offensive capabilities, the next question to ask is if states are also improving their cyber defensive infrastructure in accordance with perceived threats. While it is nearly impossible to fully protect any network, there are steps that can be taken to ensure internal cyber hygiene. One standard method of cyber security is the acquisition of secure web servers. Secure servers are those that encrypt the data being transmitted by using Secure Socket Layer (SSL) technology. The numbers of secure servers is used as our dependent variable as we measure how states have reacted to the cyber threat. The data runs from 2003 to 2014, and in this analysis we often use the standardized measure of the number of secure servers per million of the country's population to make the data more comparable between countries. Figure 2 describes the trends in the secure server data by category of economic development.

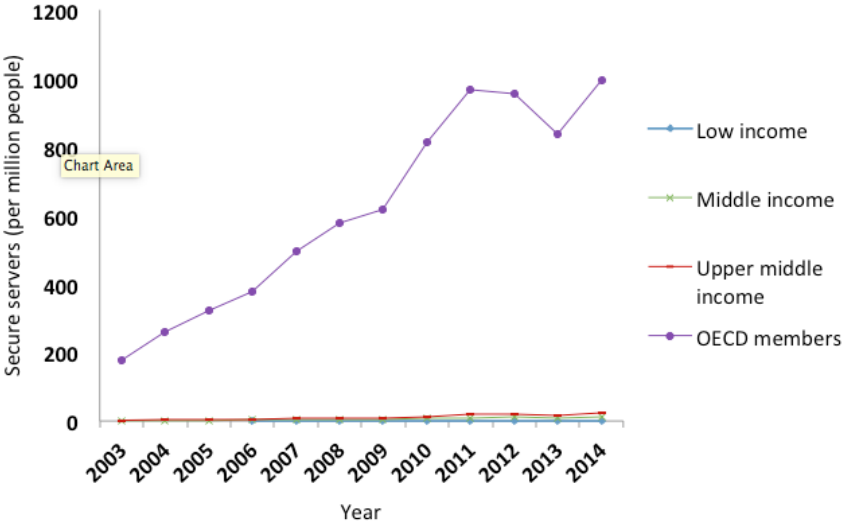

Figure 2: International trends in secure server acquisition

Numbers of secure servers have generally been on an upward trajectory due to increasing internet usage and IT infrastructure over time. What is very noticeable is that the numbers of secure servers seemingly relate to economic development, with OECD countries far exceeding less developed states in numbers of secure servers as well as in their rate of acquisition. Encryption technology is evidently more prevalent in wealthier societies where there are greater numbers of businesses with the capacity to afford such cyber security measures, as well as the more advanced levels of internet infrastructure found in developed economies generally. Poorer countries are evidently failing to catch up with the security practices of wealthier states.

As stated previously, unlike a government's move to establish cyber warfare units, increases to secure servers may not represent a direct government policy but rather a societal reaction. The data measures the number of secure servers across the whole country and so their values depend greatly on the general level of cyber security across society, including the actions of private businesses and organizations. Governments nevertheless can encourage better cyber security measures and enact legislation supporting or demanding such improvements. For example, the 2011 national cyber strategy of South Korea published in the same year as a major cyber incident from North Korea on government websites called on the public and private sectors to encrypt and back up their data.[16] This policy's potential impact is illustrated in Figure 3 which shows that the number of South Korean secure servers in relation to its population has more than doubled within a year, rising from 1128 per million people in 2010 to 2496 per million people in 2011.

