Clash of Threat Perceptions: In Nuclear and Cyber Paradigms

Rustam Goychayev

A thesis

submitted in partial fulfillment of the

requirements for the degree of

Master of Arts in International Studies

University of Washington

2014

Committee:

Christopher D. Jones

Scott Radnitz

Program Authorized to Offer Degree:

Jackson School of International Studies

University of Washington

Abstract

Clash of Threat Perceptions: In Nuclear and Cyber Paradigms

Rustam Goychayev

Chair of the Supervisory Committee:
Associate Professor Christopher D. Jones
Jackson School of International Studies

Similar to the discovery of fission, the advent of the Internet led to the dual-use nature of cyber technology. One path is the 'peaceful, commercial' use of the technology; the other is the 'weapons' path. As with nuclear technology, states quickly capitalized on cyber advancements in order to weaponize the technology. Despite the many dangers associated with cyber aggression, a treaty to curb the potential cyber war between nations has not yet materialized in the international arena. Even during the height of the Cold War, bilateral cooperation between the United States and the former Soviet Union gave birth to one of the most successful multilateral treaties the world has ever seen, the NPT. Today, conversely, cooperation between the United States and the Russian Federation, as well as the United States and People's Republic of China, on the subject of international cyber legislation is fairly limited. This could be because during the advent of nuclear weapons, both the United States and the former Soviet Union perceived other states acquiring nuclear weapons as a direct *external* threat to their power and, possibly even

existence, forcing them to cooperate. However, cyber technology creates threats from two fronts: *external* and *internal*. Aside from the ability to attack another state's networks, cyber weapons have the ability to challenge the existing authoritarian governments in a form of massive mobilization and information campaigns aimed against the regime through social media and other tools. This poses a dilemma for authoritarian state leaders who may be more concerned about *internal* challengers over *external* challengers. Thus, it is possible that the real reason for the lack of cooperation between states is the fact that the powerful states on the international area cannot find a *common threat* in the cyber paradigm due to the fundamental difference in their regime construction. It is my hypothesis that the biggest hurdle to an NPT type cyber treaty is the different types of threats each paradigm presents. Accordingly, the purpose of this paper is to address the question of how states balance *internal* and *external* threats, and how that differs by regime type.

Clash of Threat Perceptions:

IN NUCLEAR AND CYBER PARADIGMS

By Rustam Goychayev
Jackson School of International Studies, University of Washington

Table of Contents

Part I: Introduction 1

Part II: The Two Paradigms 6

Part III: The Enemy 26

Part IV: The Data 38

Part V: Conclusion 59

Appendix I 63

Appendix II 65

Part I: Introduction

In 1921, Albert Einstein won a Nobel Prize in physics for his discovery of the photovoltaic effect. In 1934, Edward Teller was rescued from Germany and later devised a spherical implosion of a plutonium pit, leading to his solving the central problem of H-Bomb Design. Lise Meitner and Otto Hahn of Berlin discovered nuclear fission in 1938; and in 1942, Enrico Fermi initiated the first chain-reacting nuclear pile, thereby opening the door to plutonium production and the explosion of the first nuclear weapon.[1] The bombings of Hiroshima and Nagasaki furthered nuclear weapons research and development for many countries all across the world.[2]

When proliferation of nuclear technologies became an obvious problem, the newly formed United Nations General Assembly proposed its first ever resolution to the problem known as the Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy; from this came the Atomic Energy Commission (AEC) in 1946. Ultimately, the AEC's success was hindered by controversy and political gridlock. Accordingly, on December 8, 1953, the next substantial movement towards international cooperation on regulating nuclear energy came about during President Eisenhower's address to the U.N. General Assembly. In his speech, President Eisenhower proposed the main pillars of the International Atomic Energy Agency (IAEA) and Nuclear Non-Proliferation Treaty (NPT). His address to the U.N. General Assembly became known as 'Atoms for Peace' and in it, President Eisenhower constructed the three pillars that would become the core principles of the NPT. The first pillar prevents proliferation (Articles I, II, III), the second pillar encourages peaceful use of nuclear

[1] Thomas Reed and Danny Stillman, The Nuclear Express: A Political History of the Bomb and Its Proliferation (Zenith Press, n.d.), 8.
[2] Richard Rhodes, Arsenals of Folly: The Making of Nuclear Arms Race, First (Alfred A. Knopf, 2007), 70.

energy (Articles IV and V), and the third pillar disarms existing stockpiles of nuclear weapons (Article VI).[3]

Despite these movements forward, proliferation fears remained strong. In 1963, President John F. Kennedy said that he feared by the end of the1970s, there could be considerable proliferation of nuclear weapons with up to twenty nations possessing the ultimate weapon.[4] To prevent the nightmare envisioned by President Kennedy, the two nuclear superpowers – the United States and the Soviet Union – worked together to implement non-proliferation agreements and safeguards for the world to abide by. In 1968, the NPT was ready for signatures and in 1970 it entered into force.

