Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

THE CYBER THREAT TO NATIONAL SECURITY: WHY CAN'T WE AGREE?

Forrest HARE[a,1]

[a]*School of Public Policy, George Mason University*

Abstract: In March 2009, the Organization for Security and Cooperation met for its first workshop on cyber security. Though the discussion was insightful, the representatives to this workshop could not reach unanimous agreement regarding the important cyber security issues on which the forum should focus. For example, some representatives believed there is a looming arms race that must be countered while others were most concerned about mounting cyber crime. As the threat from a multitude of actors in cyberspace increases, why is it difficult to reach consensus on the most pressing threats to national security? This paper postulates that different national agendas and different technology levels amongst the world's nations will lead to different prioritization of the cyber security threat. Using the Barry Buzan vulnerabilities framework, this paper will explore how countries may be driven to prioritize potential cyber threats differently. This paper concludes that, unless these national differences are accounted for, concerted international efforts to improve inter-country cooperation will be met with confusion, at best, and resistance, at worst, on the part of national, international, and private sector stakeholders.

Keywords: cyber security, security studies, neorealism, security alliances

[1] Corresponding Author: Forrest Hare; E-mail: fhare@gmu.edu.

INTRODUCTION

"…the term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security."

Arnold Wolfers (1952)

In March 2009, government experts from the Organization for Security and Cooperation (OSCE) met in Vienna for the organization's first workshop on cyber security. Though the discussion was insightful, the representatives to this workshop could not reach unanimous agreement regarding the important cyber security issues on which the forum should focus. For example, some states arrived with the message that there is a looming cyber arms race that must be countered (Streltsov, 2007); but official statements suggest that most attendees were primarily concerned about mounting cyber crime and collaborating on security measures (Vershbow, 2009). The debate over cyber security priorities is not limited to the OSCE. Nor is there agreement that cyber security threats constitute significant risks to national security. Some influential researchers providing analyses for their governments downplay the significance of many of the alarming cyber scenarios to national security (see, for example, Libicki, 2009; Cavelty, 2007). In spite of this, the United States has publicly stated in a recent cyber policy review that existing vulnerabilities in cyberspace "have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests (Obama, 2009)." So if most advanced and advancing nations consider cyber security important to their nation, why is it difficult to reach consensus on the most pressing threats in cyberspace to national security? In this paper, I argue that differing endowments of national power and socio-political cohesion amongst the world's states will lead them to characterize and prioritize cyber security threats differently. The divergent perspectives that result will impede any efforts to reach consensus on actions to counter existing cyber threats. An important first step to gaining consensus is understanding these perspectives.

The paper will begin with a discussion of the place of cyber security in the larger debate of security issues. It is important to begin placing cyber security in the context of national security matters since the issues are most often relegated to technology debates. In this section I will argue that cyber threats can be viewed as national security matters and therefore should be relevant to the security studies field and should be analyzed using security studies theories. The section concludes with a presentation of the Buzan framework for categorizing vulnerabilities taken from his book, *People, States, and Fear (1991)*. The Buzan framework classifies several potential threats to national security as viewed by different types of states. In the section that follows, I will attempt to extend the Buzan model to cyber security issues. The categorization will be illustrated with recent examples of statements by national leaders and organizations. Lastly, I will address several implications these divergent national viewpoints have on policy formulation.

1. CYBER SECURITY AS NATIONAL SECURITY

In this section, I will place cyber security in the greater field of security studies. To do so, requires an assessment of the securitization process and how cyber threats have been securitized by a diverse set of stakeholders. The goal of this section is to demonstrate that cyber threats may be considered national security issues and therefore, theories from the security studies field, specifically the Buzan vulnerabilities and threats framework, can be applicable to cyber security research and policy.

