Democracy and Security

ISSN: 1741-9166 (Print) 1555-5860 (Online) Journal homepage: http://www.tandfonline.com/loi/fdas20

The Cyber Losers

Aaron Franklin Brantly

To cite this article: Aaron Franklin Brantly (2014) The Cyber Losers, Democracy and Security, 10:2, 132-155, DOI: 10.1080/17419166.2014.890520

To link to this article: http://dx.doi.org/10.1080/17419166.2014.890520

Democracy and Security, 10: 132–155, 2014

ISSN: 1741-9166 print/1555-5860 online
DOI: 10.1080/17419166.2014.890520

Routledge
Taylor & Francis Group

The Cyber Losers

Aaron Franklin Brantly

ICT Innovation, National Democratic Institute, Washington, DC

National security cyber activities harm human rights and democracy activists. With increasing state cyber capabilities comes heightened pressure on civil society and democracy activists. We often think of the cyber arms race from the perspective of states and corporations; however, the real losers are activists who seek to promote democracy, development, and human rights. This article examines how advances in national security activities have created a new spectrum of issues for activists not previously encountered, and posits a theory of externalities emanating from the cyber arms race.

Keywords: Cyber, Democracy, Human Rights, Security Dilemma

> The essence of government is power; and power, lodged as it must be in human hands will ever be liable to abuse. —James Madison

INTRODUCTION

There is a new type of conflict brewing, and its victims are human rights and democracy activists around the world. This new conflict is rooted in the cyber domain, and it is defined by the traditional security dilemma as outlined by Robert Jervis.[1] As in any war, there are winners and losers. The current conflict is for power within cyberspace, and the losers are non-state actors engaged in human rights and democracy development work. The evolution of the security dilemma in cyberspace over the last 20 years leads us to ask how the security dilemma present in the cyber domain affects human rights and democracy activists. We posit that the security dilemma in cyberspace is reflected in an arms race between states, resulting in a category of actors being left behind, unarmed (or least significantly underequipped) and vulnerable in a domain that crosses traditional state boundaries.

Below we will illustrate how states are engaging in a cyber arms race using data from 10 countries and how this evolving arms race is correlated

Thank you to Katrin Verclas and Zak Whittington and the National Democratic Institute for International Affairs for their support and assistance.

Address correspondence to Aaron Franklin Brantly, National Democratic Institute, ICT Innovation, 455 Massachusetts Ave., Washington, DC 20001. E-mail: afbrantly@icloud.com

to increasing pressure on human and democracy rights activists in cyberspace. The article proceeds in three sections. First, we build an argument for the presence of a security dilemma occurring in the cyber domain using evidence from literature and data derived by focusing on 10 relevant countries. Second, we correlate this developing security dilemma within our sample with increases in censorship in surveillance activities targeted against individuals engaging in human rights and democracy development activities in the cyberspace. Last, we examine how externalities posed by a security dilemma in the cyber domain affect human and democracy rights activists around the world.

THE SECURITY DILEMMA IN THE CYBER DOMAIN

Since the Internet became a widely used public communications platform, it has been heralded, along with other digital technologies, as "liberation technology."[2] These tools are capable of facilitating the empowerment of individuals, communication, and mobilization.[3] The Internet, dating back to its ARPANET days, was largely designed to be an open system, free of many of the security controls now deemed necessary for everyday use. Researchers could share ideas, experiment, and engage one another at great distances. Citizens could blog or keep track of policy issues and news. As the Internet has expanded, so have the tools and capabilities associated with it. New content distribution mediums became increasingly prevalent as technological advances increased processing power and data transmission speeds. Images, videos, programs, and more could be transmitted across the Internet with increasing speed and reliability. The introduction of commerce on the Internet in the 1990s radically changed the way in which transnational commercial interactions occurred.[4]

Lawrence Lessig in *Code Version 2.0* writes of the creation of cyberspace: "The space seemed to promise a kind of society that real space would never allow freedom without anarchy, control without government, consensus without power."[5] The Internet is at once an environment of anarchy and of order. There are rules defined by code and by architecture, and at the same time the current of information and ideas has historically been considered a realm free of governance. While the notion of the Internet being free of governance is largely inaccurate, the assumption of the Internet as an anarchic domain has persisted.[6]

This environment has players of different shapes and sizes ranging from individuals to states.[7] Cyberspace is not truly a Hobbesian state of nature with an absence of government; instead environmental constraints on states in the cyber domain are approximate to the traditional anarchic constraints found in structural realism. Because there is nothing to prevent states from infringing the digital borders of other states within cyberspace, states have shifted toward developing both offensive and defensive tools. It is this production of

cyber capabilities that results in a perpetual spiral of insecurity at both the state and sub-state level.

Cybersecurity related issues date back decades. Michael Warner finds that computer systems were susceptible to leaks as early as the 1960s and were vulnerable to attacks and data theft as early as the 1970s.[8] Richard Clarke indicates that the first massive attempt of the weaponization of computer systems most likely occurred in the 1980s when the KGB stole coding used to monitor oil and natural gas pipelines.[9] The CIA, aware the code was being stolen, embedded malware into the code, causing a gas pipeline to function normally at first, only to malfunction at a later date, exploding with a blast equivalent to a three-kiloton bomb.[10] Alan D. Campen also provides compelling evidence that the first use of cyber tools in conventional conflict occurred during the first Persian Gulf War.[11] Subsequently, multiple nations have recognized the importance of cyber capabilities in the conduct of both conventional and nonconventional conflicts. Christopher Bronk even went so far as to sketch a hypothetical conflict in which China uses cyber tools to effectively collapse the United States' command and control capabilities.[12] Recognition of the importance of a new class of capabilities affecting national security has led to the creation of a cyber arms race, resulting in a security dilemma.

Jervis states: "Many of the means by which a state tries to increase its security decrease the security of others."[13] The security dilemma is the central thesis of realist international politics as outlined by Hans Morgenthau, Kenneth Waltz, John Mearsheimer, and others.[14] Although I broadly cite the literature spanning different subsets of theories within realism, I do so because each, to a large degree, roots its foundation in an anarchic environment defined by the security dilemma. To survive, states must establish and maintain their relative power positions in the context of other states. A balance of power is maintained through military and/or economic means. The nuances between the sub-theories of realism do not supersede their ontological foundations rooted in a lack of an overarching authority to prevent the infringement of sovereignty by one state over another absent the self-help development of capabilities.

Examples of the security dilemma date back centuries and focus on conventional military might in the form of navies, armies, bombs, guns, and so forth. History provides ample examples of states engaging in competitive behavior of relative power development. William H. McNeil tells the history of technological advancement in warfare and provides compelling evidence that countries unable to keep up in technological terms are often forced aside.[15] Time and time again technological advancement has led to the innovator's conquest over those slow to innovate. This was seen in military strategies of Napoleon, the English square, and other examples throughout history. The innovator has a temporary advantage that then prompts a shift in military technology and strategy. The process is an ever-evolving quest of innovation and replication in a global power struggle.