In essence, the NPT was a grand bargain between the nuclear states and the non-nuclear states. The non-nuclear states agreed to give up their ambitions towards acquiring nuclear weapons, while the nuclear states agreed to complete disarmament of existing nuclear arms. All treaty members maintained the "inalienable right" to seek nuclear material for peaceful purposes.[5] It is important to note that in his book, *Interpreting the Nuclear Non-Proliferation Treaty*, Daniel Joyner stresses that "it became clear that the treaty would need to maintain a careful balance between these three principles, so that no one principle could ever disproportionately impose itself upon the others."[6] Parties further agreed to keep the treaty in force for twenty-five years, after which it would be revisited and its progress assessed to

[3] Daniel Joyner, Interpreting the Nuclear Non-Proliferation Treaty (Oxford Press, n.d.), 6–11.
[4] Thomas Graham, Unending Crisis: National Security Policy After 9/11 (University of Washington Press, 2012), 171.
[5] Joyner, Interpreting the Nuclear Non-Proliferation Treaty, 67.
[6] Ibid., 19.

determine whether or not it should be made permanent by a majority vote.[7] In the run up to the 1995 revalidation deadline, it was an uphill battle to convince the Non-Aligned Movement (NAM) that substantial progress had been made in the disarmament process. Eventually, however, the NPT was extended indefinitely.

Even during the height of the Cold War, bilateral cooperation between the United States and the former Soviet Union gave birth to one of the most successful multilateral treaties the world has ever seen, the NPT. Today, conversely, cooperation between the United States and the Russian Federation, as well as the United States and People's Republic of China, on the subject of international cyber legislation is fairly limited. This could be because during the advent of nuclear weapons, both the United States and the former Soviet Union perceived other states acquiring nuclear weapons as a direct *external* threat to their power and, possibly even existence, forcing them to cooperate. However, cyber technology creates threats from two fronts: *external* and *internal*. Aside from the ability to attack another state's networks, cyber weapons have the ability to challenge the existing authoritarian governments in a form of massive mobilization and information campaigns aimed against the regime through social media and other tools. This poses a dilemma for authoritarian state leaders who may be more concerned about *internal* challengers over *external* challengers. The real intent of cyber treaty legislation proposals is evident in the language of the proposals. According to Tom Gjelten, for example, the Russian and Chinese draft treaty agreement "that cited the Russian U.N. resolution and elaborated on it," and was approved by all members of the Shanghai Cooperation Organization (SCO),

[7] Thomas Graham, Disarmament Sketches: Three Decades of Arms Control and International Law (University of Washington Press, 2002), 258.

> "[s]eemed to justify censorship of dissident writings on the Internet and bar countries from supporting such Internet activity in another state. The signatory countries resolved to work for 'collective measures' that incorporated those ideas. U.S. officials interpreted the agreement as expressing the Russian and Chinese vision of what a U.N. cyber arms control agreement should entail, and they suspected the accord was concluded with the idea that it might serve someday as a source of customary international law, which arises through accepted precedents and practices rather than through formal conventions."[8]

Thus, it is possible that the real reason for the lack of cooperation between states is the fact that the powerful states on the international arena cannot find a *common threat* in the cyber paradigm due to the fundamental difference in their regime construction. This threat perception difference in the nuclear and cyber paradigms seem to be the least discussed. This paper is a product of that neglect and seeks to remedy this issue. Even though other important similarities and differences have been highlighted by various scholars at length, and will be discussed in the next chapter, I will focus on the question of how states balance *internal* and *external* threats and how that differs by regime type. My hope is that in exploring this question I will be able to contribute to and shed some light onto the debate surrounding the lack of an international cyber treaty.

[8] Tom Gjelten, "Shadow Wars: Debating Cyber & Disarmament" World Affairs Journal, accessed November 16, 2013, http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament.

Part II: The Two Paradigms

The story of cyber technology is similar to that of nuclear technology; however, it is also incomplete. In 1969, the first data travelled between computers – from UCLA to Northern California – using ARPANET, an ancestor of the Internet. Similar to the discovery of fission, the advent of the Internet led to the dual-use nature of this advancement. One path is the 'peaceful, commercial' use of the technology; the other is the 'weapons' path. As with nuclear technology, states quickly capitalized on cyber advancements in order to weaponize the technology. Despite the many dangers associated with cyber aggression, a treaty to curb the potential cyber war between nations has not yet materialized in the international arena. The many reasons as to why this is the case will be discussed at a later point in this introduction.