In his seminal article, '"National Security" as an Ambiguous Symbol', Arnold Wolfers (1952) asserts that the decision to classify a threat as being one to national security, and the measures that will be taken, are political decisions, not technological or legal. Buzan et al (1997), writing half a century later, delved more deeply into the process of moving a political agenda into the forefront of security – process they call, "securitization." In other words, when an issue is presented as posing an existential threat (usually to the entire nation-state) such that it requires emergency measures (those that go beyond normal political actions), then it is being securitized (Buzan et al, 1997). Therefore, a threat, victim, and understanding of the threat to the victim, are all required to engage in the process. In cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states. The potential victims at risk from these threat vectors are also diverse. The threat actors may be in the business of stealing personal identities to commit fraud that, in the inter-connected world of cyberspace, would make all individuals in a nation potential victims. Or the threat actors may be conducting industrial espionage. In the case espionage, the direct victims are the target companies, but if the stolen information is the plans for a new fighter aircraft, the taxpayer may again be considered a victim. In cases where the identified victim is the state and its institutions, the existential threat may be one of toppling the regime or one from break-away sections of the country. In cases where individual citizens face an existential risk to their welfare, either directly or through a loss of state institutions, a justification for public action can be made because national defense is considered a public good. Politicians are therefore motivated to securitize threats to individual citizens because they are charged to represent their constituents' interests.[2] Ultimately, several potential threats to many differ-

[2] And, of course, the politician will lose their office if they don't represent their constituents' interests.

ent stakeholders can exist in cyberspace. One can appreciate that broad arrays of threat actors, and broader consideration of potential victims can lead to a variety of securitization attempts.

The ambiguous nature of national security in cyberspace also contributes to the debate about the scope of national security within the academic field of security studies. On one end of the security studies spectrum sits the neorealists. The neorealist view is championed by Stephen Walt of the Kennedy School. In an effort to form clear boundaries and ostensibly foster objective analysis, Walt (1991) contends that security studies should focus on the "phenomenon of war" as conducted by military powers under the political control of state actors. He would also include other issues of statecraft directly related to military affairs, such as arms control and crisis management, because they influence the potential for and character of war (Walt, 1991). Most likely, neorealists would argue against expanding the security studies agenda to include cyber security as long as there is still debate about the true impacts of cyber attacks to a nation's physical security, and to its military capability (for discussions of this debate, see Cavelty, 2007; Kelly & Fitzgerald, 2009; Libicki, 2009).

Researchers associated with the Danish Peace Research Institute, such as Barry Buzan, and Ole Waever, occupy the other end of the spectrum from the neorealists. Their view of security studies accepts a much broader, and deeper agenda. For example, they recognize security threats as emanating from military and political actors, but they also highlight the potential for economic, societal, and ecological threats to national security (Buzan, 1991). In addition, the referent object being threatened can encompass any actor from the individual to international level, including such actors as corporations, nations, states, and communities (Buzan et al, 1997). In this sense, cyber threats would clearly constitute security issues for a referent object even if the actor is an individual and the existential threat is a threat of economic ruin.[3]

The neo-realists and other security studies experts would not agree on the place of cyber security in the field, it is clear that states have decided there is a cyber security component to national security. As long as representatives of nation-states continue to securitize cyber threats in speeches and proposals, we must consider the role that these issues play in national security, and many academics in the field would agree. As Krause and Williams (1996) argued in their attempt to reconcile the competing academic view points, even if we are to focus on the emergency measures of nation-states, we must understand the "why" aspect of securitization. Often the "why" aspects of national security deal with the security views of stakeholders at the non-state level, and threats that emanate from non-state actors. This pertains to cyber security as well. As many authors have argued, nation-states do not hold the

[3] Neorealists would have critiques for all these points, but space does not allow for a continuation of the exchange.

monopoly on malicious capabilities in the domain (see, for example, Kramer, Starr, & Wentz, 2009). In addition, a cyber threat has the potential to span all levels of security very quickly based on the speed with which actions can occur and based upon our inter-connectedness in the domain. In a nod to the neorealist, the states most play a central role in addressing cyber threats to national security because they remain the actors with the power, and authority, to improve defenses against most existential cyber threats. While it is true the private sector actors in most countries are critical to security in cyberspace, as Krause and Williams (1996) have stated, "there can be no security in the absence of authority (p. 232)."

