Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?

Forrest HARE[a,1]
[a] *School of Public Policy, George Mason University*

Abstract. The new US administration has begun efforts to securitize the substantial problems the United States is currently facing in cyberspace. Recently, President Obama ordered his National Security Council to conduct a rapid review of existing measures being undertaken by the federal government, and provide recommendations for additional ones. Many stakeholders in the US government and private industry are watching these actions closely as there seems to be broad acceptance that the issues call for more extensive security measures. However, many issues will complicate effective securitization of threats in cyberspace. For example, not all stakeholders agree on the priorities or where the focus of security measures should be yet cyber security is a "trans-sovereign" issue affecting both developed and developing countries in an interdependent manner.

Because actors in cyberspace enjoy relative anonymity and can threaten inter-connected targets around the globe, there is considerable debate as to whether the concept of borders is relevant to the challenges of cyber security. Regardless the focus of the debate, the concept of borders is important because they define the territory in which national governments can employ sovereign measures. To analyze borders in the context of cyber security, this paper asks the question, "Is there an important role for the concept of borders, if not physical lines, in improving national security in cyberspace?" To explore the question, the paper takes two approaches. The first is a comparison of the cyber security issues to international drug trafficking in an effort to explore how sovereign measures used to combat drug trafficking may be applicable to improving cyber security. The second approach is an examination of the issue from the perspective of the Heal and Kunreuther Inter-Dependent Security Model with an attempt to inform the cyber security decision process of national governments as they consider options to invest in a higher level of security.

The paper will argue that, whether the problem is addressed from the standpoint of criminal behavior like drug trafficking, or cyber attacks in an interdependent, global domain, borders can be a potentially useful construct to address cyber security issues and inform national policy decisions, regardless of the physical location of relevant nodes. However, sovereign powers must be careful not to use the concepts of borders to curtail the progress our nations have made to connect and better the world via this evolving and expanding environment.

Keywords. Cyber Security, borders, agent-based modeling, interdependent security model

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

Introduction

In the United States, there have been multiple initiatives to raise awareness and securitize the nation's vulnerabilities in the medium of cyberspace[2]. Many stakeholders in the US government and private industry are watching these actions closely as there seems to be broad acceptance that the issues call for more extensive security measures. Two initiatives are noteworthy- the Congressional Commission on Cybersecurity for the 44th Presidency, and the Obama administration's 60-day cyber review. The commission's report [2] identified cyber security as "one of the major national security problems facing the United States (pg 1)." In addition, President Obama ordered his National Security Council to conduct a 60-day review of existing measures "to ensure that U.S. Government cyber security initiatives are appropriately integrated, resourced, and coordinated with Congress and the private sector [3]."

In many cases, for example in response to the recent violence on the U.S./Mexico border, an important component of any security response is often a call to "defend the borders". However, such measures are problematic when attempting to respond to threats in cyberspace. One of the biggest issues with applying border control measures in cyberspace is the amount of inter-connectivity with other nations in the medium. Because cyber security measures must be internationally coordinated, the question often arises as to whether the concept of borders is relevant in the domain [see 4,5]. This article explores the question, "can borders, as components of sovereignty, be relevant to addressing cyber security?" To explore this question, I will use two different analytical constructs. First, I will compare the problems with securing a nation in cyberspace to the problems of combating drug trafficking. Researchers have raised similar concerns about stemming the tide of illegal drugs crossing national borders. If these two problems appear similar in their challenges, then perhaps we can draw lessons for cyber security from border-related measures to combat drug trafficking. Second, I will apply the Interdependent Security model, on which I will elaborate in a later section, to the problem of national cyber security. If this model can be considered a valid construct, perhaps it can also point to a role for borders as the nation-state actors in the model choose cyber security investment strategies. At a minimum, it would highlight in which countries sufficient measures are being taken and where they aren't, thereby highlighting the boundaries between them. Based on these dissimilar analyses, I will argue that, regardless the challenges of applying security measures "at the borders," as concepts of sovereignty, national borders remain relevant components of state-level responses to security threats in cyberspace. This analysis will not be an attempt to find answers to empirical questions, but rather provide new frameworks beyond the purely technical/legal aspects to address cyber security and borders.

The next section will provide some background and frame the discussion more precisely. There are several challenges to even effectively securitize threats in cyberspace. For example, the nature of "cyber security" as a national security issue is ambiguous and there is a heightened potential for a security dilemma in the domain. The goal of this section will be to frame the problem in such a way that it effectively bounds the ensuing discussion and informs the questions of borders as they relate to the

[2] For the purpose of this article, "securitization" is understood as the process outlined by Buzan et al. [1]. Namely, an issue is presented as posing an existential threat to a designated referent object (in this case, a nation-state) requiring emergency measures and justifying actions outside the normal political bounds (pgs 23-24).

domain. After addressing these issues, I will present the two analytical frameworks and highlight their relevant findings. The article will conclude with a synthesis of the issues and a discussion of policy implications. Regardless the findings from this work, sovereign powers must be careful not to use the concepts of borders to curtail the progress we have made to connect and better the world via this evolving and expanding environment.

1. Framing the Issue

Effective securitization of threats in cyberspace can be complicated by many issues. First, there is little agreement as to what the security issue in cyberspace actually is. This is a common problem with issues of security that must compete to be on the public agenda. Arnold Wolfers [6] called national security an "ambiguous concept," and because of the unknown nature of actors and their motives in cyberspace, the ambiguity is only heightened in this domain. Different actors will securitize the problems according to their perceptions or agendas. For example, while one nation may assert that an existential threat is posed by a denial of service attack against their fragile banking infrastructures, another may highlight fundamentally different issues. Some policy advocates would include threats from websites critical of government regimes to be a component of cyberspace security. A. Strelstov [7], a member of a Russian delegation to the UN, identified that, "undermining a state's economic and social systems and psychological manipulation of a population for the purpose of destabilizing society," is also a component of what the Russians call international information security (pg 8).