In a book entitled, *Cyber War: The Next Threat to National Security and What to do About It*, Richard Clarke and Bob Knake provide a vivid description of the dangers associated with a cyber-attack. As it pertains to the vulnerable United States infrastructure, Clarke and Knake write:

> "You look at your watch. It's now 8:15 p.m. Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting […] Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. Freight trains have derailed outside major junctions and marshaling yards on four major railroads. Aircraft are literally falling out of the sky as a result of midair collisions across the country. Pipelines carrying natural gas to the Northeast have exploded, leaving millions in the cold. The financial system has also frozen solid because of terabytes of information at data centers being wiped out. Weather, navigation, and communications satellites are spinning out of their orbits into space. And the U.S. military is a series of isolated units, struggling to communicate with each other. Several thousand Americans have already died, multiples of that number are injured and trying to get to the hospitals."[9]

Clarke's and Knake's description is frightening (and maybe even a little sensationalist). A more measured description of the dangers associated with cyber-attacks can be found in recent history.

[9] Richard Clarke and Rob Knake, Cyber War: The Next Threat to National Security and What to Do About It, 1st ed. (HarperCollins Publishers, 2010), 67.

Perhaps the most prominent example of cyber war discussed by scholars is the 2007 cyber-attacks against Estonia. In late April 2007, the Estonian government began work to relocate a monument dedicated to Soviet troops from a busy intersection in central Tallinn to a nearby military cemetery.[10] According to Rain Ottis, author of a paper entitled *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, the statue became the symbol of tension between the local pro-Kremlin Russian minority movement – which saw the monument as a representation of the 'liberator' – and the Estonian nationalist majority movement – which saw the monument as a representation of the 'oppressor.' During the first day of work on the relocation project, Tallinn saw protests and riots, which were eventually subdued by police control. April 27th, however, was the beginning of a cyber-attack against the country that lasted a total of 22 days. According to the Center for Strategic & International Studies report, the damage of these attacks was that "[s]ome government online services were temporarily disrupted and online banking was halted."[11] The report adds that these attacks resembled more of a cyber riot than a crippling attack. What made Estonia particularly vulnerable to cyber-attacks, according to Ottis, was that it is "highly networked, so a wide scale attack on the availability of public digital services has a significant effect on the way of life of ordinary citizens and businesses alike."[12] Due to this reality of Estonia being highly reliant on digital services, writes Ottis, "these cyber attacks cannot be disregarded as mere annoyances but should be considered a threat to national security."[13] Estonian Defense Minister Jaak Aaviksoo even went as far as comparing the attacks to terrorist acts.[14] To Estonia these attacks were

[10] Matthew (editor) Warren and Rain Ottis, eds., Case Studies in Information Warfare and Security for Researchers, Teachers and Students (Academic Conferences and Publishing International Limited: United Kingdom, 2013), 121.
[11] George Perera, "Purposefully Manufactured Vulnerabilities in US Government Technology Microchips: Risks and Homeland Security Implications" (Monterey, California. Naval Postgraduate School, 2012), 1, https://calhoun.nps.edu/public/handle/10945/27886.
[12] Warren and Ottis, Case Studies in Information Warfare and Security for Researchers, Teachers and Students, 122.
[13] Ibid.
[14] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," Survival 53, no. 1 (February 2011): 32, doi:10.1080/00396338.2011.555586.

far more serious than just mere cyber riots. As a North Atlantic Treaty Organization (NATO) member, Estonia pushed to invoke Article V of the treaty – which, in general, states that an attack on one of the NATO members is an attack on all members – but NATO refused to declare that Russia was behind the attacks.

An even more recent but similar event took place during the conflict between Russia and Georgia in 2008. South Ossetian rebels provoked a conflict with Georgia by sending missiles into Georgian villages.[15] The Georgian army responded by bombing the South Ossetian capital city followed by an invasion. The Russian army quickly moved to eject the Georgian army out of South Ossetia. As the army moved in to battle, so did the cyber warriors. By utilizing the Distributed Denial of Service (DDoS) technique, a technique in which an internet site, a server, or a router is flooded with more requests for data than the site can respond to or process,[16] the Russian cyber army was able to shut down government websites, paralyze the Georgian banking sector, and disable the mobile phone system. All of this was occurring as Georgia was being bombed. The most disturbing part of the whole episode is not what *was* done but indeed what *was not* done during the conflict. Clarke and Knake write that "those operations do not begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace. The Russians, in fact, showed considerable restraint in the use of their cyber weapons […] The Russians are probably saving their best cyber weapons for when they really need them, in a conflict in which NATO and the United States are involved."[17]

[15] Richard A. Clarke, Cyber War: The next Threat to National Security and What to Do about It, 1st Ecco pbk. ed (New York: Ecco, 2012), 18.
[16] Clrake and Knake, Cyber War: The Next Threat to National Security and What to Do About It, 284.
[17] Clarke, Cyber War, 21.