Having argued that cyber threats can be analyzed from the perspective of security studies, I will now present a framework for assessing the different perspectives on cyber security vulnerabilities, based on the characteristics of the state, taken from this field. This framework was originally presented in Buzan's oft-cited book, *People, States, and Fear* (1991). To construct this framework, Buzan focuses on two key aspects of nation-states—power and socio-political cohesion. Power (or weakness) can be assessed relative to the military capabilities commanded by other states in the international system, specifically, neighbors and great powers (Buzan, 1991). Most often, weak powers must specialize their economies in order to prosper, but this specialization does not completely reduce vulnerabilities. States that do not exhibit strong socio-political cohesion are vulnerable to threats to the idea of the state, its institutions and even its territorial integrity (Buzan, 1991). Buzan recognizes the difficulty with absolute measurement of either these two factors. Therefore, this model is most effective when restricted to a comparative analysis of states relative to others in the international system. The resulting combinations of national power and socio-political cohesion, with which to assess the relative importance of threats from the perspective of the state, can be depicted in a simple matrix. Table 1 depicts the four possibilities such a model presents.

Table 1. Vulnerabilities and Types of States (taken from *People, States, and Fear* (1991))

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threat (less inclined to characterize issues as military)

Weak powers that also experience weak socio-political cohesion (P-W/SC-W) will obviously be the most vulnerable to all threats to their security at all levels and from all sectors. When such states contain resources that are of value to others, they are mostly likely under constant threat that will further exacerbate their developmental challenges (Buzan, 1991). Equally straightforward is the situation confronted by strong powers that are also socio-politically cohesive (P-S/SC-S). According to the Buzan model, such states have far fewer vulnerabilities, making it more difficult for stakeholders to successfully securitize their security agendas. In other words, even stakeholders in P-S/SC-S states will attempt to securitize issues for a host of reasons; however, the action is only successful if the collective state accepts the implementation of emergency, extra-political, or extra-legal, measures to respond to the threat (Buzan et al, 1997). In such a state, the regime faces more resistance to such measures from the populace.

States along the opposite diagonal, bottom left to top right, may have greatly divergent views of security threats. The bottom left category demonstrates the priority of states that have relatively strong militaries, but relatively less socio-political cohesion (P-S/SC-W). According to this model, these states are most concerned about the threats posed to the state's ability to maintain control over the populace. As Buzan (1991) states it:

> *"Weak states, and those with narrowly cast ideological orthodoxies, will be impelled by their domestic conditions to push the qualifications for threats to have 'national security problem' status down towards the low end of the threat spectrum. When political threats dominate, the national security agenda can become very wide-ranging indeed (p. 115)."*

Such a condition can easily lead to the continuous imposition of emergency measures and authoritarian regimes.

States in the top right quadrant have a fundamentally different perspective of their vulnerabilities to national security threats. According to the model, these states are characterized by their inability to generate significant military power but they have established strong socio-political cohesion within their borders (P-W/SC-S). Examples of such states might be small European countries and the Tigers of Asia. Since these states have stable, robust institutions, they are much less concerned about political and ideological threats to their existence. However, P-W/SC-S states are acutely vulnerable to their neighbors' military power. Limited resources may force such states to specialize economically, but this specialization makes their security situation no less fragile.