An additional concern is the heightened potential for a security dilemma in cyberspace. As characterized by Herz [8], 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. Buzan [9] goes further to identify that some ambiguous measures may actually be attempts to gain more power vis à vis potential adversaries. This challenge of what Buzan terms the "power-security dilemma" is most difficult to counter in cyberspace. When fielding tanks and anti-aircraft missiles, their presences can be declared as defensive measures and made visible to the public. However, it is much more difficult to make public or confirm the defensive nature of measures a country may employ to improve security in cyberspace. Assertions that the actions are also offensive will be difficult to counter because any offensive potential would be difficult to disprove and offensive use would be difficult to identify. Complicating the issue further, attacks within in the domain can easily be masked and attributed to a nation-state, when, in fact, they may be the actions of non-state actors (or vice versa).

Overcoming both these factors requires a common understanding of the issues. Any effort to securitize a situation requires a threat agent, a victim, and an understanding of how the threat agent causes an existential threat to the victim. In cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states[3]. The greatest challenge is determining who is conducting the attack before extensive forensics have been accomplished. The targets of these actors are also diverse. They

[3] For a good survey of the myriad of malicious actors in cyberspace, see Denning [10], Gorman [11], and Kramer et al. [12].

may be in the business of stealing personal identities to commit fraud, conducting industrial espionage, engaging in cyber extortion of critical infrastructure owners, or preparing for and conducting a deliberate conflict accompanied by actions in cyberspace. Any analysis and body of policy recommendations that attempt to incorporate every possible combination of these malicious actors and their attack methods would be hard pressed to escape the trap of ambiguity. Therefore, to narrow the scope to a level appropriate for this analysis, national-level cyber security will entail the following:

> Attacks and infiltrations by either state or organized non-state actors against government and critical infrastructure systems (privately and publicly owned) to gain knowledge of a national security value and/or attempt to degrade/disrupt such systems.

National security is about existential threats to the state. Obtaining knowledge of a national security value can create an existential threat by allowing potential adversaries to gain the knowledge to develop effective counter-measures to a nation's advanced military and other defenses. In addition, cyber attacks that degrade the ability to command and control national security assets and attacks that disrupt critical infrastructure have direct implications to national security. This infrastructure may be civilian, military, or both. In the United States, for example, the Department of Defense relies heavily on the nation's public and private cyber infrastructure backbone for communications purposes [13].[4]

Some security measures are currently in place to protect against the threats articulated above. Such measures are employed by both government agencies and the private sector owners of much of a nation's critical infrastructure [see 14]. An obvious measure to defend against the theft of sensitive information would be to place all critical information and correspondence on closed systems that are not connected to the publicly accessible Internet. In the United States, for example, this would entail containing the information within the national security system architecture managed by the National Security Agency and Defense Information Systems Agency[5]. Certainly, governments secure much of their critical information in this manner. However, it is also the case that, as we become more reliant on the Internet for collaboration on all activities, especially between the public and private sector, it is becoming increasingly difficult to keep critical information controlled in this manner. A recent incident regarding a potential loss of design information for the F-35 Joint Strike Fighter highlights this problem. The information was stolen from private, proprietary industry networks (meaning no government access or frequent auditing), and it apparently contained several terabytes of design data on the future air defense capability for several nations [15]. Remaining disconnected from the greater cyberspace could be a measure employed by critical infrastructure owners and operators also. The control networks could be closed, proprietary systems with no remote access. In fact, older generation control systems employed tailored protocols and were only managed through proprietary, closed systems because there was no Internet available at the time.

[4] Note that the focus for this article does not include industrial espionage unrelated to national security, hacking for pleasure, identity theft, and the use of the Internet for training, messaging, and internal transactions of bad actors. Though these can all be considered criminal acts in their own right, they are outside the scope of this discussion.

[5] For an overview of the U.S. National Security System, refer to the CNSS website at www.cnss.gov

However, the trend has been to install remotely maintained systems employing common OS architectures to leverage the connectivity benefits of the Internet [16]. Therefore, these critical infrastructure systems have assumed a risk common to all those dependent on the effective functioning of the Internet.

The United States, as a sovereign country, certainly has the inherent right to control all of its borders in any domain [17]. With the above considerations, it is clear the public sector cannot manage all necessary security actions alone. Private companies are an important part of the dynamic that is absent in other areas of national security where the actions of the military, or law enforcement, dominate the response options. We have no early warning radar system or Coast Guard to patrol the borders in cyberspace. Unlike in other domains, information of an attack will come first from those being attacked. Therefore it is highly unlikely that a government organization, unless it is actually the target of a cyber attack, will have greater situational awareness. An effort must be made to incentivize the private sector to invest in cyber security as well. In many cases, national security depends on it. But if none of the measures being employed have a border patrol component, does that necessarily mean that borders are not significant in cyberspace? The next two sections will introduce two different frameworks to address this question. In the first of the two analytic frameworks, I will compare the problems of securing a nation against cyber threats to the challenges of securing a nation against international drug trafficking.

2. Comparison with Drug Trafficking

In a way, the world has become a victim of its own developmental successes. Over the last two decades, we have seen an incredible amount of openness in commerce and the exchange of ideas. However, with openness comes much vulnerability. Several authors have highlighted the fact that increased globalization and economic interdependence have been accompanied by greater economic disparities. Globalization has also created an environment where it is much easier for clandestine transnational actors (CTAs) to operate [see, for example 18][6]. As such, it has been increasingly difficult to secure nations against the growing, non-traditional threats from these CTAs. However, it is possible that efforts to do so can inform the challenges of cyber security. But how similar are the issues?