It is clear, from recent empirical evidence and educated assessments regarding the damaging effects future cyber conflicts could bring about, that cyber-attacks or cyber war against a nation can have a devastating impact. This is not the first time the international community has encountered a menace as grave as the cyber threat. During the Cold War, cities across the United States lived under a shadow of a nuclear annihilation. Why has the international community not approached this threat in the same way it approached the nuclear threat? While the international community was able to come together on the issue of nuclear security, it is unable to do the same for the cyber security paradigm. What is preventing the international community from adopting an NPT type treaty to reduce the threat of cyber war? In order to answer this question, we must first explore the similarities and differences between these two threats.

Some elements of the nuclear threat are strikingly similar to the cyber threat. For instance, the way in which Russia became interested in acquiring nuclear weapons is similar to the way in which the Chinese became interested in cyber technology and advancing their war fighting capabilities. More specifically, towards the end of WWII, the United States dropped two nuclear bombs on Japan. In *The Nuclear Express*, authors Thomas Reed and Danny Stillman state that "only with the bombing of Hiroshima and Nagasaki did Stalin come to appreciate the political significance of those weapons."[18] The bombings also proved to be the catalyst for nuclear weapons research and development for many countries all across the world.[19] In 1991, the world, and in particular China, was watching as the first Gulf War, also known as operation Desert Storm, was unfolding. For the first time, the United States military embraced the use of computer networks to target the Iraqi army by introducing "smart bombs" to the battle field. As Clarke and Knake point out, "[d]esigned to

[18] Reed and Stillman, The Nuclear Express: A Political History of the Bomb and Its Proliferation, 29.
[19] Rhodes, Arsenals of Folly: The Making of Nuclear Arms Race, 70.

replace traditional bombs that required many missions and many tons of munitions dropped to destroy a target, 'smart bombs' were designed to put one bomb, and one bomb only, precisely on each target every time."[20] Watching the war unfold, the Chinese understood that this was the direction warfare was moving towards, and worse, that they were decades behind.[21] The United States' ground war lasted one hundred hours, following thirty-eight days of air strikes that resulted in decisive victory for the United States. Saddam Hussein's army was the fourth-largest in the world whose weapons were Soviet made, just like China's.[22] As Clarke and Knake point out, "[The Chinese] soon began referring to the Gulf War as *zhongda biange*, 'the great transformation.' […] Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability and also thought that it might itself be targeted by cyber war."[23] The first Gulf War was to China what the bombings of Hiroshima and Nagasaki were to Stalin's USSR.

There is also a similarity in which the two weapons can be used in a devastating fashion. It is important to preface this paragraph by noting that I recognize that there is a vast difference between disruptions of critical infrastructure, economy, and military's defensive and offensive capabilities and that of an attack by an X megaton nuclear warhead on a major city, which leaves hundreds of thousands of people dead instantly and the destruction of buildings at an unimaginable scale. Yet, it is important to note that the effects of cyber warfare should not be taken lightly as they can turn the tide of a battle leading to loss of life, economy, and military assets. As Jeffrey Carr, author of *Inside Cyber Warfare*, writes "[cyber attack cannot in and of itself rise to the level of a nuclear attack], but a

[20] Clarke and Knake, Cyber War: The Next Threat to National Security and What to Do About It, 48.
[21] Ibid., 49.
[22] Ibid.
[23] Ibid., 49, 54.

sufficiently large-scale cyber attack that takes down critical networks and in return results in systemic failures of safety systems at nuclear power plants could have devastating consequences, including loss of life."[24] As substantial progress was being made in the realm of cyber technology and warfare techniques, the world saw such advancements applied on the battlefield in a more devastating manner as highlighted earlier with the examples from Estonia and Georgia. The Israeli bombing of Syria's secret nuclear site in 2007 – what Carr calls "maybe one of the most successful known acts of cyber warfare"[25] – is another such example. Syria spent billions of dollars on its Russian built air-defense systems and yet Israeli non-stealthy jets were not only able to penetrate Syrian airspace, but they were also able to attack the intended target and fly back home completely unharmed. How could this be? The Syrians eventually realized that their radar systems were hacked and that the images they were seeing on their radars were placed there by the Israeli military.[26] The air-defense systems could not shoot down planes that, according to their radars, were never there. It is not hard to imagine the devastating strategic insecurity such an attack would create for the victim state.

Another example of the powerful ability of a cyber-attack, which stands out in both its sophistication and execution, is the now famous Stuxnet example that targeted Iran's nuclear program. As it turns out, Stuxnet had two variants: the original code and the updated version. The knowledge of the date (or even the year) when either version of Stuxnet became operational is not concrete. The general consensus, however, is that Stuxnet could have been in use as early as 2005.[27] Counterintuitively, the original version of the code is far more complex and sophisticated than the

[24] Jeffrey Carr, Inside Cyber Warfare, 2nd ed (Beijing ; Sebastopol, CA: O'Reilly, 2012), 33.
[25] Clarke, Cyber War, 251.
[26] Ibid., 5.
[27] Lee Ferran and Kirit Radia, "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet," ABC News Blogs, July 9, 2013, http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/.