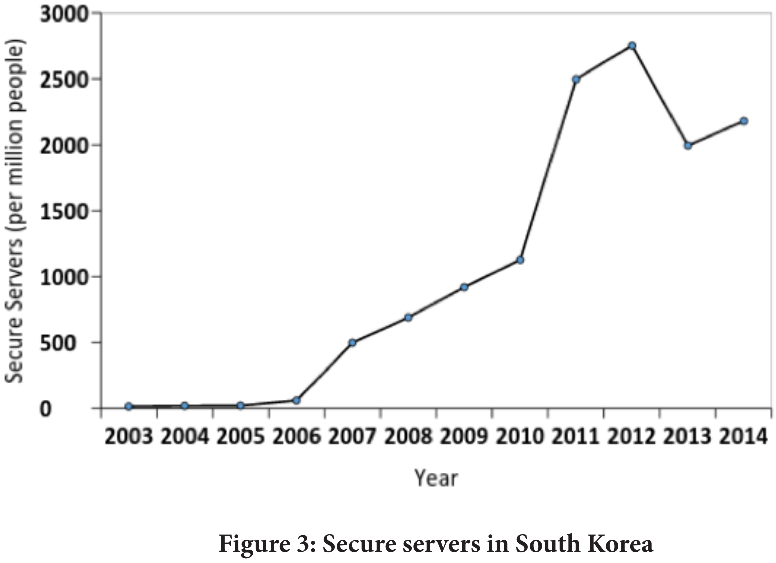

Figure 3: Secure servers in South Korea

[16] A. Schweber, *"South Korea Develops Cyber Security Strategy,"* Intelligence, August 28, 2011, http://blogs.absolute.com/blog/south-korea-develops-cyber-security-strategy/

In the following analysis we use threat perception as the independent variable and secure servers as the dependent variable. Figure 4 shows the plot of the relationship between threat perception and secure servers per million people in the year 2014, the closest available year in the dataset to the year the survey was taken.

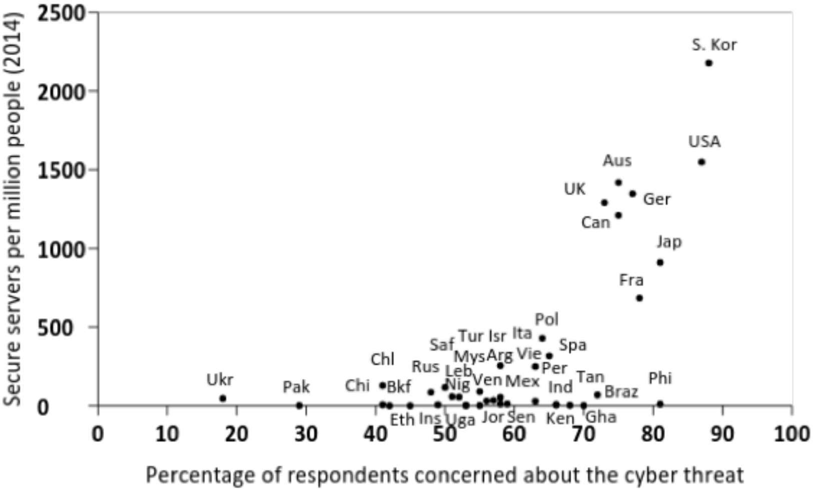

Figure 4: Threat perception and secure servers (2014)

The scatter plot suggests a weak positive relationship between threat and secure servers. States like South Korea and the United States with high levels of threat perception have many more secure servers than states like Ukraine or Pakistan with less fear of cyber attacks. Threat may not necessarily be driving secure server increases however. The relationship may work in reverse in that countries with more secure servers are attacked more frequently and therefore have heightened perceptions of threat. Because greater number of secure servers is symptomatic of a more economically and technologically developed country, such countries may be at greater risk of intrusions from outside hackers. Furthermore, a country with more secure servers is necessarily a more "connected" country with extensive networks and internet usage meaning that cyber methods will be generally more successful than if they were targeted against a less connected country. These factors are likely to result in comparably greater levels of threat perception.

As we are interested in measuring a reaction, instead of using the absolute values the average annual change in secure servers is also calculated for each country. Figure 5 shows the relationship between countries' levels of threat perception and the level at which they tend to increase their secure servers.

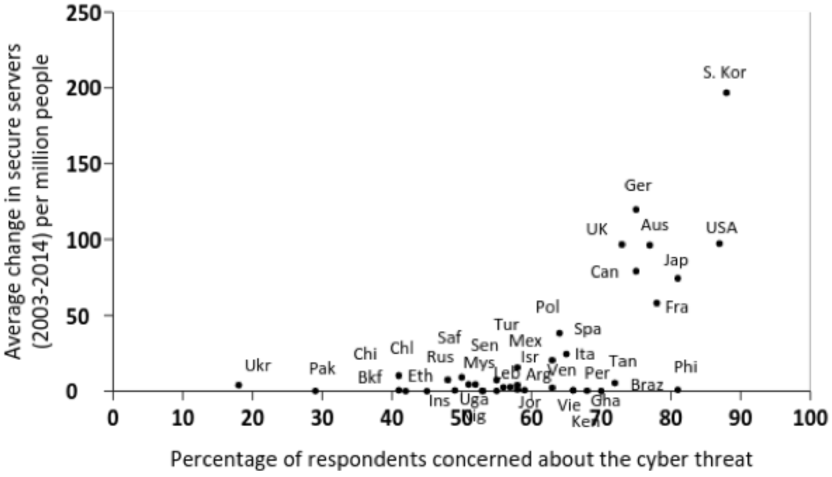

Figure 5: Threat perception and secure server change (2003–2014)

The picture is remarkably similar to Figure 4 demonstrating how closely correlated overall numbers of secure servers are with their rate of acquisition. In other words, states with more secure servers tend to increase them in larger amounts, demonstrating a growing popularity of encryption methods among the developed countries.