From my perspective, there are at least six factors in combating drug trafficking that compare to the challenges of cyber security. First, CTAs engaging in the drug trade are based in countries with few legitimate economic opportunities [18]. Legal activities, such as growing subsistence crops have little chance of competing with the lure of income from growing poppy seeds in countries like Afghanistan and Thailand. A similar trend has been developing in cyberspace. Several developing countries have become sanctuaries for cybercriminals, or transit points for malicious actors located in other regions. A recent arrest in Romania highlights the growing hacking community in Eastern Europe. A hacker nicknamed “Wolfenstein” is suspected of breaking into US Department of Defense computer systems and planting malware [20]. Brazil has also been identified as a growing contender for the cyber crime capitol of the world. In 2004, the Brazilian federal police claimed that it was home to 80% of the world’s hackers [21]. In addition to these countries, researchers consider China to be a growing threat

[6] The term “clandestine transnational actors” is adopted from Andreas [19].

[22]. But due to problems of attribution, it is difficult to tell if the actions are state-sponsored, or private actions [23]. Regardless the location, or identity of a specific attacker, a nation-state may be involved as the sponsor. Many countries would be interested in information about rivals thereby acting as customers to those providing national security-related data obtained through cyber espionage.

Second, but closely related to the previous point, illegal drug control regimes rely almost exclusively on the coercive actions of national governments, but the trade is conducted in areas where actions at the state level are often ineffective [24,18]. Because each country is sovereign and reserves the right to draft and enforce it's own laws, international drug control actions must contend with widely differing legal regimes. Compounding the problem, developing countries have much less effective law enforcement. The same barriers confront cybercrime responders. For example, as recently as 2004, hacking was not considered a criminal offense in Brazil [21]. Only recently have such vehicles as the European Cyber Crime convention and other bi-lateral agreements led to improvements in synchronizing legal regimes to combat cyber offenses.

Third, the Internet itself is an excellent source of knowledge on how to engage in the drug trade [24]. One can easily find instructions for how to make such drugs as LSD or methamphetamine (see, for example, www.homemadedrugs.net) by browsing websites or conversing with others in forums. Just as easily, one can find the tools required to break into computer systems, as well as instructions for their use in news groups (see, for example, www.sectools.org). During the conflict between Russia and Georgia, for example, there was substantial evidence that the attacks on Georgian governmental websites were directed via web forums [25]. In neither the case of drug trafficking nor hacking is formal training required or even available. The only actors who may have received formal training would have done so as former security officials.

Fourth, customs agents have to sift through ever increasing amounts of legitimate goods and people to find illegal drugs. According to Stephen Flynn [26], a border security expert and former US Coast Guard officer, customs agents must patrol a continuous stream of peoples and goods at more than 3,700 terminals at over 300 points of entry. As he states, it "[i]ntercepting the ripples of danger in this tidal wave of commerce is about as likely as winning the lottery (pg 57)." Similar challenges exist in cyberspace. With well over 3 Tbps traversing international routes between the US and the rest of the world, it is virtually impossible to differentiate legitimate Internet traffic from traffic with a malicious purpose[7]. Information that has been stolen from somewhere, or that contains commands that will "flip a switch" in such a way as to cause severe damage to a critical infrastructure system, is extremely difficult to identify. Intercepting it requires previous knowledge that the information should not be traveling across the Internet in the first place. In other words, you can train a dog to identify marijuana, but it is unlikely it can be trained to identify the difference between Bayer aspirin and a generic or that the prescription has expired and belongs to someone else.

Fifth, efforts to combat retail drug transactions are constrained by civil liberty concerns. Victims, who could be considered accomplices in an illicit transaction, can hide behind privacy rights [24]. Oftentimes the victims of cyber espionage may choose to cover the event as well, but for slightly different reasons. Since cyber crimes can be

[7] 3 Tbps is an educated guess based on analyzing the Telegeography data source used for the second analysis of this paper. An exact figure would be extremely difficult to obtain and would only be valid for a few seconds.

hidden from the public by both the victim and the perpetrator, a company that has been infiltrated may chose not to report an event for fear of assuming liability for the actions [27]. They may also be concerned about a reduction in customers' trust in their ability to safeguard sensitive information. In fact, it may not be until the recipient nation of stolen data has built an exact replica of a system, for which they have obtained the design secrets, that there is any indication that a theft has occurred.

Lastly, there is little agreement on what exactly constitutes the "evil to be eradicated" when assessing and implementing counter-drug trafficking measures [24]. For example, the current debate surrounding the drug cartel violence in Mexico centers on the role of the United States in creating the problem [28]. What is worse, trafficking drugs or supplying criminal gangs with automatic weapons? In the current conflict across the border, the drug cartels are armed with a much more powerful arsenal than the local police. Law enforcement officials confront similar challenges when combating the growth in cyber crime. Many criminals use the defense of, "I just did it to see if I could get into the system and didn't know what I was getting." Being a red, white, grey, or black hat may depend on a person's perspective. Many of these actors see themselves as beneficial to the network security industry and downplay their influence on cyber criminals (which they often once were). Movies, such as "Hackers" continue to glorify the actions of teen-agers who break and enter systems in cyberspace, when such actions against a physical facility would be clearly viewed as trespassing. As stated above, as recently as 2004, hacking was not even considered a criminal offense in Brazil.

There may be several more similarities, but is should be evident from this presentation that there are many conceptual similarities between these two types of non-traditional threats to national security. With this in mind, I will discuss how borders have played a role in the international war on drugs to determine if such measures can illuminate the complexities of countering attacks through cyberspace. As stated, in this age of globalization, it is virtually impossible to detect contraband crossing national borders. The US has, for example, 106,000 miles of physical borders and shorelines and over 400 million people transit those borders yearly [26]. Though we cannot completely secure the borders against drug smuggling, they still seem to play an important role in efforts to combat the trade. The recent measures by both the US and Mexican governments along their shared borders highlight the political importance of actions taken to secure borders against the movement of drugs. Arguable the measures were enacted due to a perceived loss of control of the borders to the drug cartels. Peter Andreas, Harvard Professor and the author of *Border Games* [29], asserts that border control measures are an important symbolic and perceptual response that the state is defending its sovereignty and its citizens from an existential threat. By "sending in the troops," the state can demonstrate its moral resolve and commitment to maintaining its territorial integrity. Even if there is little empirical evidence that any measures enacted to defend the borders against the flow of drugs has an effect at reducing the inflow to the US, there is tremendous pressure to take action. Besides demonstrating resolve, the visible actions remove pressure to confront the more difficult but root causes of the drug trade-the insatiable demand.