updated version. Developed jointly by the United States and Israel,[28] Stuxnet's original code attacked Iran's gas centrifuges by denying the flow of gas out of each chosen cascade and thereby raising the pressure of the centrifuges. Ralph Langner, author of *Stuxnet's Secret Twin*, refers to this attack variation as the 'overpressure attack.' As described by Langner,

> "Gas centrifuges for uranium enrichment are extremely sensitive to increases of pressure above near vacuum. An increase in pressure will result in more uranium hexafluoride getting into the centrifuge, putting higher mechanical stress on the rotor. Rotor wall pressure is a function of velocity (rotor speed) and operating pressure; more gas being pressed against the rotor wall means more mechanical force against the thin tube. Ultimately, pressure may cause the gaseous uranium hexafluoride to solidify, thereby fatally damaging centrifuges."[29]

What is brilliant about these attacks is that the code was designed to hide its tracks by recording stable functionality of the centrifuges before executing the attacks, then playing back the recording during the attack leaving facility operators completely oblivious to the fact that anything is wrong, while at the same time facility's infrastructure was being physically damaged. Further brilliance of the execution of the Stuxnet's code is evident in the decision by the attackers to abort each attack sequence just before total destruction of the centrifuges was achieved, thereby increasing rotor stress and causing rotors to break early – not coinciding with the waves of attacks – thus avoiding detection. The updated version of the code was much simpler, less stealthy, and attacked the centrifuge drive system that controls rotor speeds. In essence, this second wave of attacks – which used the updated code – caused the centrifuges to spin much faster than originally intended (from 63,000 rpm to 84,000 rpm) for approximately 15 minutes, then slowing them down to a virtual stop, then again getting the centrifuges to spin at higher than intended speeds. This continued for 50 minutes, which drastically increased the chances of rotor failure. By Langner's estimates, "Stuxnet

[28] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," The New York Times, June 1, 2012, sec. World / Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
[29] Ralph Langner, "Stuxnet's Secret Twin," Foreign Policy, November 19, 2013, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

set back the Iranian nuclear program by two years; a simultaneous catastrophic destruction of all operating centrifuges wouldn't have caused nearly as big a delay."[30] These recent events demonstrate how devastating cyber-attacks, like nuclear attacks, albeit in vastly different ways, can be.

Another similarity between cyber and nuclear weapons is the fact that they both share the principal of "dual-use technology." In the nuclear paradigm, the technology used to create the bomb is the same technology that is used for peaceful purposes (e.g. civilian energy). The difference between the uranium in the bomb and the uranium used to power cities is that the bomb requires more highly enriched uranium. This dual use nature of nuclear technology is the biggest hurdle for regulating nuclear energy so that rogue actors do not acquire nuclear weapons capabilities. In his book, *Interpreting the Nuclear Non-Proliferation Treaty*, Daniel Joyner stresses this point by stating that "[i]t cannot be over emphasized that the dual-use nature of materials and technologies associated with nuclear energy underlines all of the difficulties in regulating nuclear energy through international legal sources."[31]

It is through manipulation of this nature of nuclear technology that A. Q. Khan was able to build his underground proliferating empire. David Albright, the author of *Peddling Peril,* writes:

> "Abdul Qadeer Khan took advantage of this loophole on an unprecedented scale. A.Q. Kahn stole the secrets of how to construct European gas centrifuges which then allowed Pakistan to buy the individual pieces for a gas centrifuge plant in Europe, Japan, and the United States. With China providing nuclear weapon designs and its initial weapon-grade uranium, Pakistan succeeded in obtaining nuclear weapons by 1984. Khan would then go much further, selling secrets and nuclear weapons capabilities to Iran, Libya, and North Korea."[32]

[30] Ibid.
[31] Joyner, Interpreting the Nuclear Non-Proliferation Treaty, 2.
[32] David Albright, Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies, 1st ed. (Free Press, 2010), 9.

The dual use nature of equipment allowed Khan to approach companies, such as Fysisch Dynamisch Onderzoek-Technische Adviseurs (Physical Dynamic Research Laboratory or FDO) based in Amsterdam, to acquire less sensitive equipment. Albright writes that "[i]n September 1976, FDO's sales manager […] visited Pakistan to explore selling a range of dual-use equipment" even though the sales manager was aware that Khan could have been a spy, which did not deter him from pursuing business with Khan.[33] As Khan realized that he needed more than FDO had to offer, he started shopping around the world for necessary items.[34] He set up fake front companies that he used as buyers of the dual use materials. Companies that sold Khan the materials were completely complacent in doing business with Khan even though there was a wide range of warning signs that Khan was building a secret gas centrifuge plant.[35] Firms were eager to sell to Khan's front companies; as he recalls in his writings that "[f]irms and people chased us with figures and details of equipment […] they literally begged us to buy their equipment. It was a competition to woo us. They were willing to do anything for money, if the money was good."[36]