The struggle for security is mirrored in virtually every domain and in most countries. Not all countries are financially able to compete at the same level, yet the general trend of competition is maintained. The fundamental concept of competition spans domains in those sectors relevant to the national needs of various states. Nations with sea borders are likely to develop naval capabilities, whereas landlocked nations are unlikely to do so due to a lack of relevance. States are likely to try to compete with those nations that directly affect their national security and attempt to balance against major powers when they are unilaterally unable to provide for their own security.[16]

Increasingly, the cyber domain is one in which the national borders of one nation rub against those of another both physically[17] and virtually. The development of offensive and defensive cyber capabilities in a domain in which tangible national boundaries are limited has a unique effect on the security dilemma as the line between the international security dilemma and the domestic security environment overlap. As states perpetually attempt to establish strength and to defend against weaknesses, both acts form a spiral of insecurity—a spiral that is evident in cyberspace today. Herbert Lin refers to the spiral in the security dilemma as a mechanism of deterrence to dissuade the use of significant cyber weapons.[18] This spiral is often predicated on an uncertainty of relative capabilities. And, as Lin notes, in cyberspace there is an added complexity associated with the security dilemma revolving around issues of attribution, therefore necessitating an overcalculation or estimation of capabilities due to issues of relevance for all facets of classical deterrence.[19]

Jervis argues that the severity of a security dilemma is dependent on "the balance between offense and defense, and the ability distinguish offense from defense."[20] The similarity of development and implementation of tools in cyberspace makes it difficult to distinguish between offensive and defensive capabilities. Likewise, legal and regulatory framework designed to protect against terroristic activities in cyberspace can be used, in turn, as a precursor for legal and regulatory justifications of oppression or offensive actions against other states.

The increasing capabilities of states in cyberspace over the course the last 20 years is staggering. Since May 2006, the Center for Strategic and International Studies (CSIS) under James A. Lewis has identified 127 significant cyber incidents that, according to their definition, were successful attacks on government agencies, defense, and high-tech companies or were economic crimes of more than a million dollars.[21] These attacks are large-scale and represent an enormous impact in terms of both time and money spent. Expanding the general trend of significant cyber incidents beyond the CSIS's sample, a 2012 Microsoft Security Intelligence Report indicated more than 49,000 unique threat families of malware.[22] The data in the report indicates a near-exponential growth rate in malware types over a 20-year period. While malware might be a poor heuristic for state use of cyber, there is likely a

correlation between the creation of state cyber capabilities to defend against malware and capabilities as a whole within the cyber domain. This is best evidenced in the increasing stand up of Computer Emergency Response Teams (CERTS) within nations around the world and the policy documents of nations to establish positions to safeguard government and critical infrastructure against malware.

There are two aspects of both the CSIS and Microsoft data of importance to a discussion on the rise of a security dilemma. The first is that there are clearly incidents of international hostilities occurring within cyberspace as demonstrated by the CSIS data, and second, there is a large volume of incidents that are affecting actors beyond just states. While the first provides an impetus for an insecurity spiral, the second would seem to suggest there are groups of actors unable to make even the most basic of attempts to safeguard themselves in relative terms within the domain.

The security dilemma is demonstrated in conventional domains by the creation of offensive and defensive military capabilities and by a common lexicon of bombs, guns, and so forth. However, the language of the security dilemma has progressed within the literature as highlighted by Andrew Colarik and Lech Janczewski when they write, "many other defense forces are also developing or mobilizing themselves for cyber conflicts on a national and international level."[23] The capabilities being developed and mobilized for cyberspace can be examined in the context of computer network operations (CNO). Table 1 provides a detailed definition of each of the subcategories under CNO. We used these definitions as a rubric for defining cases included in our dataset. We identified instances of states developing a capability in any of the four categories listed below.

Below we illustrate the development of a security dilemma in cyberspace using data from 10 countries. The data is derived from public reports,[24] books,[25]

Table 1: Categories of capabilities under computer network operations.

Computer Network Attack (CNA)	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Defense (CND)	Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.
Computer Network Exploitation (CNE)	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
Legal and Regulatory Development (LRD)	The development of laws and/or regulations directly affecting the operation of or strategy for a nation in cyberspace.

and reporting on the purchase of tools[26] and classified according to the categories identified in Table 1. Because this is a preliminary study, we limited the scope of our data search to the United States, China, Russia, Iran, Indonesia, India, Pakistan, Turkey, and Syria. We chose these countries based on availability of data and likely power interactions at both the global and regional level. We hypothesize a diffusion of capabilities in cyberspace across the subcategories of computer network operations identified in Table 1. As one nation develops a capability, nations of relative power or those nations that identify a relative threat are likely to also develop capabilities. Thus, if the United States were to develop a capability in year 1, we hypothesize Russia and China would follow suit as quickly as possible. As China follows suit, we expect those nations along its periphery will also begin to develop capabilities. In this diffusion or arms race, we expect to see an increasing trend upward over time rather than a leveling off of capabilities.

We examine capabilities as the development of tools, capabilities, and legal/regulatory developments in the year they were developed and create an additive function that increases as states add to their potential arsenal. These capabilities are examined in the context of the definitions outline in Table 1. Thus, if China develops its first CNA tool in 1999 and its second in 2000, then the number of CNA tools going into 2001 is two. We do this for two reasons. Unlike in conventional arms races, where one tool can obviate the need for another, we assume, based on field experience, this additive function on the premise that in cyberspace it is the knowledge and organizational context that becomes the primary tool, more than the code itself. Since in the development of cyberspace capabilities, knowledge is cumulative, we have developed a learning model. It is also important because, unlike in conventional arms races, in cyberspace security is also cumulative. Failure to update one's cyber capabilities can result in persistent vulnerabilities. It is not possible to simply build the next biggest gun; states and individuals must also fix the holes created by previous generations of tools.

Using a pure measure of power in this instance would be inappropriate in many ways. Using a measure such as a Composite Index of National Capability (CINC) score would pull in too many tangential aspects not necessarily relevant to understanding an arms race. Our specification is important because we are not making the argument solely for the purpose of illustrating a desire for maintenance of relative power, but rather the correlative relationship of the development of capabilities in cyberspace to the increased use of those and similar capabilities on non-state actors. On the most basic level, we are following in the footsteps of what William H. McNeil illustrated as a classic arms race prior to and following World War I, when nations developed bigger and bigger dreadnoughts, each with bigger guns than the last.[27] Here we are attempting to illustrate the progressive development of cyber weapons by states.

We expect the cyber arms race to progress similarly to how conventional arms races progress: As one nation develops a capability, those nations in close

proximity will follow suit until there is an eventual trend of development of all nations toward developing similar capabilities. The initiation of capability development likely does not begin at the same time, and, more importantly, it is likely to follow structural power patterns. Thus major powers develop capabilities, followed by powers on the next tier. The process continues to progress all the way down the chain until all countries start developing cyber capabilities relative to their security context.

Figure 1 shows, over time, each of the countries in our 10-country sample initiated capability development within the cyber domain. However, because they separated, it is somewhat difficult to identify the security dilemma in action. Figure 2 provides a series of maps of capability development over time in which darker colors reflect larger capabilities within our sample. It is possible to see a clear development of and arms race between major powers and, subsequently, regional powers.