In addition to the largely symbolic nature of recent actions on the US-Mexican border, law enforcement officials do attempt to achieve a deterrent effect with their actions. In this and other border regions, measures have gone beyond the dedication of more personnel. Enforcement measures have relied on improved surveillance technology but also such measures as "pushing out" borders [19]. For example, in both the case of European Union countries and the United States, the immediate neighbor countries are enlisted to “thicken” the border defenses. In the case of the United States, the problem of drug trafficking is not limited to the immediate border. The drugs originate in several source regions and many are funneled through Mexico. According to Andreas [19], by supporting Mexican efforts deep in Mexican territory, a larger buffer zone is created while supporting the smooth flow of legal cross-border commerce. In the European Union, member countries encourage neighboring countries to improve coordination with their law enforcement efforts by making tighter law enforcement actions pre-conditions for admission to the EU. Lastly, efforts can also focus on commercial trans-shippers of legitimate goods who depend on speedy transit of international customs facilities. Flynn [26] suggests that it is in the interest of transnational shipping companies to tighten their own logistics and transportation procedures. As the logistics infrastructure continues to improve and widen the markets for perishable goods and “just-in-time” deliveries, shippers are under increasing pressure to maintain delivery schedules. Therefore, they have a tremendous incentive to avoid any potential delays that could be created if they are found to be lacking controls on their cargo. Customs officials could use this incentive structure to their advantage and encourage commercial trans-shippers to help reduce the potential smuggling of illicit drugs.

These three example measures could have implications for patrolling the borders in cyberspace. First of all, as threats in cyberspace become increasingly securitized, we can expect the same pressure for national governments to take action as they have done in the wars on drugs. This will undoubtedly entail largely symbolic actions to attempt to secure national borders in the domain. In the case of the US, such efforts may be cast as an attempt to “regain the control of cyberspace” it ostensibly maintained during the early years of Internet development. At the time, it was managed by the US Department of Defense and then the National Science Foundation. The symbolic gestures to “regain control” can be reified by technological border control points, attempting to thicken the cyber borders, or both.

For example, a border control point could be established at the terminus between undersea cables and fiber optic lines. At these points, customs, law enforcement, or other agents of the federal government could employ any of several technical solutions such as deep packet inspection devices or Anagran flow management devices [17,30]. Other solutions suggest labeling traffic to identify countries of origin and destination [31]. The intent here is not to debate the technical or practical feasibilities of such measures[8]. Without employing any such measures, there is no empirical evidence available to determine their efficacy, or if they will slow Internet traffic appreciably. The point here is to show that several measures have been researched and, enacting any or all would, at a minimum, be symbolic statements to assert sovereignty over national territory in cyberspace.

More practical measures would mirror the defense-in-depth approach taken by Europe and the United States to combat drug trafficking and other CTA activities. For example, nations with more developed legal and law enforcement regimes could encourage neighboring nations to improve their legal regimes. Developed nations could also provide technical support to others’ national cyber security centers. One unique characterization of cyberspace is that neighboring nations in the domain are not always

[8] For an in-depth discussion of a multi-agency Internet Border Inspection Station concept, see Upton 2003. For details on the Anagran technology, see http://www.anagran.com/products_fr_1000_intelligent.php.

physically contiguous. However, that should not limit the possibilities for cooperation. As with drug trafficking, the focus must be both on nations where attacks have historically transited, and those where the attacks are perceived to be originating. A recent effort in Europe to "thicken the cyber borders" has been the broad adoption of the Council of Europe Convention on Cyber Crime. Six countries signed, ratified and entered it into force by 2004. However, since that time, an additional nineteen countries, to include the United States have adopted the convention[9].

Additional defense-in-depth measures could focus on the cyberspace common carriers- the Internet Service Providers and Backbone companies. They are the carriers of the legitimate traffic in which the contraband is hidden. Like the international trans-shippers of physical goods, these are the commercial interests that would be adversely impacted by tightened border controls that may result from the emplacement of government-monitored border inspection devices. Employing such a suite of inspection tools, which would adequately provide for the protection of civil liberties, would invariably slow Internet traffic. Therefore, ISPs would be expected to have a great incentive to support the improvement of self-regulated inspection regimes. If they can be motivated to improve their internal procedures to help law enforcement combat cyber attacks, then there will be less pressure for more restrictive national-level. Perhaps, the absence of a real threat of employing federal border security measures has contributed to neglect on the part of ISPs to better control the activities of their customers. Regardless the exact point of entry of goods and people in any domain, states have sovereign rights over all their territory and can also pursue legal recourse against cyber crimes committed anywhere within their borders. Though effectiveness has been limited, we must continue to rely on state responses for the foreseeable future.

This section of the paper used a comparative case study approach to identify lessons that could be taken from the fight against international drug trafficking and applied to cyber security. The next section of the paper will take a fundamentally different approach and explore the use of a game-theoretic construct and novel quantitative methodology to address the issue. The analysis expands on a theory that has been previous employed to research situations in which the security of one actor depends substantially on the actions of other actors in their system.