When it comes to cyber technology, as with nuclear technology, the dual nature of its use is obvious. This contributes to concerns about the spread and offensive use of cyber capabilities against a state through back channels and other security vulnerabilities. People have computers with Wi-Fi connectivity to a router; perhaps they check their e-mail, shop, watch movies, or talk to friends or relatives that live in another country. Indeed, the Internet, coupled with the right hardware and software, can be limitless. On the other hand, a person with the same equipment and a bit more knowhow can use this technology as a weapon. Not only can the technology be used for dual

[33] Ibid., 31–32.
[34] Ibid., 35.
[35] Ibid., 31.
[36] Ibid., 35.

purposes, but the attacks can be aimed at 'dual-use infrastructure' such as telecommunications, space-based sensors and relays, automated aids to financial and banking networks, power production and distribution, and media to shape public perceptions. Robert Miller and Daniel Kuehl, authors of *Cyberspace and the 'First Battle' in 21st – century war*, write that 'dual-use infrastructures' can be anything that is "owned and operated by the private sector that both society itself and military forces depend on for daily functioning of critical capabilities."[37] An army of cyber warriors can wreak havoc on a state's infrastructure. First, however, weaknesses must be found or created in the hardware and/or the software. Just like Khan manipulated the dual nature of nuclear technology, the same was done by the Chinese in the early 2000's with cyber technology. They did so by going after the United States computer industry's biggest players in networking technology, Microsoft and Cisco. Clarke and Knake write:

> "By threatening to ban Chinese government procurement from Microsoft, Beijing persuaded Bill Gates to provide China with a copy of its secret operating system code. Microsoft has refused to show that same code to its largest U.S. commercial customers. Then China copied the Cisco network router found on almost all U.S. networks and at most Internet service providers […] Chinese then sold counterfeit Cisco routers at cut-rate discounts around the world. The buyers allegedly include the Pentagon and other federal government entities […] customer list included the Marine Corps, the Air Force, and multiple defense contractors. A fifty-page report […] concluded that the routers could be used by foreign intelligence agencies to take down networks and 'weaken cryptographic systems.'"[38]

Clarke and Knake conclude that with such intimate knowledge of Microsoft and Cisco software and hardware, China's cyber army could shut down most networks. Today, the world is even more connected and global. Computers and routers, e-mail and webpage servers, and all other Internet-related technologies are made by a large number of companies. Any current Personal Computer (PC) on the market will have different parts made in multiple countries. The screens may come from

[37] Robert A. Miller and Daniel T. Kuehl, Cyberspace and the'First Battle'in 21st-Century War (Defense Horizons, Number 68, September 2009) (DTIC Document, 2009), 3, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA508696.
[38] Clarke and Knake, Cyber War: The Next Threat to National Security and What to Do About It, 55–56.

Japan, the memory from Germany, the hard drive from South Korea, and the motherboard from Taiwan; all are most likely assembled in Malaysia or China. This is important because just as software (e.g. Microsoft) can be manipulated and used as a weapon, so can the hardware (e.g. Cisco), the chips, and the circuits within it. This creates a substantial opportunity for the malicious use of cyber related technology because the only distinguishing feature of cyber offensive capabilities from those of peaceful use capabilities are 'intention' and 'organization' (e.g. state sponsorship/resources/cyber army) of the actor. This sentiment is echoed by Scott J. Shackelford, the author of *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. He writes that "aggressive acts in cyberspace are not [only] assessed by their consequences, but also by their intentions, such as inchoate crimes. The difficulty lies in proving those intentions."[39] In other words, the dual use nature of cyber technology resides in the difficulty of proving that a cyber activity was intended to directly cause physical destruction or injury.

There are also a large number of differences between nuclear and cyber conflicts, some more obvious than others and have been mentioned previously. Let's begin with the difficulty of defining the terms that are widely used: 'cyber-attack' and 'cyber war.' Unlike the nuclear paradigm, an attack in cyberspace is not a concrete event – there are different ways in which an attacker can proceed in cyber space. In the following list, Carr uses the word 'aggression' instead of 'attack' in order to illustrate the different forms of cyber-attacks:[40]

- Cyber aggression against government or critical civilian websites or networks without accompanying military force
- Cyber aggression against government or critical civilian websites or networks with accompanying military force
- Cyber aggression against internal political opponents

[39] Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkley Journal of Inetnational Law (BJIL) 25, no. 3 (April 28, 2009): 245, http://ssrn.com/abstract=1396375.
[40] Carr, Inside Cyber Warfare, 32.