Figure 5 shows that larger average increases in secure servers are associated with higher levels of threat perception. At the lower end of the spectrum we see Ukraine, where cyber was a major concern for <20% of respondents and where secure servers have tended to increase very minimally. At the other extreme, South Korea has increased its secure servers by an average of almost 200 per million people in each year and has accordingly experienced the highest levels of threat. But there is evidently a split in the data sample in that for certain states the change in threat perception has no bearing on their secure server acquisition. Many of these countries in which the relationship does not hold appear to be the less developed. They may lack the resources to invest in improving their cyber security and this is a factor that even a high degree of threat perception will be unable to alter. For the more developed countries on the other hand, threat perception and secure servers seem to be more positively correlated.

Despite the relationship we cannot conclude that the threat is *causing* states to increase their secure servers and other factors may better explain the relationship. A possibility is that economic development is an intervening variable explaining both high levels of threat perception, because richer countries are more frequently targeted, as well as explaining levels of secure servers as was previously demonstrated. In other words, the correlation between fear and secure servers may not be a result of states responding to threat, but rather a result of economic development making states ripe targets whilst also being the cause of greater numbers of internet servers.

To investigate further we use an alternative survey data source to determine if the relationship still holds. In Figure 6, we use the 2014 Eurobarometer survey on cyber security[17] as the independent variable which asks respondents from the 28 EU member states their views on the cybercrime threat. We use the data on respondents who "completely agreed" that the threat of cybercrime was increasing. This is a separate question from the last source because it asks about cybercrime as opposed to cyber attacks. Our selection of EU threat data will help control for the influence of economic development as EU states have relatively good levels of development. That potential intervening variable is therefore being kept more constant. One may even expect a stronger relationship when using this cybercrime survey data because the encryption of data via secure servers is particularly applicable to issues of online theft.

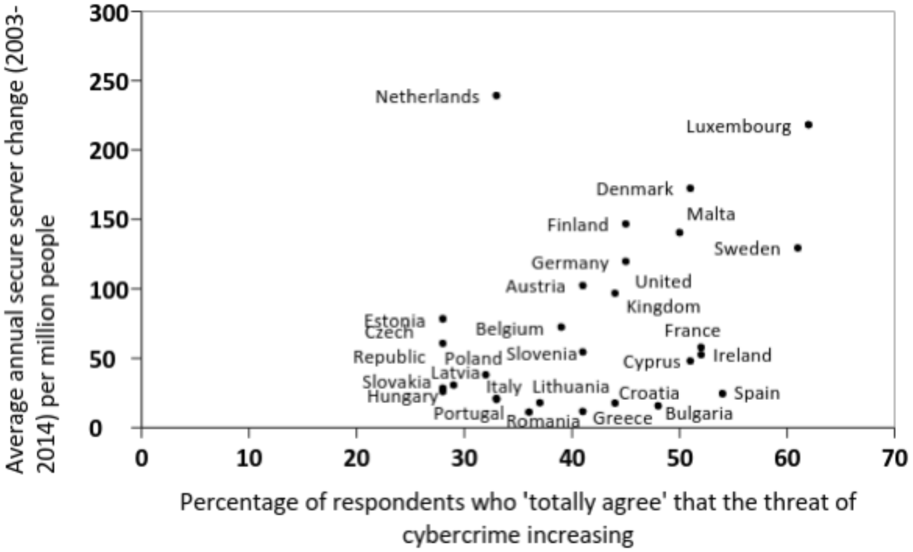

Figure 6: Cybercrime threat perception and secure server change (2003–2014)

Figure 6 highlights the weakness of the relationship between threat and defensive infrastructure developments. The data points do not follow a consistent pattern to enable us to identify a correlation. Although some states may be responding to levels of threat, many other states in the sample are evidently not doing so. Maybe this is evidence that many states and private organizations are failing to take the cyber security issue seriously. Moreover, we see states like the Netherlands, an outlier, having the highest changes in secure servers but relatively low levels of threat perception within the population, suggesting that the reasons for increasing cyber security measures are broader than simply levels of threat.