There are few surprises in the data. The United States, Russia, and China began to develop capabilities earlier than other countries within the sample. These nations are considered the big power players within our sample, and the similar trend lines would indicate a common grouping. Similarly, we see the

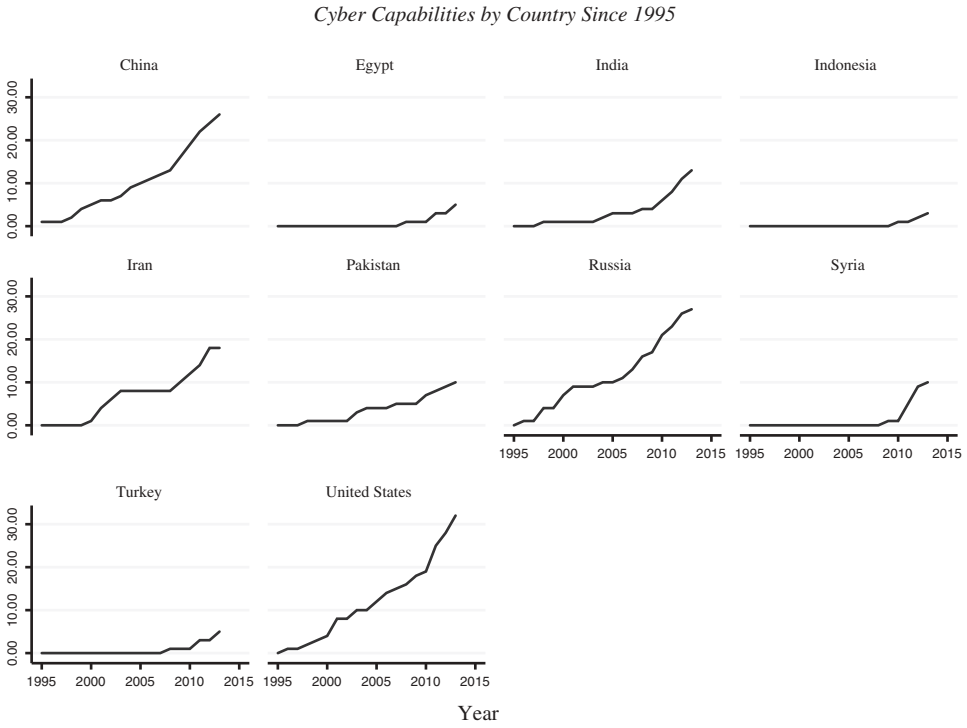

Figure 1: The progression of the cyber arms race over the last 18 years. *Source*: Aaron Brantly, "Cyber Capabilities by Country." http://bitsbytesrights.org/cyber-capabilities-by-country/

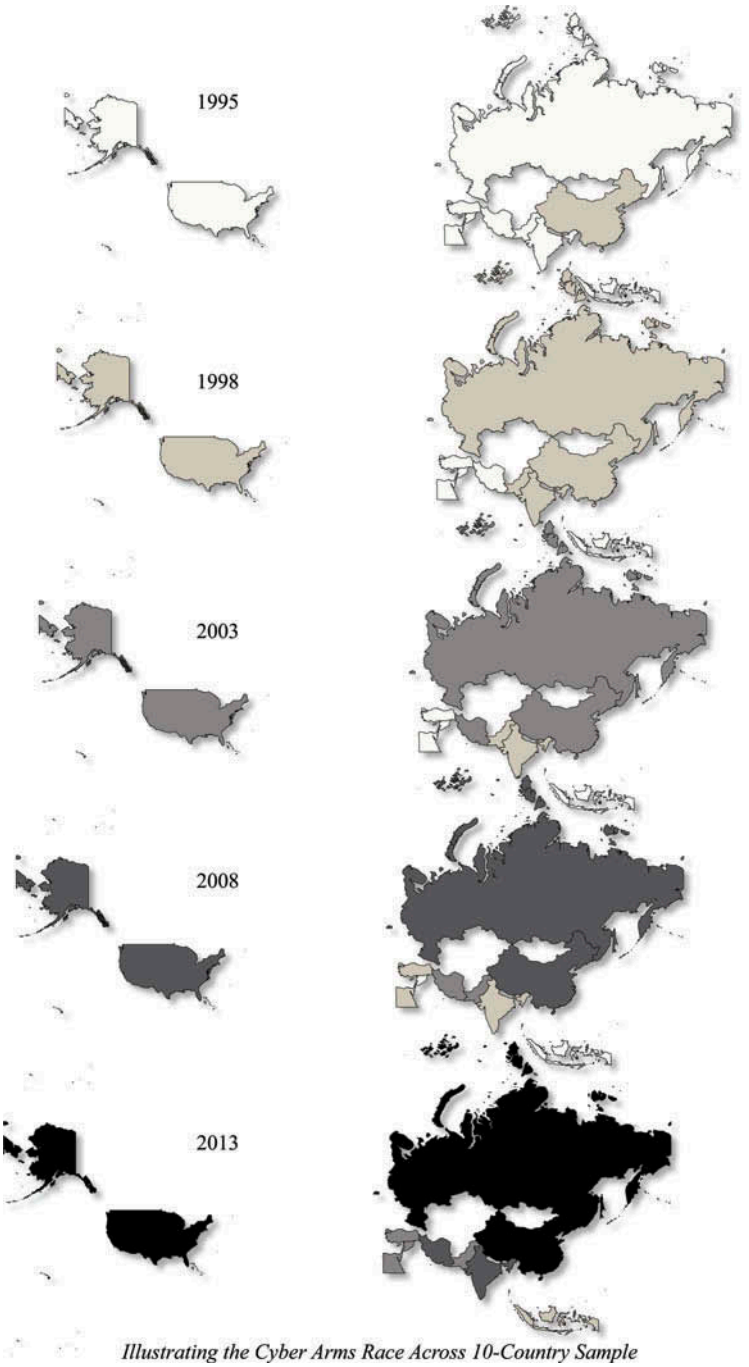

Figure 2: Mapping the security dilemma in cyberspace over time. *Source*: Aaron Brantly, "Cyber Capabilities by Country." http://bitsbytesrights.org/cyber-capabilities-by-country/

development of cyber capabilities of other nations over time following closely or relatively closely to regional and/or international influences. Increasing development of capabilities across the sample is evident in the last decade. Particular emphasis should be placed on the increasing development of capabilities in all nations following the cyber attacks against Estonia in 2007, the cyber attacks against Georgia in 2008, and the revelations in 2010 of the use of Stuxnet against Iran.

Figure 3 overlays the trends of cyber capability developments to further illustrate the trend in development both between major powers and, subsequently, within regional powers. There is a clear upward trend with little to no leveling off at any point in time once the security spiral is entered into.

Because our data is limited, we also wanted to seek confirmation of the general trends by finding a proxy measure. We have used media mentions of cyber within a country as a proxy measure of cyber capability development. The measure is inaccurate, and we were concerned only with confirming our general trend in development. Figure 4 illustrates a similar trend to our own dataset by providing contextual analysis of the term "cyber" and the country within the sample since 1995 across major media outlets as defined by LexisNexis.