Obviously, this framework is not designed to comprehensively classify all types of states, nor depict all the potential threats against which a state will consider itself vulnerable. As stated earlier, all analyses of state behavior within the international system can only be assessed relative to other states. However, the model's coarse classification allows the researcher and policymaker to understand the intersections of two polemics, regarding power and socio-politics, and how these characteristics potentially influence the security agendas of many states. This framework provides a compelling starting point when assessing the securitization actions of states both internally and in international forums. Perspectives and prioritization of security threats vary most markedly from the bottom left quadrant to the top right. In addition, states in the bottom right and top left quadrants may share perspectives of states in the top left and bottom right quadrants depending on the nature of the threat, and their relative vulnerabilities to the threat, at any given time. For example, a P-S/SC-W state may find support from P-W/SC-W states for justifying measures to combat ideological threats if both are sensitive of a minority's separatist agenda, even if the states do not have common ideologies or the same minority. In international engagements, P-W/SC-S states may find support for the relative prioritization of certain threats against critical infrastructure, if not the magnitude of the threat, from P-S/SC-S states. Clearly, any efforts toward consensus views on security issues will be met with structural resistance. We should expect cyber security to be no different.

2. SECURITY STUDIES APPLIED TO CYBER SECURITY

As argued earlier, the potential for existential threats to states' and individuals' security can exist via cyberspace. Therefore, cyber security can be viewed from the standpoint of national security. It then follows that models used to understand national security should also be applicable to studying cyber security issues. In this section I will present a possible construct for such an application.

Whereas the Buzan framework was developed for security issues in general, Table 2 depicts potential ways that various nation-states would securitize their vulnerabilities to cyber threats.

P-W/SC-W: According to this model, states that fall into the top-left quadrant will be concerned about most all types of threats that can occur in cyberspace from destabilizing political web forums, to attacks on any Internet infrastructure, to criminal actions that can quickly undermine their financial systems and citizens' welfare. The government institutions in such states most likely lack expertise both on how to secure their IT systems, but also to understand the true extent of the threats the face. Some threats may be much more substantial than government officials may anticipate, such as their vulnerability to e-government website hacks. Other threats, in that they are difficult to quantify due to animosity and ambiguity, may lead to a heightened fear of the unknown. For example, a statement made by the Georgian National Security Council chief, Eka Tkeshelashvili, at 2009 GovSec Conference characterized computer scientists in a foreign nation as "soldiers" who worked with other non-governmental "mercenaries" in a concerted cyber attack on her country (Shachtman, 2009). Such statements can be analyzed to find evidence for how cyber threats are be securitized by a P-W/SC-W state.

Table 2. Cyber Vulnerabilities and Types of States

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDOS and other major attacks on critical infrastructure*
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

* A distributed denial of service attack, or DDOS, occurs when many computers, usually surreptitiously controlled, are used to inundate a web server with requests and cause it to become overwhelmed to the point that service is denied.

P-S/SC-S: Moving on the diagonal from the top left to bottom right quadrant, P-S/SC-S states have the ability to maintain stronger military and economic forces within the international system, and are therefore most reluctant to securitize threats in cyberspace at the same level they have for more conventional threats. Because they recognize that would-be adversaries can potentially hold their critical infrastructure at risk in cyberspace, there has been substantial writing on this potentiality in many technologically advanced countries (see, for example Kramer et al, 2009; Cavelty, 2007; Arquilla & Ronfeldt, 1998). Absent a significant attack, the true extent of vulnerability is difficult to measure. As a result, few states have effectively securitized these vulnerabilities to the degree they have securitized conventional military and terrorist threats. For example, no states in this category have begun to heavily regulate cyber security in critical infrastructure sectors (Assaf, 2008; Brown, 2006). In these states, cyber security typically remains a responsibility of the private sector owner-operators.