- Cyber intrusions into critical infrastructure and networks
- Acts of cyber espionage

Perhaps clarification on defining cyber-attacks can be sought from the Tallinn Manual, which was commissioned by NATO and created by several dozen experts in an attempt to study how international law applies to the new cyber dimension by focusing on principles of *jus ad bellum*, that determines the use of force in international law, and *jus in bello*, that dictates conduct in armed conflict. Rule 30 (dealing with the definition of cyber-attack), Sections 2-3 of the Tallinn Manual state that

> "The notion of an 'attack' is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilian and civilian objects may not be 'attacked' (Rule 32). This rule sets forth a definition that draws on that found in Article 49(1) of Additional Protocol1: 'attack means acts of violence against the adversary, whether in [offense or defense]. By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military operations. Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks."[41]

The Tallinn Manual introduces the concept of 'violence' into the cyber-attack debate. However, it does not get into the specificities of what 'violence' really means. Does this violence have to be lethal? Does a bodily injury suffice for a cyber aggression to become a cyber-attack? Where does physiological violence fit in this debate? These small distinctions are important to defining cyber aggression, which will ultimately help identify the acts that will be covered under an international cyber treaty. For example, it is extremely unlikely that cyber espionage will be covered under such a treaty because it is missing the 'violence' component of the aggression.[42] To add to the existing complexity, even smaller distinctions must be sorted out in the cyber-attack debate in order for the subject to move forward. In fact, the distinctions in some cases are so small that verification of any

[41] Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (New York: Cambridge University Press, 2013), 106, http://issuu.com/nato_ccd_coe/docs/tallinnmanual/127?e=0.
[42] John Steinbruner, "Prospects for Global Restraints on Cyberattack," Arms Control Association 41 (December 2011), http://www.armscontrol.org/act/2011_12/Prospects_for_Global_Restraints_on_Cyberattack.

cyber treaty would prove to be extremely difficult, if not impossible. John Steinbruner, author of *Prospects for Global Restraints on Cyberattack*, points out – for example – that intrusion with the goal of exploitation and intrusion with the goal of destruction is "presumably unmanageable" and intrusive and robust regulations would be necessary for the cyber treaty to be successful.[43] I will address the issue of verifications in more detail further down.

In addition to determining what constitutes a cyber-attack, scholars are also confronted with the question of which attacks constitute an act of cyber war.[44] Thomas Rid, a professor in the Department of War Studies at King's College London, fellow at Johns Hopkins University's School for Advanced International Studies, and an author of *Cyber War Will Not Take Place*, argues that "all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage," and that any offensive act – including cyber-attacks – must meet "certain criteria in order to qualify as an act of war."[45] Other scholars have also provided their definitions of cyber war. *Cyberwar: A New 'Absolute Weapon'?* author, Adam Liff, defines cyber war in the following manner:

> "[cyber warfare is] a state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of [Computer Network Attacks] against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes."[46]

[43] Ibid.
[44] A related topic that I will not discuss here as it is outside of this paper but is worth mentioning is that there is considerable disagreement on whether cyber war has occurred or will occur in the future Suggested authors for further information on this topic: Thomas Rid, Adam Liff, Timothy Junio, and Volodymyr Lysenko.
[45] Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35, no. 1 (February 2012): 6, doi:10.1080/01402390.2011.608939.
[46] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Journal of Strategic Studies 35, no. 3 (June 2012): 408, doi:10.1080/01402390.2012.663252.

In response to both Rid and Liff, Timothy Junio, author of *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate*, writes that

> "Rid, Liff, and this author at least agree on the following: cyber war is a coercive act involving computer network attack. Network attack means information is disrupted, degraded, or destroyed. 'Coercive' means using force to change or preserve a political status quo. A point of contention is lethality, which Rid believes is necessary for cyber 'war'. This is an extreme and undesirable requirement, particularly because (as Rid himself points out) non-lethal cyber attacks may be more costly than conventional warfare."[47]

Then there are those who unify the ideas supported by Rid and Junio. Scott Beidleman, author of *Defining and Deterring Cyber War*, argues that the key to understanding cyber war is the concept of 'armed attack' as defined by United Nations General Assembly Resolution 3314. He writes that "… any cyber-attack that causes the same level of damage as a traditional armed or kinetic attack, either through the destruction of physical property or loss of life, would be considered an armed attack." In other words, "[w]hether a power plant is bombed by aircraft or its electrical grid destroyed by malicious code, a blackout is a blackout."[48] Shackelford similarly argues that because cyber-attacks are unique and different from classic kinetic attacks, they require the same effect level of the attack as traditional kinetic attacks in order to be classified as armed cyber-attack. This would justify retaliation in self-defense due to irrefutable proof of aggression within the acts.[49] It is, however, not clear how the international community will go about defining cyber-related attacks as armed attacks.