Although not as accurate as our dataset on cyber capabilities, the media mentions of cyber in the context of the countries in our sample indicates a similar trend in awareness of cyber as an issue of importance across countries growing in prevalence, particularly in the last decade. The one glaring exception to the media-mention data is Indonesia. Indonesia in 1999 experienced a democratic transition of sorts with its first free election since 1955. There was also a large volume of cyber attacks that coincided with this election. Taking a

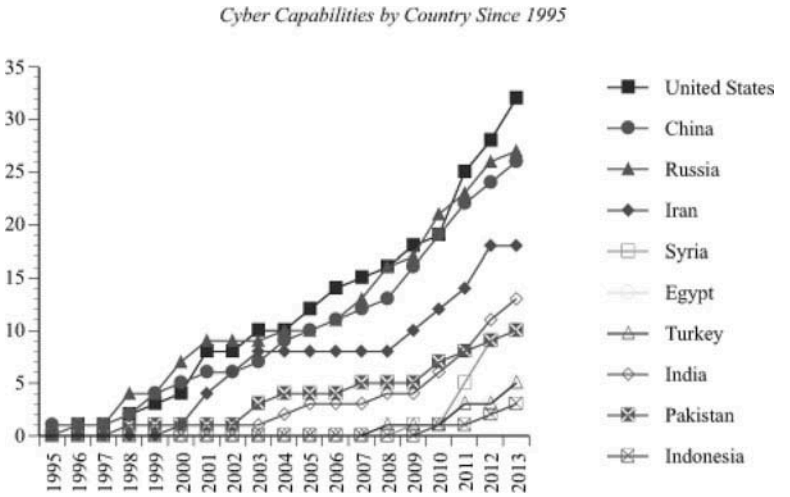

Figure 3: Overlay of country trends in cyber capability development across sample. *Source*: Aaron Brantly, "Cyber Capabilities by Country." http://bitsbytesrights.org/cyber-capabilities-by-country/

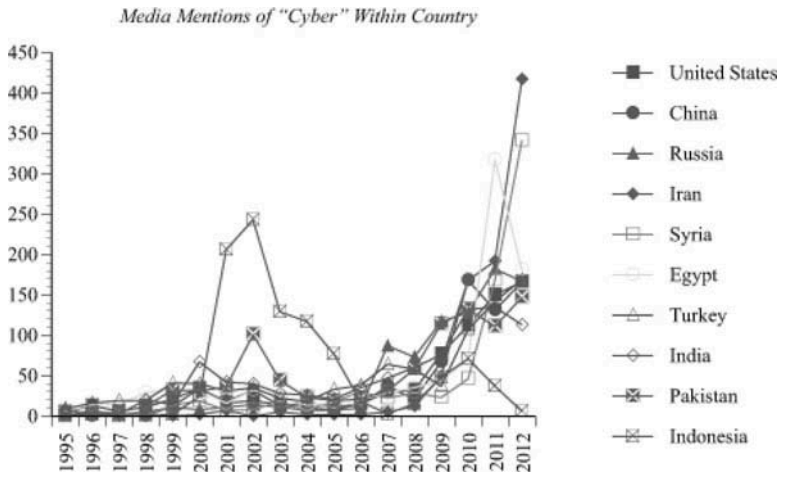

Figure 4: Media mentions of "cyber" and country in sample.

step back and examining the broad trends of 9 out of the 10 countries, we see a clear rise in the prominence of "cyber." Although the lexicon of the Internet has also changed over the years to more fully encompass the term "cyber," the general trend in attention largely matches the trend in cyber capability development by states within our sample.

The evidence of an increasing focus across the board by nations within our sample seems to indicate the existence of a security dilemma. States are developing and purchasing tools for offensive, defensive, and espionage uses in the cyber domain. The trend in both Figures 1, 2, and 3 mirrors sentiment expressed by Chrisella Herzon in the Diplomatic Courier when she writes, "Government officials cannot evolve on what protective defensive measures to implement fast enough to keep up with advances in technology, let alone hacker's techniques."[28] A recent issue of *Wired* magazine reiterates the evolving security dilemma in cyberspace by remarking on states: "in their willingness to pay top dollar for more and better zero-day exploits, the spy agencies are helping drive a lucrative, dangerous, and unregulated cyber arms race."[29]

Because cyberspace is both a domain of international interaction among nations and simultaneously between national governments and sub-state actors, there is a two-level game occurring. We argue that there is a correlation between the security dilemma occurring at the international level and a security dilemma between the state and its citizens. Not dissimilar from Robert Putnam's notion of two-level games in the formation of international agreements, there is a dynamic process of interaction of the international and domestic environments in the development of capabilities in cyberspace.[30] However, unlike Putnam's argument, the argument in cyberspace focuses more on individual and group relationships with the state rather than legislative representatives. Additionally, the interaction is, in large part, reversed with

respect to Putnam's argument, with events occurring on the international level having a significant effect on conditions at the national and subnational level. The next section focuses on the increasing prevalence of digital human rights violations and attempts to establish a correlative measure that corresponds to the development and purchase of state cyber capabilities.

DEFINING THE LOSERS

The data above goes a long way toward illustrating the presence of an evolving security dilemma in cyberspace. However, the argument above is predicated on a spiral of insecurity at the international level. Assuming that the trends are accurate and that the data presented indicate an evolving security dilemma at the international level, what effect does this have on sub-state actors? Much the same way conventional weapons can be turned against one's own people, so, too, can cyber weapons. The major differences between cyber and conventional weapons are found in their visibility and in their violence. A man standing in front of a tank in Tiananmen Square and a South Vietnamese soldier summarily executing a suspected communist are visible and violent examples of state oppression. These acts have a profound effect on those who bear witness. The same effect is not present when a blogger is arrested in the quiet of his home or a DDoS attack denies access to a communications platform for citizen mobilization.

The physical blocking of protestors marching to a central square in a city elicits a more profound psychological response than a similar action designed to prevent an online group from mobilizing. Just as the guns and tanks bought for external military use in the above examples were turned internally, so, too, can cyber tools and capabilities. Nations frequently prevent or limit the sale of certain types of arms for humanitarian or national security reasons.[31] However, despite significant evidence that Western companies are selling technologies that enable the surveillance, arrest, and manipulation of citizens under authoritarian regimes, rarely are companies prohibited from selling to nondemocratic states these capabilities.

"Internet freedom," the term popularized by former Secretary of State Hillary Clinton, is defined as "the freedom to connect—the idea that governments should not prevent people from connecting to the Internet, to websites, or to each other."[32] We hypothesize a correlation between the security dilemma and digital human rights. The externality of the cyber arms race is a general reduction in Internet freedom within countries globally. This reduction in Internet freedom is seen in several areas. First, it is seen in the development of filtering technologies to limit access of citizens to certain sites and resources in cyberspace. Second, it is seen in the development of surveillance mechanisms to monitor and track the online activities of individuals in cyberspace. Third,

it is visible in the increased number of arrests and prosecutions of individuals based on their activities in cyberspace.

Figures 5 and 6 illustrate our hypothesized relationship between increased state cyber capabilities and the related reductions in Internet freedom. The figures illustrating the relationship are not meant to be exact representations; they are stylized to reflect general associative trends.

We hypothesize a corresponding trend in the decline of aggregate Internet freedom with increases in state cyber capabilities. Because this trend is in its early stages and limited in scope, it is too early to make a causal argument linking the two trends.[33] However, we believe the evidence presented here illustrates a clear correlative relationship between the increasing development of capabilities by states and their subsequent use for political and human rights oppression within countries.

The first question that needs to be asked before fully delving into the data itself is, Why do states develop or purchase cyber capabilities and subsequently turn those capabilities against their own citizenry? We hypothesized above that states purchase and develop weapons to keep up in an anarchic structural environment. They are essentially forced to develop capabilities relative

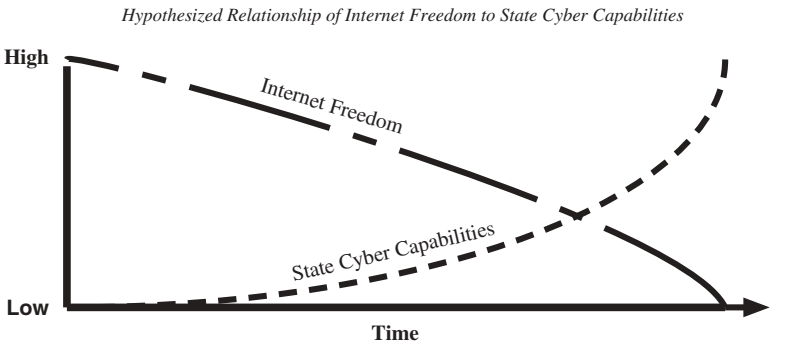

Figure 5: Corresponding trends of Internet freedom and state cyber capabilities.