As discussed earlier, P-S/SC-S states are technologically advanced relative to those in the top left quadrant. They also have larger economies and therefore rely heavily on cyberspace for financial transaction and the development of intellectual property. Because the value of information and finances that are stolen in cyberspace can be directly measured, stakeholders in these economic sectors may have more success securitizing their vulnerabilities. For example, though it did not explicitly list crime as the most significant cyber threat, the cyberspace policy review (2009) conducted by the Obama administration stressed at several points the need to improve international cooperation on information and finance protection issues. It states, " the United States should accelerate efforts to help other countries build legal frameworks and capacity to fight cyber crime and continue efforts to promote cyber security practices and standards (p. 33)." In addition, none of the recommendations in the report support the enactment of emergency, extra-political measures to improve national security.

P-W/SC-S: In a conventional sense, P-W/SC-S states are vulnerable to most threats of military force because their infrastructure and population are highly-susceptible to military attacks. Small countries that have strong socio-political cohesion are often highly developed countries that have made the full transition to e-governance. Citizens may now be dependent on cyberspace for every day life. As these countries have advanced technologically, their infrastructure has become inter-linked and inter-dependent through this medium. This advancement has made such systems equally vulnerable to cyber attacks. However, such countries may find it difficult, either physically or financially, to develop the redundant capabilities and bandwidth that would be required to withstand concerted attacks on their cyber infrastructure. Such states would therefore be most inclined to securitize the threat of DDOS and other major cyber attacks on critical infrastructure. As a result, P-W/SC-S states are most interested in developing strong security measures that will make their infrastructure systems less vulnerable to cyber attacks, as well as supporting international efforts that will categorize cyber attacks on their infrastructure as threatening as physical attacks. A recent strategy report by the Estonian Ministry of Defence contains statements that could be used as evidence for this focus of securitization. For example, the top cyber threat identified in this strategy is attacks against critical infrastructure (Estonia, 2008). The only other threat this report identifies is the threat of cyber crimes committed for financial gain.

P-S/SC-W: As stated earlier, countries that are militarily powerful, yet lack strong social-cultural cohesion within their borders, tend to securitize the threat of de-stabilizing rhetoric emanating from within its borders, and from hostile parties abroad. Cyberspace has now vastly increased the challenge for central regimes that desire to control the spread of information they consider subversive. For one, it allows greater anonymity to those who would publish the rhetoric. Second, the spread of cyberspace allows for much quicker communications. And third, it links communities both within and outside of a country. This increased linkage facilitates alternative interpretations of internal events for the international community. Because the tools of messaging are open to all, the bar is raised for P-S/SC-W. Such states see the spread of cyberspace and the influence of the Internet as de-stabilizing to their efforts to improve social-cultural cohesion and maintain existing state institutions. Accordingly, these countries would be most interested in enacting measures that will justify greater control of information flowing through cyberspace, both within their sovereign territories and to the international community. An article by Streltsov (2007), a member of the Russian delegation to the UN Group of Governmental Experts to a cyber security meeting in 2004, contains extensive language regarding his country's concern for socially de-stabilizing actions in cyberspace. For example, he identifies threats that "undermine a state's economic and social systems and psychological manipulation of a population for the purpose of destabilizing society (p. 8)," as ones that require international efforts to combat. In fact, his government stresses the concept of "information security" above "cyber security." According to Streltsov (2007), the idea of information security concerns threats such as; "spreading disinformation or creating a virtual picture partially or totally misrepresenting reality in the communications sphere; or producing disorientation, loss of will power or temporary destabilization among the population (p. 7)." These are clearly threats of a political nature that would conform to the Buzan model as being representative of a P-S/SC-W state's desire to maintain internal cohesion.

As with conventional threats, states in different quadrants may form cyber "securitization alliances." For example, the Estonian cyber security strategy highlights many of the same threats that the US cyber policy review identified. It is possible that these two nations, when discussing issues in international forums, may support each other's efforts to securitize specific threats such as cyber crime. Also as with conventional threats, perspectives and prioritization of security threats would be expected to be most divergent from the bottom left quadrant to the top right. According to this model, P-W/SC-S states would not prioritize the threat from the spreading of disinformation as highly as a P-S/SC-W state relative to the threat from attacks on critical infrastructure. Therefore, one would expect little, if any, agreement between states in these two quadrants during international forums on cyber security issues regardless the unique relationships between the states.