3. Interdependent Security Theory

In his book, Micromotives and Macrobehavior, Nobel laureate Thomas Schelling [32] described the concept of binary, "either-or," choices that create externalities on the decisions of others. To explain the concept, he described several different situations where the question was not about how much anyone does, but how many make one or the other choice. For example, the decision to follow daylight savings time or joining a boycott would be considered binary. The interesting implication of Schelling's model is the potential to "tip' the collection of decision makers from one decision to the other. This tipping effect could reduce the potential social costs when not enough actors initially make the socially beneficial choice. The model can also be applied in situations where actors must coordinate security decisions. Economists Kunreuther and Heal [33] built on this concept of interdependent decision-making after the events of

[9] Assessment based on a table from the Council of Europe website at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

9/11. They introduced a game-theoretic approach to explore more deterministic outcomes of a class of binary choices, the interdependent security (IDS) investment decision. Kunreuther and Heal's focus has been on the existence of Nash-equilibria in the decision whether or not to invest in security measures. Of particular note, in an IDS model, a fundamental assumption is that an indirect attack, or an attack that originates from within the system due to a failure by a partner actor, cannot be defended against. For example, no matter how much an airline invests in security at their terminal location, if a partner airline allows a bag with a bomb to be transferred to their airplane bypassing the terminal inspection, the investment is for naught.

Arguably, this analytic framework can be applied to the cyber security problem at the nation-state level. In this case, the actors making a security investment decision would be national level governments. The investment could be undertaken by private or public agents, but the security action would be those measures required to secure the critical infrastructure cyber systems and the information systems containing data of a national security value, in other words, the targets of the attacks specified early in the paper. Attackers could be any actor that has the ability to hold the above targets at risk either through a direct attack on a country from a location therein, or indirectly through other countries' national IT systems.[10] In other words, attribution of an attack is not necessary to use this framework.

Understanding that inter-connectivity and inter-dependence is a complex issue at the national level, this analysis must generalize these aspects of the model. Specifically, I make several important assumptions. First, I must assume the state, or an agent acting on its behalf (such as the Department of Homeland Security in the US), can maintain some level of control over the actions of the owners and operators of the national critical infrastructure. In other words, the national government must have the ability to ensure a cyber security investment is executed. Secondly, the analysis assumes that it is possible to invest at a level that significantly protects these systems from failure or information theft that would create an existential risk to the nation. In other words, applying the theory at a national level means that not every single attack must be thwarted as national systems do have some resilience. Lastly, it assumes that actions taken to secure a nation's critical assets in cyberspace can be made visible to others[11].

Even with the above assumptions, there are two additional challenges to applying the IDS theory in this situation. First, it is difficult, if not impossible, to obtain the empirical data regarding the security investment decisions of these agents (especially if many nations do not oversee cyber security at the national level), and the interdependent nature of the decisions by so many actors can be difficult to calculate as their decisions are updated. In such situations, an agent-based model can be useful. Agent-based models employ object-oriented software programs to model the behaviors of inter-acting agents endowed with specific parameters that govern their behavior. Such tools can also model the dynamics created by changes in the behavior of the agents. They are ideal for game theoretic decision problems amongst many actors. In order to conduct this analysis using an agent-based modeling technique, the first decision that must be made is the size and composition of the sample. Who are the representative agents making the investment decisions? Conceivably, I could have

[10] In other words, the exact identity or sponsor of the hostile act is not required for this model to function.

[11] For such an assumption to be valid, it would imply close coordination of efforts amongst those who have chosen to make the necessary investments. For example, partner nations could have liaisons working in each other's national response centers.

constructed a model of all the nations of the world. It would not have created a computational problem for an agent-based, but it would probably not closely reflect the "real world" in cyberspace[12]. Instead, I identified a more practical sample based on the most highly connected nations in the world. The sample network used for this analysis is comprised of the 21 largest countries, in measure of 2008 bandwidth connectivity, as reported by Telegeography[13]. While this sample does not necessarily represent existing cyber security cooperation, it is intended to capture two features. First, nations with the most extensive international Internet connections can be assumed to be those for which cyber security is most critical. Secondly, it identifies which countries have the greatest imperative to work together due to their existing high level of inter-connectivity. A graphic depiction of the sample network is presented in Figure 1. Again, this is only a representative sample to illustrate the potential for this type of analysis. The nodes are representatives of the 21 countries with the highest amount of Internet traffic, and they are connected by non-valued links symbolizing the overall traffic route (i.e., there may be several physical connections between the nodes).

The particular structure of this network has a potential benefit for most of the involved nations. For example, assuming that the vast majority of international traffic must flow through one of the few central actors in this network, a cyber attack that successfully breaches the critical systems in any nation must, in many cases, flow through (or originate) in one of the central countries in order to reach one of the other nations connected to the world only through that central nation. Though this does not reduce the external risk for the few central actors, the structure greatly reduces the externality problem encountered by the rest of the countries in this network. Therefore in practice, though the sample contains 21 agents (nation-states), the interdependent nature of the security investment decision for most "non-central" nations is reduced immediately to a two-player game minimizing risk estimation[14].

Constructing an agent-based program for this model is fairly straightforward. However, an accurate calibration can be challenging. A complete discussion of the construction and calibration is contained in Appendix 1. Based on the data collected from several cyber security sources, the model was run at varying levels of externally generated risks by altering the probability of an indirect attack. The output of the model is most easily interpreted by comparing graphic depictions of the investment decisions over time. Encouragingly, the series of graphics in Figures 2-4 suggest that the agents in this sample network, the highly connected nations, could behave in a manner consistent with the IDS theory.

[12] For example, the investment decisions of the Maldives may have little effect on those of the United States.

[13] http://www.telegeography.com/products/map_internet/index.php

[14] Interestingly, the sample network does exhibit features that make it theoretically feasible to extend these findings to a much larger set of nations. The network appears to be a scale-free form. For a good discussion of the implications of this characteristic, see Barabasi [34].