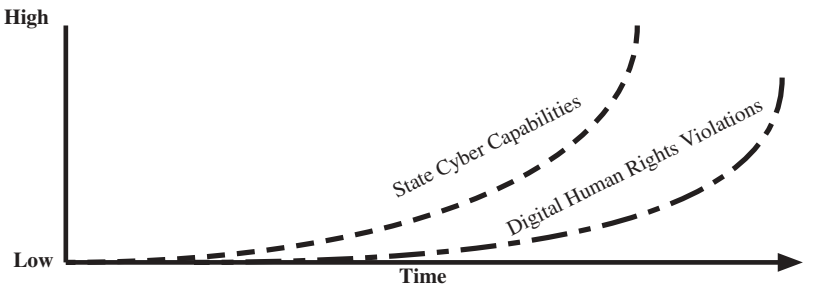

Figure 6: Corresponding trends of digital human rights violations and state cyber capabilities.

to their position. The specific tools and capabilities are likely developed with the intent of safeguarding against specific threats. Often this process of safeguarding comes in the form of classical deterrence or the creation of tools and capabilities to indicate a cost associated with a potential attack in the form of retaliation.[34] Whereas China, Russia, and the United States compete on a spectrum of high-level threats of attacks against systems and infrastructure, the development of lower-level surveillance and filtering capabilities are targeted against a different classification of perceived threats. These threats are targeted not at the technical infrastructure of the state or its military weapons systems as much as they are at the social and political foundations of the state itself. Therefore, although above we analyze the development of trends across all types of capabilities, the reality, upon nuanced examination, is that different tools are developed by different states for different reasons. Those states with the financial and technical capital to build the entire spectrum of tools in cyberspace are likely to do so.

By bringing to the forefront of global dialogue the concept of Internet freedom and, subsequently, the "Arab Spring" uprisings of the last several years, there has been an increasing call to arms by authoritarian regimes to develop or to purchase tools to minimize the likelihood of mass mobilization against the state. Gary King, Jennifer Pan, and Margaret Roberts illustrate in detail China's efforts at filtering and censorship.[35] They identify not a carte-blanche effort to censor and filter, but rather a strategic and tactical approach designed to provide the illusion of Internet freedom while maintaining tight control on those activities that might lead from cyberspace to the real world. The Chinese strategy is in line with stopping both internally instigated political or social movements and externally inspired ones.

There is ample evidence of political and military action by democratic countries against nondemocratic ones. One particular focus of democratic states is assistance in democratization or development of human rights in non- or less-than-democratic states. Although from a Western perspective, this assistance or intervention is well intentioned, it can also be perceived as invasive interference in the domestic sphere of influence. Increasingly, the influencing medium for human and democratic rights is not driven solely by external states. Instead, new technology platforms such as Google, Twitter, and Facebook provide access to information and tools for mobilization. Within this context, it should be noted that technology, although capable of facilitating citizen mobilization, is not sufficient in and of itself.[36]

Although the data in this field is still relatively limited, Figures 6 and 7 provide a breakdown of filtering by type across the countries in our sample by requests for removal of content by Google since 2009.[37] It should be noted that these are official requests of Google and do not include filtering, censorship, or other means to prevent the distribution of content.

This data is included not because it illustrates an increasing trend in takedown requests, but the reasons underlying those takedown requests. This is primarily to dispel any notions that the takedown requests are occurring solely for the purpose of removing illegal content. After having met with Google engineers, we are able to report that the removal requests are complied with both on the basis of local law, US law, and international law. The number and types of takedown requests included in Figure 7 are aggregate and include those requests Google denied. To understand the full relationship between increased cyber capabilities and the subsequent reductions in freedoms, it is necessary to have a holistic view and understand that one country's tool can be perceived as a weapon by another country.

Figures 8 and 9 demonstrate a trend in increasing requests by countries of Google to remove content.

The data presented in Figures 8 and 9 illustrates a continuous trend over the time period for which data is available of increasing requests for the removal of content both within countries and across the sample as a whole. This trend is consistent with our hypothesis of increased digital human rights violations as states develop tools and capabilities in the context of a cybersecurity dilemma. While not all content removal is equal, a trend in requests for removal suggests an evolution in removal over time. It is important to note that the content being taken down is not child pornography or other illegal content in most instances; instead, it is being taken down for many of the reasons associated with a lack of Internet freedom.

Another snapshot of the progression of digital human rights violations is derived through crowd-sourced reporting of Internet filtering, blockages, and DoS attacks. Crowd-sourced data is derived from Harvard's Berkman Center for Internet and Society's project, Herdict. Figures 10 and 11 illustrate reported blocked sites in each of the countries in our sample by country and across the sample starting in 2007. Here we have provided date only for countries within our sample. Because Herdict is crowd sourced, it is susceptible to potential

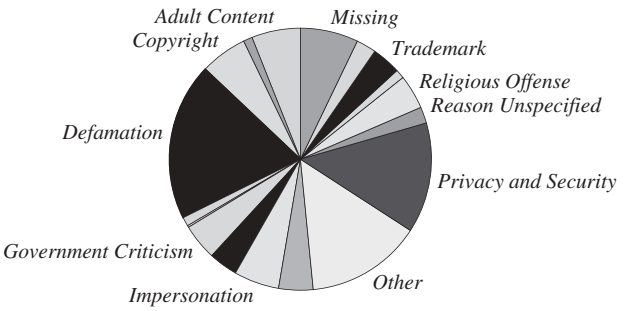

Figure 7: Reasons for Google content removal requests by countries in sample. *Source*: "Google Transparency Report," Google Inc. https://www.google.com/transparencyreport/

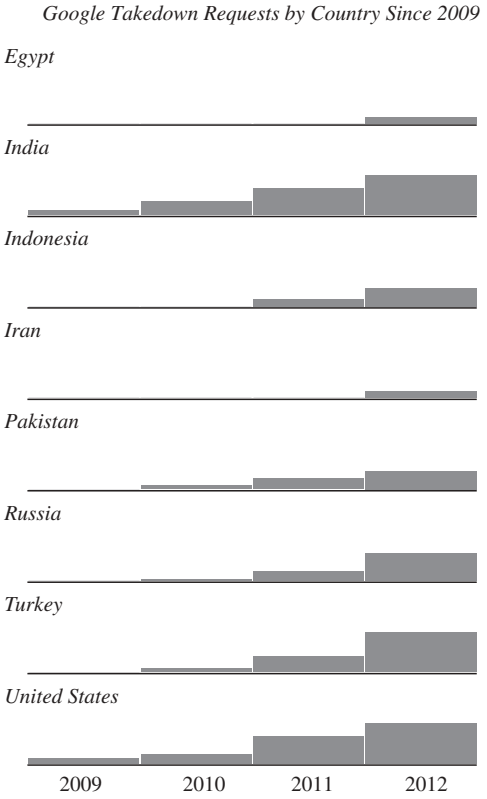

Figure 8: Requests trends by country within sample from 2009 through 2012. *Source*: "Google Transparency Report," Google Inc. https://www.google.com/transparencyreport/

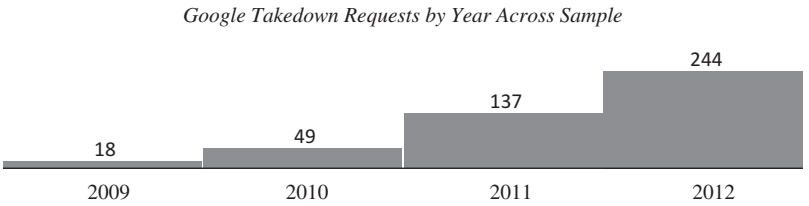

Figure 9: Request trends across sample from 2009 through 2012. *Source*: "Google Transparency Report," Google Inc. https://www.google.com/transparencyreport/

bias in countries where the project is more widely known and or accessible. However, the general trends should be maintained both within and across the sample.