The discussion above might suggest that I have categorized specific countries according to this model. On the contrary, I will not do so in this paper for two reasons. First, the statements used as example evidence were merely intended to show representative acts of stakeholders securitizing particular cyber threats. Though they were from official sources, they were not meant to suggest that the states these actors represent are necessarily representative of a specific quadrant, nor that the cyber threat highlighted in the statement is always the most important one from their state's perspective. This is not to say that future research could not gather empirical evidence to conduct such an analysis. Secondly, the dynamic nature of cyberspace makes it probable that countries will find themselves shifting between the quadrants in the matrix. For example, a country that is normally considered to be socio-culturally cohesive may abruptly find its state in a weak position because a de-stabilizing influence on the Internet, such as a video of police attacking students, spreads quickly through cyberspace. Or, a country that is normally considered to have weak socio-cultural cohesion may confront a military threat that improves their cohesion, but places their cyber infrastructure directly at risk. This combination would lead to a prioritization of threats that is characteristic of the right-hand column. Any useful analysis from a public policy standpoint must account for how these dynamics influence international interactions on cyber security.

3. PUBLIC POLICY IMPLICATIONS AND CONCLUSIONS

All securitization acts are conducted to support an agenda for public or state-directed action. In this section, I will address two ways this model could support public policy formulation and analysis. First, I discuss how the framework can help policymakers understand and reconcile competing policy agendas that result from securitization of cyber threats. Then I postulate how the divergent perspective of cyber security threats from Table 2 may impact existing security alliances.

Policy analysts and policymakers are often confronted with recommendations for public action that seem to be contradictory, or at least in some way conflicting, when presented side-by-side. For example, one stakeholder may argue for a test ban to halt the development of "cyber weapons" while another may call for greater funding for cyber forensic analysis. For international organizations, such as the UN or NATO, proposals may be assessed without a complete understanding of how or why the threat leading to the proposal had been securitized. The model in this paper based on the Buzan vulnerability framework, can support cyber security policy formulation and coordination in at least two ways. First, using the model to assess the underlying assumptions and overall security agenda of relevant state actors can add needed perspective to an analysis of competing cyber security proposals. In addition, a wider acknowledgment and understanding of the assumptions behind the cyber security agendas of state actors and other stakeholders may reduce the potential for security or defense dilemmas in the cyberspace.

Ultimately, nation-states have two options to reduce their insecurity; they can either make themselves less vulnerable to security threats, or attempt to prevent or lessen perceived and real threats (Sundelius, 1983). There is no clear principle that supports efficacy of one policy direction over another. Even if all stakeholders agree that a threat should be securitized, it does not guarantee agreement on the correct response to the threat. Strong arguments can be made for taking either, or both routes. Wolfers (1952) provided a useful illustration. If one nation had a policy to maximize its security by relying on armaments and alliances, while another did so based on maintaining strict neutrality, "a policymaker would be at a loss where to turn (Wolfers, 1952, p. 490)." In cyberspace, there are many proposed solutions to addressing a wide array of threats. For example, Libicki (2009) concludes in his recent monograph, Cyberdeterrence and Cyberwar, that the best way for the US military to improve cyber security is by improving computer security measures. This solution may be likened to the position of maintaining strict neutrality. Streltsov (2007) argues that the international community should forbid the use of information and communications technologies that are used to damage critical infrastructure. This solution is akin to arms control policies and treaties. Finally, a 2008 study to prepare the new US president to address cyber security challenges recommended strong federal oversight of both governmental and private actions (while being careful to highlight civil liberty issues) (Lewis, 2008). These, and other policy agendas by state and non-state stakeholders are all based on securitization of particular cyber threats. Disagreement of the feasibility of these recommendations is compounded by disagreement on the significance of underlying threats. As stated above, important first step toward consensus on policy measures is to understand and try to rectify the disagreements on the securitization acts behind the policy proposals. The framework presented in this paper is a tool that can be used to assess the underlying cyber threats and how each stakeholder sees them as being significant. For example, Libicki's proposal to rely on network security to combat cyber threats is a practical proposal if the object of interest, in this case, the US military, is not vulnerable to political threats. According to the framework, this proposal would probably not meet with widespread acceptance in international forums where other participants consider political threats in cyberspace to be significant. Policymakers must recognize these influences before expending unnecessary diplomatic energy on their policy agendas.