[17] European Commission, Special Eurobarometer 423: Cyber Security, February 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

We can approach our research question from another angle by operationalizing the dependent variable in terms of percentage change as opposed to absolute increases. Using percentage change will measure the increase in secure servers relative to the state's pre-existing secure servers and thus is more useful for modeling the increased effort invested into improving cyber security. It will also control for our previous finding that economically developed states tend to have larger absolute increases. Accordingly, Figure 7 plots the relationship between threat, using the original PEW data, and the average annual percentage change in secure servers from 2003 to 2014.

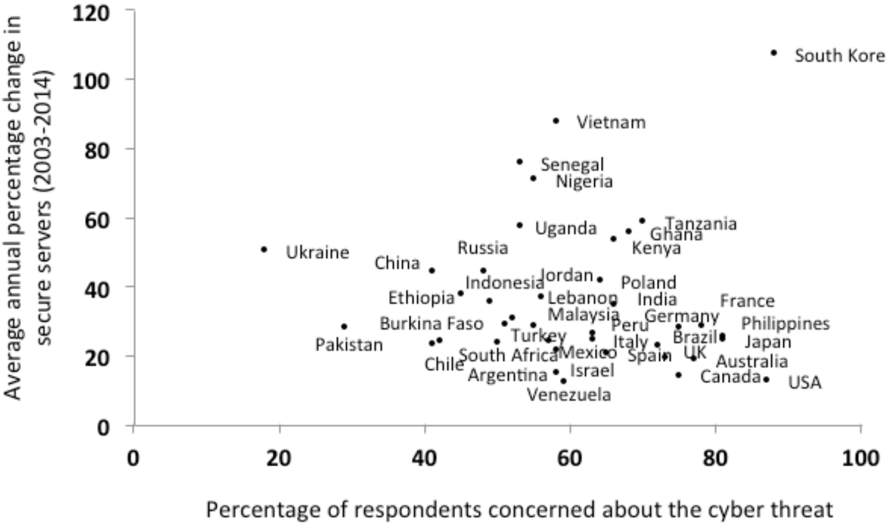

Figure 7: Threat perception and secure server percentage change

When using percentage change the results become very different. Where there was a correlation before, now there is no such identifiable trend in the data with dots widely spread. Heightened fears about cyber attacks are not associated with greater secure server growth rates. Perhaps only a few states are responding to the threat in this way such as South Korea, which in accordance to its very high perception of threat as a result of continual cyber incidents from the North has the greatest secure server growth in the sample. With 88% of respondents concerned about the threat, South Korea has on average more than doubled its numbers of secure servers each year. Yet the data shows that this certainly does not apply to the sample generally.

To analyze this further, a *t* test is conducted to ask if there is a statistically significant difference in means between two groups: states with below average secure server percentage growth and states with above average secure server percentage growth over the whole period. The results are shown in Table 2.

Table 2: Threat perception and secure server growth (2003–2014)

	Below-average secure server growth ($N = 30$)	States with offensive capabilities ($N = 17$)
Mean percentage of respondents concerned about the cyber threat	61.1%	56.4%
	$t = 0.80$, degrees of freedom = 37, $p = 0.43$	

Going against some of the previous findings, states with above average percentage growths in secure servers from 2003 to 2014 had in fact lower average levels of threat perception than states with smaller growth rates, although the result is not statistically significant with a *p*-value of 0.43. This analysis has shown that, when measuring secure servers by percentage change rather than absolute increases, there is no suggestion that threat is driving states to put increased efforts into improving their cyber security infrastructure.

Nevertheless, this does not settle the issue regarding the previously observed finding that there was a correlation between threat perceptions and secure servers. The possibility that this was explained by intervening variables was raised but this cannot be confirmed with the limited survey data we have. To gain a larger sample size with more explanatory power, we instead use data on cyber incidents (Valeriano and Maness 2014) and build a statistical model to account for numbers of secure servers. This method allows us to control for other variables in order to help isolate the independent effect that being the victim of a cyber incident has on cyber security infrastructure.