Unlike Google requests, the reports from Herdict are likely to be more prevalent in times of political or social unrest. The data in Figure 10 in particular illustrate that targeted state interference on the Internet arises differently

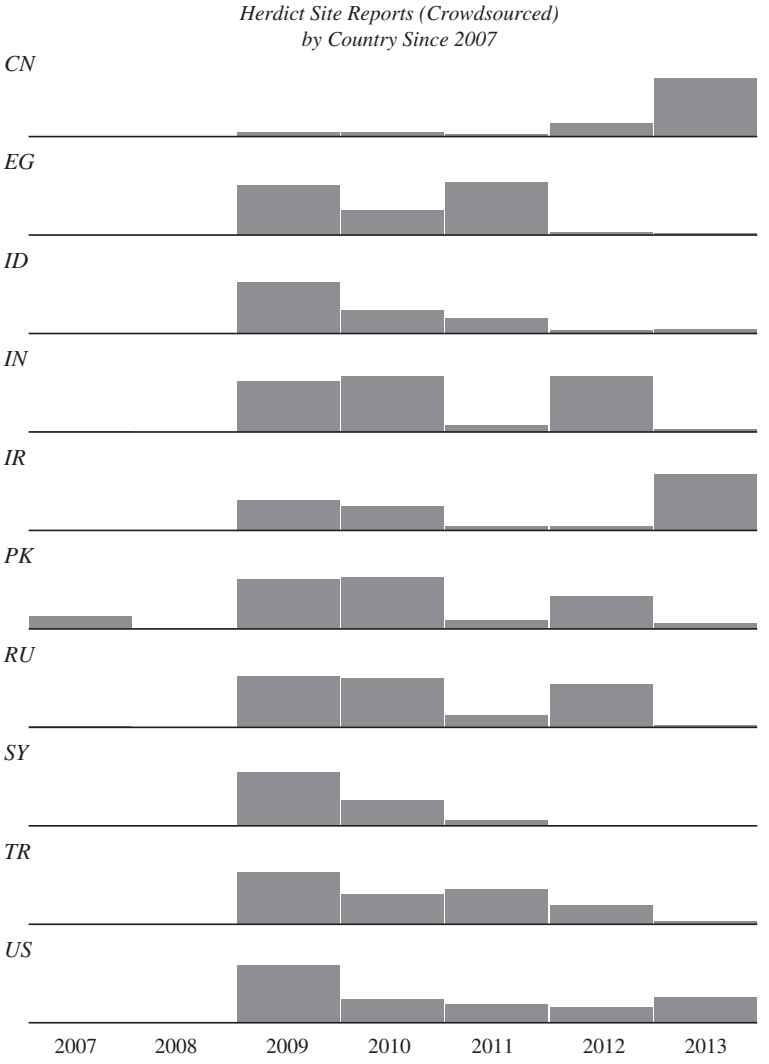

Figure 10: Crowd-sourced reports of Internet filtering, blockages, DoS attack by country and year since 2007. *Source*: "Herdict," Berkman Center for Internet and Society at Havard University. https://www.herdict.org/

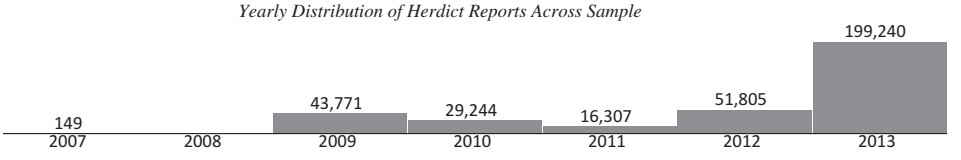

Figure 11: Crowd-sourced reports of Internet filtering, blockages, DoS attack across sample yearly since 2007. *Source*: "Herdict," Berkman Center for Internet and Society at Havard University. https://www.herdict.org/

at different times. The peaks and valleys correspond to events occurring within these countries, such as elections or news and events possibly leading to mass citizen mobilization. When the sample trend is examined in Figure 11, the general trend assumption is maintained in large part because of significant increases over time in reporting on Chinese Internet manipulation. After having met with the Herdict Project managers, they acknowledge the limitations of their data. They hope that a more consistent data measure can be generated that illustrates online censorship over time, yet they contend that on aggregate their data reflect the larger macro trends in censorship reasonably well.

Finally, to further illustrate the trend of increased pressure against human and democracy rights activists is the trend data from Philip Howard's dataset: When do States Disconnect Digital Networks? (WSDDN).[38] Within the WSDDN dataset, we have selected only countries within our sample. Figure 12 illustrates the expected trend in recent years toward increases in disconnection of networks for political reasons.

Figure 13 overlays sample trends across datasets for Google takedown requests, filtering and attacks, and network disconnection based on political reasons in comparison to our own dataset on cyber capabilities development. The data on capabilities and political disconnections are represented as bars, and the data from Google and Herdict are overlaid as lines.

Although the trend analysis is not perfect, the comparison across the three datasets representing digital and human rights violations appear to approximately match the general trend in the development or purchase of cyber capabilities by states. Absolute numbers are not comparable; rather it is the upward trends that we are most interested in. Absolute numbers are not comparable for the simple reason that one filtering technology developed or one computer network attack tool is capable of affecting multiple sites or computers. Our data overlaid with that of the data from several different

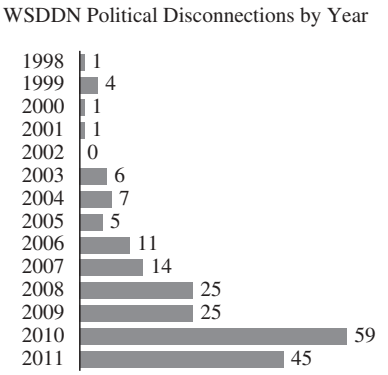

Figure 12: State disconnections of networks for political reasons since 1998. *Source*: Phillip Howard, "When Do States Disconnect Digital Networks (1995-2011)." Retrieved from http://pitpi.org/index.php/research/datasets/