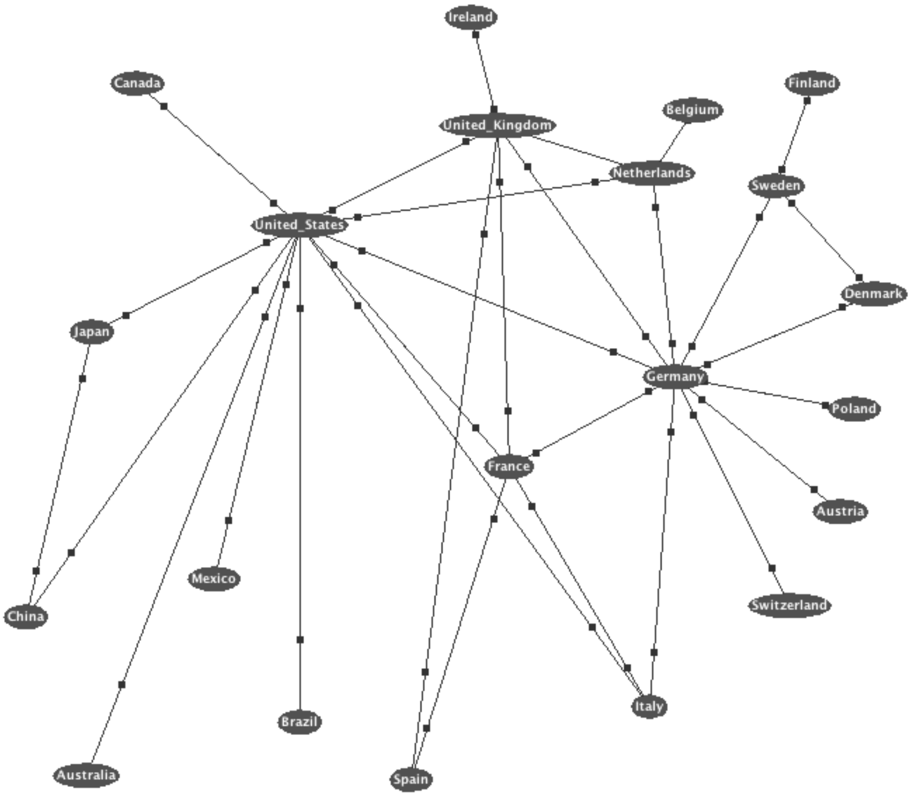


Figure 1. Sample Network of Nations

For the model run depicted in Figure 2, the probability of an indirect attack is set at 0.2. In this instance, the probability is sufficiently low that all the agents in the model find it feasible to invest in security to thwart direct attacks from "outside the system." Skipping Figure 3 for the moment and moving to Figure 4, we find the opposite results. In this case, only a handful of minimally connected nations choose to invest. Since no other nations choose to join these actors once they have decided to invest, the system contains both investors and non-investors at equilibrium. The more interesting result is obtained when the risk of indirect attack is at a point in between. In Figure 3, the probability of indirect attack is set at 0.3. In this scenario, all but the central actors find it advantageous to invest regardless the decision made by other agents. After T_2, the risk of indirect attack to the central actors has now been reduced to the same level faced by the periphery in T_1. As a result, the central actors now find it in their interest to invest. In other words, the conditions are such that the system will cascade to a state of full investing as predicted by the IDS game-theoretic model.

Figure 2.

Full investing on first round

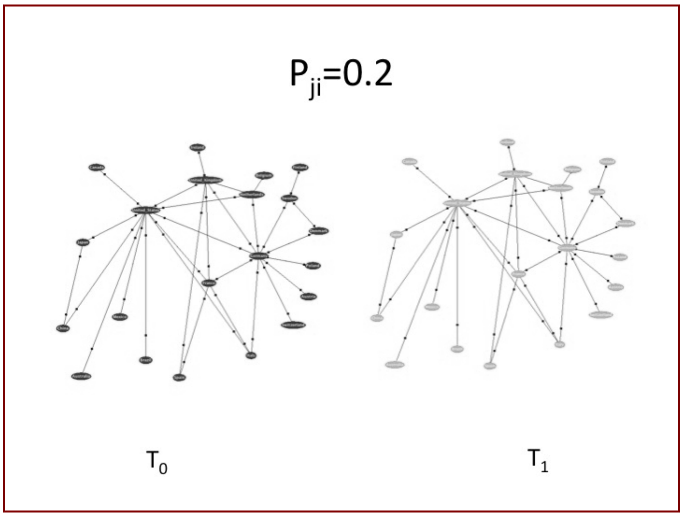


Figure 3.

Full investing after several rounds

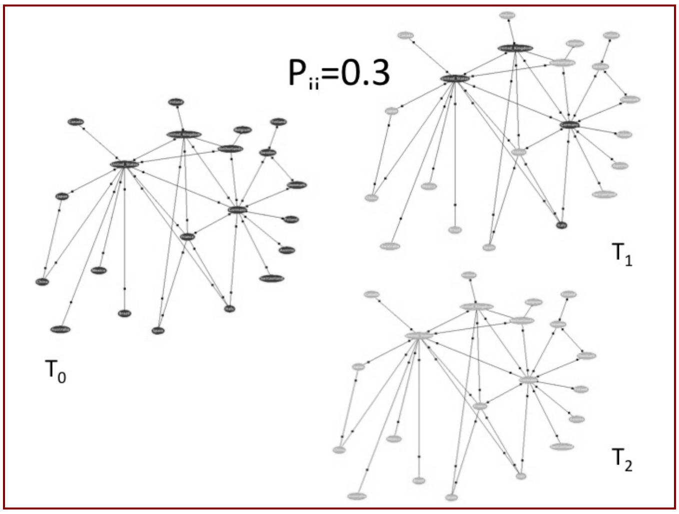
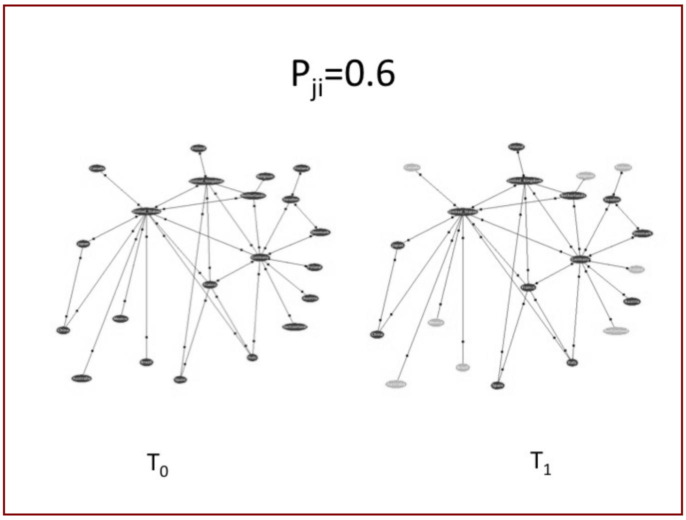


Figure 4.