Another concern that stems from differing perspectives on the significance of cyber threats is the potential for a security dilemma in cyberspace (Hare, 2009). As characterized by Herz (1950), a security dilemma may arise as one nation's efforts to arm themselves in defense may provoke another nation to do likewise, thereby creating a greater threat. Since it is much more difficult to make public or confirm the defensive nature of cyber security measures, other states may characterize any actions as potentially hostile. Differing perspectives on the significance of cyber threats will compound these misperceptions. For example, investments in technologies to secure e-governance sites and information forums may not be seen as threatening by states that do not consider themselves vulnerable to political threats. However, P-S/SC-W states may interpret these measures as preparations for information attack purposes and therefore feel threatened by them. For this reason, it is important for one state to be aware of differing perspectives on cyber security in order to understand how other states will perceive their cyber security measures.

The existence of differing perspectives of cyber security based on the framework presented in this paper may have interesting, yet counter-intuitive implications for cyber defenses within a security alliance. In their analysis of the NATO security alliance from an economic perspective, Olson and Zeckhauser (1966) addressed the traditional complaint that larger countries bear a disproportionate burden of providing for the alliance's defense. Collective action theory suggests that larger nation's place a greater value on the alliance while smaller nations tend to free-ride. In their study, the authors discover that when there is a decline in the strength of the alliance, expenditure on defense goes up amongst the smaller nations. The result is that, as long as the alliance holds, the overall expenditure may come closer to the optimal level (Olson & Zeckhauser, 1966). This observation has implications for cyber security within a security alliance as well. If the member nations of the alliance have different perspectives on cyber security based on Table 2, they will have difficulty agreeing on how the alliance should work together to defend against cyber threats. Some states will assert that they must work together in the areas of law enforcement and not consider military response actions to cyber attacks. Others may lobby for collective military responses if they consider threats to their infrastructure to be existential. In the absence of concurrence, each member state will be required to create their own strong cyber defenses against all potential threats they consider existential. Therefore, as long as the alliance generally holds in the face of a concerted attack across the alliance, the lower level of cohesion may actually improve the defensive response. Due to the inter-connectedness of states and reduced relevance of geography in cyberspace, on state cannot provide a security umbrella for the entire alliance. In fact, one should assume that all states are equally at risk in cyberspace and therefore require their own defenses of their critical cyber systems. At the same time, an unsuccessful defense in any one nation may have a significant impact on the entire alliance. As a result, it is possible this counter-intuitive outcome of differing security agendas may improve the defenses of all nations in the alliance.

In this paper, I have argued that threats in cyberspace can be viewed as concerns for national security. However, as with all issues of national security, multiple perspectives must be expected. This paper introduced a framework, based on work by Barry Buzan of the Copenhagen School of Security Studies, with which to assess divergent and complimentary perspectives of vulnerability to threats in cyberspace. This framework incorporates a consideration of both military power and socio-political cohesion in order to understand what threats may be considered threats to national security. While the model was not tested empirically, it does suggest that states in each quadrant of the matrix may not support policy agendas of states in other quadrants with divergent perceptions of their vulnerabilities in the domain.