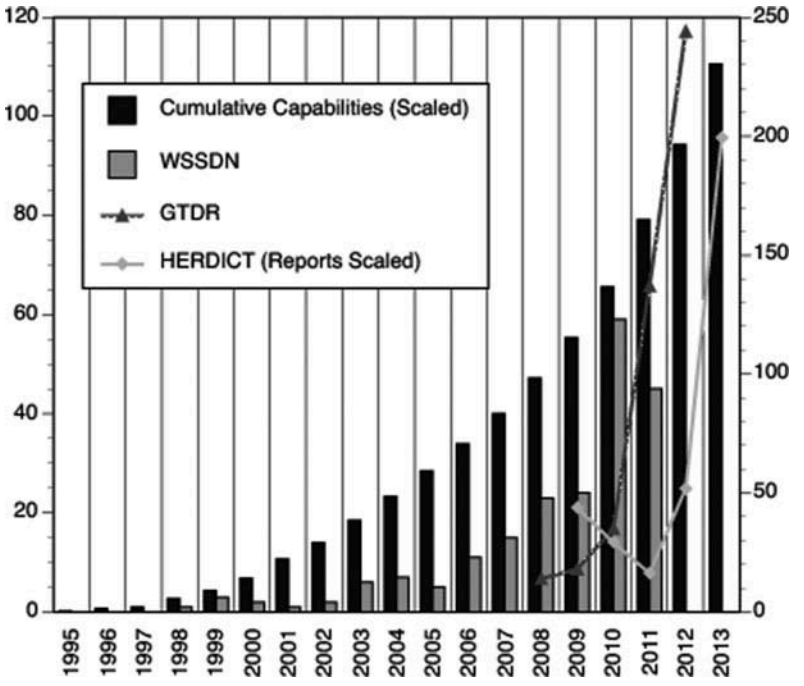

Figure 13: Overlay of data across datasets for general trend analysis.

datasets on digital human and political rights violations implies a correlative relationship between increases in state capabilities within the international environment and their subsequent use on domestic actors.

The data is incomplete and unbalanced across the sample and requires additional collection and analysis over time. Due to the limited nature of our data, we illustrate correlation only through the analysis of the common trends. However, the data we have amassed directly follows our hypothesized trend. Despite this simple anecdotal confirmation of our pattern, we are at present unable to determine a direct causal relationship. This isolation of a causal relation will be the purview of future research. Despite an inability to test causality, the data indicate the possibility of a negative externality of an international security dilemma in cyberspace affecting human and democracy rights activists. Even the possibility of this relationship is extremely important, and it has an enormous impact on human and democracy rights activists operating in or through cyberspace.

With the limited data available, we do identify what we believe to be the implications based both on our experiences in the field and the data we have analyzed. The next section offers up a series of implications for the interaction of the increasing security dilemma at the international level and its effect on domestic actors.

IMPLICATIONS OF THE CYBERSECURITY DILEMMA

We use the term "cyber losers" to describe the sub-state category of actors forced to compete with states in a quasi-anarchic environment. Roger Hurwitz notes that there is a depleted level of trust and cooperation because of significant disagreements about roles and responsibilities of states and other actors in cyberspace; in turn, this disagreement dramatically influences the common pool resource (CPR) of the Internet.[39] While Hurwitz indicates that this is a collective action problem, not all actors are created equally; resources are difficult to allocate efficiently, particularly when states have divergent goals and objectives. As our above analysis should indicate, some states are developing tools and capabilities that exceed those of others and those of sub-state actors as well.

Our primary focus is on human and democracy rights activists who use the Internet and associated technologies to advocate for a variety of causes ranging from democracy and rule of law to minority and women's rights. These individuals are not losers because their causes are not worthy of attention, and they are not losers because their messages are lacking in substance; they are losers because in a race of giants with deep pockets, it is activists who are struggling to keep up. Ron Deibert reiterates this sentiment throughout his recent book *Black Code: Inside the Battle for Cyberspace.*[40] The promise of the Internet was a domain where individuals could globally interact; they could communicate and share ideas freely. However, as our data above and the literature indicate, this space is becoming increasingly constrained.[41]

Rebecca Mackinnon poses the question in the context of a networked world: "How do we make sure that the people with control over our digital lives will not abuse that power?"[42] As governments engage one another in the cyber domain and enter increasingly into a spiral of insecurity, where do activists fall? Anja Kovacs and Dixie Hawtin further deepen the question by stating:

> Among the important issues that are obfuscated by the current lack of precision in cyber security debates is the fact that rivalries between states are among the chief security threats with the narratives of cyber war and cyber arms race rapidly gaining ground at the interstate level. In particular, a number of countries are investing heavily in developing offensive capabilities.[43]

Whereas in the 1980s it was predicted, "the Goliath of totalitarianism will be brought down by the David of the microchip," the reality is turning out to be something different.[44] There are optimists and pessimists on both sides of the fence, yet it is the pessimists who have the majority of the resources. The amount of money that states and corporations spend on purchasing computer system vulnerabilities, developing filtering technologies, and paying to manipulate the flow of content dwarfs the amount of money spent on technologies to circumvent or guard against these technologies. President Obama's

2013 budget proposal included $4.7 billion dollars for cybersecurity initiatives.[45] The massive allocation of funds by the United States to cybersecurity dwarfs the largest allocation of Internet freedom funds ever granted to the State Department in 2010, which maxed out at $30 million.[46] Figure 14 shows the relationship of US federal government spending in relative terms between the largest ever-allocated amount for Internet freedom and the current federal budget for cybersecurity.

The relative percentage of spending on cybersecurity in comparison to Internet freedom is 99.37 percent to .63 percent. The disparity in the relationship between security and freedom is astounding. More astounding is that the United States is the only country in our 10-nation sample that devotes any significant amount of money to Internet freedom. With billions of dollars being spent on cybersecurity by countries across a wide range of technologies, it is little wonder that independent actors would feel the pinch.

The United States, as one of the largest developers of cyber capabilities, leads the charge into the spiral of insecurity. The amount of funds and the pressure generated by a cybersecurity arms race is, as the anecdotal evidence would suggest, creating a negative externality—one which the United States has made only minimal efforts to combat. Thus, in an effort to secure cyberspace and generate a mechanism to spread democracy and capitalism around the world, it sowed many of the seeds of the current problems.

Does this mean that the United States should halt development of its offensive and defensive cyber programs? No—a country that gives up ground in a security dilemma, according to the literature, would suffer adverse consequences to its relative security. Yet, as a promoter of democracy and human rights globally, the United States necessarily needs to be cognizant of the

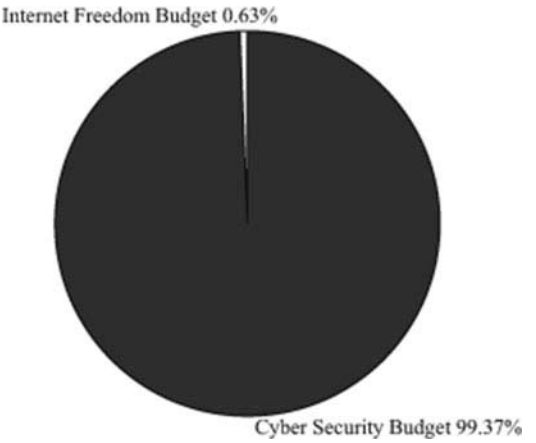

Figure 14: Comparison of largest ever Internet freedom budget FY-2010 to FY-2013 cybersecurity budget.

environment being created by this security dilemma. Cognizance helps policy makers to orient their priorities. If the Internet is to be a critical domain in facilitating freedom of connection and expression, then the United States needs to organize its resource allocations accordingly.

Human rights and democracy activists lose in cyberspace not for a want of trying. They lose because it is a multivector attack environment in which they struggle to keep up. They are fighting hundreds of battles all at the same time. The technologies that were once meant to liberate are now constraining. An activist who links to his or her contacts on Facebook has now compromised not just one link in a network, but rather the entire network. Documents on organizations and activities, which were once accessible only by raiding an office, are now available through cyber attacks such as GhostNet. Organizing democracy and human rights projects in cyberspace is increasingly difficult.