Mixed investing at equilibrium



These results demonstrate how the actions of one country to improve their national cyber security, whether enacted publicly, privately, or in concert, could positively impact the decisions of other countries confronted with similar challenges. Though we are far from such a reality, the results suggest that when it is possible for a nation to secure its territory within cyberspace, then borders become increasingly important components of cyber security. Namely, they become important as concepts that delineate which portions of cyberspace may be more secure than others. There may not be a cyber security measure enacted directly at physical border post, but when state actors can determine at which point their activities stop and the actions, or inactions, of a neighbor occur, than they can better determine the relative values of enacting their own security measures.

Hopefully, this model demonstrates the importance of coalition building. The border that may be important may not be national borders, but the borders between the investing coalition and others. Until the entire system becomes part of the coalition, there will always be a border between those inside the security umbrella and those outside. As the security umbrella grows and strengthens, the borders will be more sharply delineated. In addition, those outside the security framework may increasingly become the focus of attacks themselves, or the assumed source of malicious actions. Neither condition would be considered very favorable and would lead to increasing pressure to join the coalition of those who have chosen to secure their territory in the domain.

4. Conclusions

This article sought to demonstrate the relevance of borders in issues regarding cyber security. As stated earlier, nation-states have borders. Domains, as merely mediums in which we interact, do not have borders. However, the relevance of a nation's borders in each domain is related to a nation's willingness and ability to assert their sovereignty in them. As long as threats are directed at nation-states, and legitimate response actions are retained by the state, they will remain important actors and their borders will continue to be relevant. Borders can be equally important in cyberspace because borders define boundaries of sovereignty regardless the domain and the ability to locate them physically. Even though borders have become less significant for all legal commerce, they have become even more significant for policing action against transnational threats. To explore their significance, I employed two dissimilar frameworks in an effort to broaden the discussion beyond purely technical and legal dimensions.

In comparing international drug trafficking with the national security elements of cybercrime, we see that there are several similarities. These similarities suggest that we can learn lessons from measures to secure borders against the shipment of illicit drugs. Whether the measures are largely symbolic or actually effective, they demonstrate national resolve and a determination to exert sovereignty. If the current drug wars teach us anything about national responses to transnational problems, the borders will become important in the fight to secure cyberspace if only for their political significance. More effective measures seem to center less on a tight control of the border itself, and more on improving the behavior of companies engaged in legitimate trade across the borders, and the behavior of surrounding countries within their territories.

The agent-based model of the IDS problem provided a theoretically different perspective. In this model, the exact location of the borders is not relevant. What is more important is the potential of, and benefit from coalition-building by actors responsible for securing their portions of cyberspace. If the IDS model teaches us anything, it is that we must work together on an international level. Unilateral efforts to secure borders are a losing proposition in today's interdependent reality. Nowhere is this interdependence more visible than in cyberspace.

The paper also included some considerations for public policy. Specifically, efforts can be made to induce better self-regulation of ISPs to avoid more intrusive border control measures. Also, measures to increase the visibility of national and private security measures can increase the incentives for others to make similar investments, and reduce the potential for a security dilemma arising between nation-states in cyberspace. Continuing to support and encourage neighboring countries to improve their legal regimes and law enforcement efforts is also an important step. However, some findings lead to further policy questions. For example, how do we change cultural attitudes to criminalize hacking behavior? Also, how and when do we increase visibility and share information with countries that may be the source of many threats in the domain? A final note of caution for policy consideration: sovereign powers must be careful not to use the concepts of borders to curtail the progress our nations have made to connect and better the world via this evolving and expanding environment. In other words, we can no more lock down the borders to counter malicious actors in cyberspace than we can lock down our nation's physical borders to fight terrorists and drug-traffickers.

If we accept that nations can play a role to improve cyber security in their country (within their borders) and influence others to do so as well, then there will continue to be an important role for borders as a physical and legal concept. However, if we find that it is not plausible for the state to affect security in its portion of cyberspace either technologically or conceptually, then the existence of borders in any sense becomes less relevant. Assuming this paper successfully demonstrated the former case is more true than the later, then regardless their exact physical location, the very existence of borders demonstrates a need for us to work together as an international community to develop transnational solutions.

Appendix 1: Agent-based Model Construction and Calibration

Most agent-based models are constructed in an object-oriented computer programming language and they interact in an environment. As described in the paper, the agents in this analysis interact within a network. Based on the IDS model equations, the significant parameters are as follows:

Agent Parameters

- c = Cost of investing in security to a level that defeats existential threats through cyberspace
- L = Loss of critical information from a successful attack
- p_{ii} = Probability of a direct, successful attack
- $p_{ji\,=}$ Probability of an indirect, successful attack that occurs from within the network of highly-connected nations
- Network neighborhood
- Investment State (invest or not invest)

The next challenge is estimating the values of these parameters. All of the nations in the sample have made some level of investment, and the cost, at a national level of achieving an efficiently secure state of security can only be guessed in the absence of specific data on the threats to each. Therefore, another simple convention is employed. The agents are heterogeneous in that initial endowment of c, L, and p_{ii}, are randomly distributed amongst the agents. However, the possible values of these variables are normally distributed about a mean value. This convention allows us to assess the actions of the agents when changing the probability of indirect attack, $p_{ji,}$ while holding other parameters within realistic bounds[15]. The value for p_{ji} for each agent is also normally distributed about a mean value, but it is a single variable for the agent's entire network neighborhood[16]. After consultation with cyber security experts regarding the potential costs and losses at the firm level[17], the remaining parameters were estimated by the following mean values:

c = $1,000,000
L =$10,000,000
p_{ii} = 0.4

Though the empirical data is not available, a mean value for p_{ii} was set at 0.4 based on a recent SANS Institute report [35] regarding attacks on firms in several industries. While holding these parameters constant, p_{ji} was varied from 0 to 1 to explore whether this sample network can behave in a manner predicted from IDS theory.