We use a panel dataset of 64 countries observed from the years 2003 to 2012 and run a fixed-effects regression model. This technique controls for country specific effects which may correlate with the independent variables. The country sample is determined by two factors. Firstly, only countries involved in ongoing interstate rivalries are included due to the nature of the incidents dataset. The second condition is that these countries must also have cyber security programs as these are the countries with the capacity to coordinate a response and are therefore of most interest when investigating the dynamics within the cyber domain. These countries are determined by the UNIDIR cyber index[18] which identifies countries with notable cyber security policy developments within their military or civilian sectors.

Our dependent variable is the number of secure servers a country possesses per one million of its population, and the three control variables included are: GDP per capita[19] in thousands of US dollars, to account for the economic development that has been previously shown to explain levels of cyber security; military spending measured

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

[19] World Bank, GDP per capita, November 1, 2015, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD

in billions of US (constant 2011) dollars[20]; and the levels of internet penetration in society, indicated by the numbers of internet users per 100 people.[21] Stronger military powers may be expected to invest more into cyber security to protect their critical infrastructure and military networks, and clearly more internet users in a country necessarily entails more servers, so these are factors that should also be controlled for.

The key independent variable is whether or not the state was victim to a cyber incident within the past 2 years of the year under observation, thereby giving sufficient time to observe a reaction. Cyber incidents data is used instead of the survey data because it provides us with not only cross sectional but time series data, thereby increasing the sample size for use in a more sophisticated statistical model. The regression will predict the effects of each independent variable on a state's numbers of secure servers while holding constant the impact of the other variables. This therefore allows us to get a better idea of whether cyber threats on their own motivate the acquisition of secure servers.

Table 3: Fixed effects regression on secure servers (2014) per million people

Variable	**Coefficient (std. error)**	***p*-value**	**95% interval**	**Confidence**
Internet users	6.75 (.95)	0.000	4.88	8.62
GDP per capita	22.69 (6.64)	0.001	9.64	35.74
Military expenditure	2.91 (1.05)	0006	0.85	4.97
Cyber victim	–16.36 (52.40)	0.755	–119.29	86.56
(Constant)	–455.35 (104.48)	0.000	–660.59	–250.11

[20] Stockholm International Peace Research Institute, Military Expenditure Data, October 27, 2015, http://www.sipri.org/research/armaments/milex

[21] World Bank, Internet Users per 100 people, November 1, 2015, http://data.worldbank.org/indicator/IT.NET.USER.P2

Table 3 shows the results of the fixed effects regression model on the number of secure servers (per million people), using a sample size of 604. The number of internet users in a country was a significant predictor of the number of secure servers. An increase of 1 internet user per 100 people is associated with 6.75 more secure servers per million people. GDP per capita is also significant, and an increase of 1000 dollars per person is associated with 22.7 more secure servers per million people. Military spending is also positively and significantly correlated with more secure servers. A 1 billion increase in military expenditure is associated with having 2.9 more secure servers per million people. Although statistically significant, these are not very large effects in real terms. The R2 value of 0.43 indicates that 43% of the variance in the data is being accounted for by the model, and there are clearly more variables to consider when trying to explain levels of encryption technology in a state.

Our key variable of interest is whether a country was a victim of a cyber incident in any of the two previous years as this might be a critical indicator of heightened awareness of the cyber threat to a state's national security. Our analysis is sufficient to show that this indicator is not a significant predictor of the number of secure servers. The relationship is negative but not statistically significant, suggesting that the previously observed correlation between cyber threat and secure servers was spurious, and better explained by other factors such as economic development.

Summary

We first provided evidence supporting the claim that states are reacting to their cyber threat concerns by developing offensive cyber capabilities. This is consistent with the cyber arms race proposition. States in which the public had greater fear of cyber attacks were more likely to be making offensive preparations. This is worrying because it suggests that the security dilemma in cyberspace is driving states toward more confrontational policies as a means to achieve security.

What would be even more concerning is if this was occurring at the expense of basic cyber hygiene domestically. We investigated this question by looking into the specific practice of securing web communications via encrypted servers. Because much of the cyber threat relates to the unauthorized access into private networks and theft of sensitive data, secure servers are an important as well as relatively basic cyber security measure. Acquisition of such technology would appear to represent the initial step that can be taken toward establishing basic levels of protection and hygiene that are needed in an internet connected society. Despite this, our statistical investigation suggests that the cyber threat whether real or perceived does not in and of itself motivate states to increase their nationwide cyber security infrastructure in this way.