We believe we have taken the first steps down the path of illustrating the presence of a security dilemma in cyberspace, and second, identifying the negative externalities this security dilemma generates with respect to increased censorship, filtering, oppression, and other hostile acts directed against domestic actors.

Is there any hope? There is, indeed, a growing group of actors attempting to provide solutions for the continuance of democracy and human rights activities. Organizations such as Tor, Guardian Project, Whisper Systems, New America Foundation, CitizenLab, the National Democratic Institute, and many others, to name but a few, are devoting resources to develop technologies and to train activists on digital security around the world.

Among these projects, one of the most successful is Tor. Tor has been working with funding from various organizations, including the US government, for years to develop a secure means for individuals to access the Internet and communicate on a regular basis. More recently, there have been entire bootable software packages, including the Tails package, created to provide activists and journalists around the world a secure means by which to access the Internet on their own computer or computers at cyber cafes. Tails even comes with a Windows "cloaking" mode that disguises the operating system to look like Windows XP. The Guardian Project produces a range of products funded by US grants. The Guardian Project's work includes secure chat tools, tools to obscure photographs, private web-browsers, and panic buttons.

Organizations such as the National Democratic Institute and Internews, to name just two, train individuals around the world on the use of secure communications and the proper use of technology to protect them against potentially repressive governments. The University of Toronto's CitizenLab and Harvard's Berkman Center monitor and track issues such as censorship and surveillance on the Internet; in the process, they provide a valuable data resource for policy makers to name and shame states.

These organizations are providing valuable tools, trainings, and data. Yet at the same time these organizations are competing against nation-states and corporations with substantial human and financial resources. If an activist fails to secure his or her activities online, it can mean the difference between freedom or incarceration. The stakes in the spiral of security at both the international and sub-state level are extremely high.

NOTES

1. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214.

2. Larry Diamond and Marc Plattner, *Liberation Technology: Social Media and the Struggle for Democracy* (Baltimore: Johns Hopkins University Press, 2012).

3. Ibid.

4. Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century* (New York: Farrar, Straus and Giroux, 2005).

5. Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), Kindle Locations 163–164.

6. See Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, MA: MIT Press, 2009) for a discussion of Internet governance.

7. Throughout the article, the reference to "states" relates directly to sovereign territories in the context of the Peace of Westphalia.

8. Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781–799.

9. Richard Clarke and Robert Knake *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010). This incident is also cited by Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011). However, both take as their root public source: Gus W Weiss. Central Intelligence Agency Washington, DC, Center for the of Study Intelligence. *The Farewell Dossier.* Ft. Belvoir: Defense Technical Information Center, 1996. All cited authors were potentially in positions to thoroughly investigate the validity of the claims.

10. Ibid.

11. Alan Campen, *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International Press, 1992).

12. Christopher Bronk, "Blown to Bits: China's War in Cyberspace, August–September 2020," *Strategic Studies Quarterly* 5, no. 1 (2011): 1–20.

13. Jervis, "Cooperation under the Security Dilemma," 167–214.

14. Hans Morgenthau, *Politics among Nations; the Struggle for Power and Peace* (New York: Knopf, 1967); Kenneth Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); John Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001).

15. William Hardy McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000* (Chicago: University of Chicago Press, 1982).

16. John Mearsheimer, *The Tragedy of Great Power Politics*.

17. It is important to remember that the Internet is a physical as well as a virtual space. There are physical choke points where cables actually cross from one nation to another, creating an actual physical boundary between states.

18. Herbert Lin, "Laying an Intellectual Foundation for Cyberdeterrence: Some Initial Steps" in Jörg Krüger, Bertram Nickolay, and Sandro Gaycken. *The Secure Information Society Ethical, Legal and Political Challenges* (New York: Springer, 2013), Kindle Locations, 308–311.

19. Lin, Kindle Locations, 324–326.

20. Jervis, "Cooperation under the Security Dilemma," 167–214.

21. James Lewis, "Significant Cyber Events since 2006," Center for Strategic and International Studies, http://csis.org/publication/cyber-events-2006.

22. "Microsoft Security Intelligence Report," Microsoft.com, July 7, 2013, http://www.microsoft.com/security/sir/default.aspx.

23. Andrew Colarik and Lech Janczewski, "Establishing Cyber Warfare Doctrine," *Journal of Strategic Security* 5, no. 1 (2012): 31–48.

24. James Andrew Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization" (Washington, DC: Center for Strategic and International Studies, 2011); Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness around the World," Security and Defense Agenda, 2012.

25. Jeffrey Carr and Lewis Shepherd, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010).

26. "Bugged Planet," July 7, 2013, http://buggedplanet.info/index.php?title=Main_Page.

27. William Hardy McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*.

28. Chrisella Herzog, "Duck and Cover: Cyber Instability," *Diplomatic Courier* 6, no. 6 (2012): 27.

29. James Bamford, "The Secret War," *Wired*, July 7, 2013, http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/.

30. Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42, no. 3 (1988): 427–460.

31. "Arms Embargoes Database," edited by Stockholm International Peace Research Institute, Stockholm, 2013.

32. "Remarks on Internet Freedom," United States Department of State, July 7, 2013, http://www.state.gov/secretary/rm/2010/01/135519.htm.

33. The scope is limited due to a spread in information communications technology capacity across nations. As ICT, in particular Internet penetration reaches saturation there is an increasing demand for cyber capabilities.

34. Lin, Kindle Locations, 308–311.

35. Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticisms but Silences Collective Expression," *American Political Science Review* 107, no. 2 (2013): 1–18.

36. Chris Bronk, "Laying an Intellectual Foundation for Cyberdeterrence: Some Initial Steps," in Jörg Krüger, Bertram Nickolay, and Sandro Gaycken. *The Secure Information*

Society Ethical, Legal and Political Challenges (New York: Springer, 2013), Kindle Locations, 83–84.

37. "Google Transparency Report," Google Inc., July 7, 2013, https://www.google.com/transparencyreport/.

38. Phillip Howard, "When Do States Disconnect Digital Networks (1995–2011)," July 7, 2013, http://pitpi.org/index.php/research/datasets/.

39. Roger Hurwitz, "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly*, Fall (2012): 20–45.

40. Ronald Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013).

41. Ronald Deibert, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT, 2007); Ronald Deibert, Palfrey John G. Rohozinski Rafal Zittrain Jonathan, OpenNet Initiative, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010).

42. Rebecca MacKinnon, *Consent of the Networked: The World-Wide Struggle for Internet Freedom* (New York: Basic Books, 2012), 18.

43. Anja Kovacs and Dixie Hawtin, "Cyber Security, Cyber Surveillance and Online Human Rights," in *Stockholm Internet Forum* (Stockholm: Global Partners & Associates, 2013).

44. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 49.

45. Danielle Walker, "Obama Proposes $800m Cyber Budget Increase for Pentagon," *SC Magazine Online*, July 7, 2013, http://www.scmagazine.com/obama-proposes-800m-cyber-budget-increase-for-pentagon/article/288672/.

46. Mary Beth Sheridan, "Congress Trims State's Internet Freedom Funds," *Washington Post*, July 7, 2013, http://articles.washingtonpost.com/2011-04-13/world/35230216_1_internet-freedom-freedom-funds-circumvention-technology.