As with all collective action at the international level, a coalition of diverse actors must be built in order to make progress toward the collective good. Therefore, the model can be useful to identify areas of consensus between different states. The coalition may begin with a small "securitization alliance" and then expand to include others that are not completely aligned, but can find common ground in an effort to achieve a measure of progress. Once states in three of the four quadrants have joined in the coalition, they may encourage commitment from actors with the most divergent viewpoint. For example, this may be one strategy to bring the P-S/SC-W and P-W/SC-S states together on a security agenda they would otherwise not desire to support. But as long as states within the international system occupy all four quadrants, any international efforts toward greater security in cyberspace must contend with divergent security agendas based on differing prioritization of the multitude of threats in the medium.

REFERENCES

- Arquilla, J., & Ronfeldt, D., 1998. Cyberwar is Coming! In G. Stocker & C. Schoepfer (Eds.), *Infowar* (pp. 24-50). New York: Springer Verlag.
- Assaf, D., 2008. Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection, 1,* 6-14. doi:10.1016/j.ijcip.2008.08.004
- Brown, K., 2006. *Critical Path*. Fairfax, Virginia: Spectrum Publishing Group.
- Buzan, B., 1991. *People, states, and fear: The national security problem in international relations* (2nd ed.). Boulder: Lynne Rienner.
- Buzan, B., Wver, O., Wilde, J. D., & Waever, O., 1997. *Security: A New Framework for Analysis*. Lynne Rienner Pub.
- Cavelty, M. D., 2007. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (1st ed.). Routledge.
- Estonia., 2008. *Cyber Security Strategy* (Committee Report). Tallinn, Estonia: Ministry of Defence.
- Hare, F., 2009. Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield:Perspectives on Cyber Warfare,* Cryptology and Information Security. Tallinn, Estonia.
- Herz, J. H., 1950. Idealist Internationalism and the Security Dilemma. *World Politics, 2*(2), 157-180. doi:10.2307/2009187
- Kelly, J., & Fitzgerald, B., 2009. When a Cup of Coffee Becomes a Soy Decaf Mint Mocha Chip Frappuccino. *Small Wars Journal*. Retrieved January 31, 2010, from http://smallwarsjournal.com/blog/2009/09/when-a-cup-of-coffee-becomes-a/
- Kramer, F. D., Starr, S. H., & Wentz, L., 2009. *Cyberpower and National Security* (1st ed.). Potomac Books Inc.
- Krause, K., & Williams, M. C., 1996. Broadening the Agenda of Security Studies: Politics and Methods. *Mershon International Studies Review,* 40(2), 229-254.
- Lewis, J., 2008. *Securing Cyberspace for the 44th Presidency* (Commission Findings) (p. 72). Washington, D.C.: Center for Strategic and International Studies. Retrieved from http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=5157
- Libicki, M. C., 2009. *Cyberdeterrence and Cyberwar*. RAND Corporation.
- Obama, B., 2009. Cyberspace Policy Review. Executive Office of the President. Retrieved from http://www.whitehouse.gov/cyberreview/documents
- Olson, M., & Zeckhauser, R., 1966. An Economic Theory of Alliances. *The Review of Economics and Statistics, 48*(3), 266-279.
- Shachtman, N., 2009). Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It. *Wired*. Retrieved from http://www.wired.com/dangerroom/2009/03/georgia-blames/
- Streltsov, A., 2007. International information security. *Disarmament Forum, 3,* 5-14.
- Sundelius, B., 1983. Coping with structural security threats. In O. Hoell (Ed.), *Small States in Europe and Dependence*. Wien: Austrian Institute for International Affairs.
- Vershbow, A., 2009. *OSCE: Building a Europe Whole, Free and at Peace*. Washington, D.C. Retrieved from http://www.csce.gov/index.cfm?Fuseaction=Files.Download&FileStore_id=1531
- Walt, S. M., 1991. The Renaissance of Security Studies. *International Studies Quarterly, 35*(2), 211-239.
- Wolfers, A., 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly, 67*(4), 481-502.