Although we initially uncovered a correlation between heightened threat among a population and increased secure servers the use of alternative measurement techniques gave different results, and when controlling for other variables there was no statistically significant relationship. Overall, it appears that the acquisition of secure servers is not driven by how threatened the country feels in the cyber realm.

Despite positive albeit weak correlations between secure server increases and threat perception, it seems there may be intervening variables like economic development at play. Indeed, the regression results indicate that GDP per capita as well as military spending, and internet penetration, are more significant predictors of secure servers than past experience of cyber incidents.

Conclusion

This research has helped to provide a macro picture of cyber security practices in the global system, and how they may relate to perceptions of the cyber threat to national security. If states are indeed reacting to their security concerns through mainly offensive cyber warfare preparations, it raises worrying prospects for international relations. The escalatory potential of the global cyber arms build-up should be of great concern to scholars working on these issues. More work is needed on how the security dilemma and action reaction processes operate in this domain, as well as its implications for interstate cyber conflict.

On the other hand, we have not seen much evidence that states are taking the necessary steps to ensure their own internal protection against growing threats. Data encryption is of course only one method of protection, but we are unfortunately constrained as to what data is available. It is very possible that states are reacting defensively to the threat by other means. Future research will examine this possibly with both data sources and qualitative methods.

Attempts to boost cyber security throughout wider societal projects are difficult for governments who lack control over the private sector. Regardless of levels of threat, a lack of cooperation between governments and private business will likely hinder any substantial improvements to a country's cyber defenses. In fact, private sector-led improvements in cyber security might be more effective than government-directed efforts. Unfortunately, such questions are beyond the scope of the data analyzed here but our study nonetheless points to the idea that states, in the face of increased threats, are not doing all they can to build networks that can withstand attack in the first place.

Acquiring layers of defense is moreover only one model for a cyber security strategy, and the debate may be moving toward the concept of resilience rather than defense. Determined hackers will likely always find a way in and adopting a strategy of resilience would instead involve the ability to anticipate attacks and recover systems quickly in order to minimize damage and disruption.

Empirical research in cyber security is only in its nascent era. Our modest effort is an attempt at what we hope others in the field will seek to accomplish, which is to uncover the dynamics of cyber security processes by analyzing evidence rather than focus on the pronouncements and bluster that so often pervade the cyber domain. More considered and careful data work must be undertaken because this domain is critical. Beyond its potential military uses, the opportunity for cyber connectivity to embolden education, research, business, and commination is clear.

References

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

Craig, Anthony J. S., and Brandon Valeriano. 2016. "Conceptualizing Cyber Arms Races." *Submitted to the 8th International Conference on Cyber Conflict*. Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, June 1–3, 2016.

Diebert, Ronald. 2011. "Tracking the Emerging Arms Race in Cyberspace." *Bulletin of the Atomic Scientists* 67 (1): 1–8.

Dunn Cavelty, Myriam. 2012. "The Militarisation of Cyberspace: Why Less May Be Better." *Presented at the 4th International Conference on Cyber Conflict*, eds C. Czosseck, R. Ottis, and K. Ziolkowski. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, June 5–8, 2012.

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

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.

Gortzak, Yoav, Yoram Z. Haftel, and Kevin Sweeney. 2005. "Offense-Defense Theory: An Empirical Assessment." *Journal of Conflict Resolution* 49 (1): 67–89.

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

Hammond, Grant T. 1993. *Plowshares into Swords: Arms Races in International Politics, 1840–1991* (Columbia: South Carolina Press).

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

Jensen, Benjamin, Ryan C. Maness, and Brandon Valeriano. 2016. "Cyber Victory: The Efficacy of Cyber Coercion." *Presented at the Annual Meeting of the International Studies Association*.

Jervis, Robert. 1978. *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press).

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

Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyber Warfare 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.

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. 2013. *Cyber War Will Not Take Place* [Kindle], London: C Hurst & Co Publishers Ltd.

Sample, Susan. 1997. “Arms Races and Dispute Escalation: Resolving the Debate.” J*ournal of Peace Research* 34 (1): 7–22.

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

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities* (New York: Oxford University Press).

Valeriano, Brandon, and Ryan C. Maness. 2016. “Caution in the Cyber Realm: The Inadequacy of Deterrence Frameworks.” Presented at the Annual Meeting of the Midwest Political Science Association, Chicago, IL.

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.