[15] In this assessment, 'realistic bounds' means relative to the other agents. The author did not attempt to estimate the actual, absolute costs of any of the parameters nor was it necessary to do so.

[16] In other words, the risk from each other agent, to which an agent is connected, is the same. This convention was necessary to generate a less complex decision algorithm for the basic model.

[17] For this analysis, it is only important that the relative values be appropriate and therefore it is assume that the values at the firm level can be scaled to the national level with the understanding that, just like the difference between small and large firms, the costs at a national level can vary widely as well.

In addition to the agent parameters, there are rules that govern agent interaction. The agents make the security investment decision according to the interdependent security pay-off algorithms of the Kunreuther and Heal model[18]. In the current model, the behavior of the agents is determined by the following:

Interaction Rules

- Identify how many others in your network neighborhood have not yet invested in security
- Calculate the external risk created by their decision not to invest
- Determine if the external risk is less than or greater than the cost to invest
- If the cost is less, then decide to invest. If not, then decide not to invest
- Once all agents have made this decision, everyone changes their state as appropriate
- Repeat the above process until no one wants to change their state again

Initially, the agents are in a state where they have not invested. Since Kunreuther and Heal (2003) identified that the cost of the risk externality as the significant limiting condition, agents choose to invest in security when the inequality, $c < p_{ii}(L - X)$, is true. In this equation, X is the externality generated by others in the network that have not invested in security.

References

[1] B. Buzan, O. Wver, J.D. Wilde, O. Waever, Security: A New Framework for Analysis, Lynne Rienner Pub, 1997.

[2] J. Lewis, Securing Cyberspace for the 44th Presidency, Center for Strategic and International Studies, Washington, D.C., 2008.

[3] Office of the Press Secretary, (2009).

[4] B. Kahin, C. Nesson, Borders in Cyberspace: Information Policy and the Global Information Infrastructure, The MIT Press, 1997.

[5] C.C. Joyner, C. Lotrionte, Eur J Int Law 12 (2001) 825-865.

[6] A. Wolfers, Discord and Collaboration: Essays on International Politics, The Johns Hopkins University Press, 1965.

[7] A. Streltsov, Diarmament Forum 3 (2007) 5-14.

[8] J.H. Herz, World Politics 2 (1950) 157-180.

[9] B. Buzan, People, States, and Fear: The National Security Problem in International Relations, University of North Carolina Press, 1983.

[10] D. Denning, in:, J. Arquilla (Ed.), Networks and Netwars: The Future of Terror, Crime, and Militancy, Rand, Santa Monica, Ca, 2001, pp. pgs 239-288.

[11] S.P. Gorman, in:, P.E. Auerswald, L.M. Branscomb, T.M.L. Porte, E.O. Michel-Kerjan (Eds.), Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, 1st ed., Cambridge University Press, 2006, pp. 239-257.

[12] F. Kramer, S. Starr, L. Wentz, eds., Cyberpower and National Security, Potomac Books, Dulles, Virginia, 2009.

[18] See Heal and Kunreuther [36] for a complete explanation of the pay-off matrix according to a two-person game.

[13] C. Wilson, Information Warfare and Cyberwar, Congressional Research Service, The Library of Congress, 2004.

[14] DHS, National Infrastructure Protection Plan, Department of Homeland Security, 2006.

[15] S. Gorman, A. Cole, Y. Dreazen, Wall Street Journal (2009) 3.

[16] Energetics, Roadmap to Secure Control Systems in the Energy Sector, 2006.

[17] O. Upton, Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection, Master of Arts Thesis, Naval Post Graduate School, 2003.

[18] L. Shelley, Geo. J. Int'l Aff. 6 (2005) 5.

[19] P. Andreas, International Security 28 (2003) 78-111.

[20] J. Leyden, The Register (2009).

[21] T. Gibb, Bbc (2004).

[22] T. Thomas, Cyber Silhouettes, 1st ed., Foreign Military Studies Office, Fort Leavenworth, 2005.

[23] R. Deibert, R. Rohozinski, Tracking Ghostnet, Centre for International Studies, University of Toronto, Toronto, 2009.

[24] S. Flynn, in:, Beyond Sovereignty: Issues for a Global Agenda, Palgrave Macmillan, 1999, pp. 44-66.

[25] B. Krebs, Report: Russian Hacker Forums Fueled Georgia Cyber Attacks (2008).

[26] S. Flynn, Foreign Affairs 79 (2000) 57.

[27] W.S. Baer, A. Parkinson, Security & Privacy, IEEE 5 (2007) 50-56.

[28] H. Lafranchi, Christian Science Monitor (2009).

[29] P. Andreas, Border Games: Policing the U.S.-Mexico Divide (Cornell Studies in Political Econ, Cornell University Press, 2001.

[30] P. Bartram, (2009).

[31] J.E. Molini, Computers & Security 16 (1997) 189.

[32] T.C. Schelling, Micromotives and Macrobehavior, New, Norton, New York, 1978.

[33] H. Kunreuther, G. Heal, Risk and Uncertainty 26 (2003) 18.

[34] A. Barabasi, Scientific American 288 (2003) 9.

[35] SANS Institute, Top Ten Cyber Security Menaces for 2008, SANS Institute, 2008.

[36] G. Heal, H. Kunreuther, Journal of Conflict Resolution 49 (2005) 201-217.