Another difference between the cyber and nuclear paradigms is the concept of deterrence. Deterrence does not apply to cyber conflict as it has for nuclear conflict. The concept of deterrence can be defined as the use of threat by one party to convince another party to refrain from initiating

---

[47] Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," Journal of Strategic Studies 36, no. 1 (February 2013): 126, doi:10.1080/01402390.2012.739561.
[48] Scott W. Beidleman, Defining and Deterring Cyber War (DTIC Document, 2009), 13, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA500795.
[49] Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 236.

some course of action. A threat serves as a deterrent to the extent that it convinces its target not to carry out the intended action because of the costs and losses that target would incur.[50] Deterrence was used during the Cold War with the threat of nuclear weapons, but, as Clarke and Knake observe, of all the nuclear-strategy concepts, […] deterrence theory is probably the least transferable to cyber war."[51] Nuclear deterrence is based on credible threats; nuclear power has been demonstrated through its use in Japan as well as through a multitude of tests that were conducted by nuclear states. This demonstrative nature of deterrence is not applicable to cyber conflict because no country can fully test and reveal its real cyber strength, as doing so would require an actual attack on a country, which may cause serious damage to said country and even achieve the required criteria, as described by Rid, in order to constitute an act of war. As observed by Steinbruner, "social disruption by cyberattack is massive, and the practice of the type of deterrence that is widely believed to have so far prevented the actual use of nuclear weapons is dramatically less reliable. Because the parties responsible for a cyberattack cannot always be reliably identified, the threat of retaliation is less credible and less effective."[52]

This brings us to the problem of attribution. It is much easier to identify the attacker in a nuclear conflict (assuming it is a state to state conflict) than, in a cyber-conflict where, it can be difficult to trace the roots of the attack. As Carr points out,

> "[a]lthough states can trace cyber attacks back to computer servers in another state, conclusively ascertaining the identity of the attacker requires intensive, time-consuming investigations with the assistance of the state of origin. Given the prohibition on responding with force until an attack has been attributed to a state or its agents, coupled with the fact that the vast majority of cyber attacks are conducted by nonstate actors, it should come as no surprise that states are reluctant to treat cyber attacks as acts of war and risk violating international law."[53]

[50] Huth P. K., Deterrence and International Conflict: Empirical Findings and Theoretical Debate, vol. 2, Annual Review of Political Science (Annual Review of Political Science, 1999), 25–48.
[51] Clarke and Knake, Cyber War: The Next Threat to National Security and What to Do About It, 189.
[52] Steinbruner, "Prospects for Global Restraints on Cyberattack."
[53] Carr, Inside Cyber Warfare, 47.

Whom does the state retaliate against if it cannot prove who attacked it? Indeed, a state may not retaliate against an attack if it does not know who attacked it.[54] Additionally, as highlighted by Carr, cyber-attacks are far more likely to be carried out by non-state actors – thus forcing states to think twice before classifying a cyber-attack as an act of cyber war. It is not that non-state actors necessarily prefer cyber weaponry – it is clear that a nuclear weapon is far more devastating; however, nuclear materials are much harder to access due to the cooperation of major nuclear states under the NPT and other international agreements and safeguard regimes. Two examples of the difficulty of attribution are useful for better understanding of this problem: 1) a spyware program named "GhostNet" was traced to China but the Information Warfare Monitor (IWM) could not determine whether it was controlled by the Chinese government or a private actor residing in China, and 2) the origins of a 2009 worm called "Cornflicker," which was used to attack the Republic of Korea and the United States, is still unknown.[55] As demonstrated in these examples of our recent past, attribution becomes far more difficult in cyber space due to the time-consuming investigations involved, an increased likelihood the attack was carried out by a non-state actor, and insufficient international cooperation in the cyber sphere.

Another major distinction from the nuclear paradigm is that it is much harder (if not impossible) to build abundant enough offensive power to deter the use of cyber weapons in retaliatory strikes.[56] Indeed, regardless of how effective Mutually Assured Destruction (MAD) has

[54] Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 237.
[55] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View," ed. Peter Berkowitz, Future Challenges in National Security and Law, February 2011, 10, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.
[56] Ross M. Rustici, "Cyberweapons: Leveling the International Playing Field," Parameters (Autumn 2011), 2011, 40.

worked in the past, the debate has shifted towards looking at whether a strong defense is more effective at deterring states from attacking than a robust counteroffensive. In an article in Foreign Policy entitled *Cult of the Cyber Offensive*, authors P.W. Singer and Allan Friedman write that "the most important lesson researchers have learned in traditional offense-defense balances – and now in cyber security – is that the best defense actually is a good defense. Regardless of which side has the advantage, any steps that raise the capabilities of the defense make life harder on the offense and limit the incentives for attacks in the first place.[57]

If we can learn anything from the lessons of nuclear threat management during the Cold War, it is that the deficiency of verifications in cyberspace may have a direct negative impact on the existence of arms control application for cyberspace. Verification was the biggest reason behind why nuclear arms controls, put in place by the United States and the Soviet Union during the Cold War, worked. In their book, *Spy Satellites*, Thomas Graham Jr. and Keith Hansen point out that "[v]erification, therefore, became the core issue of all strategic nuclear arms control agreements between the two countries. Without effective verification, the Cold War might not have ended as peacefully as it did, and U.S. and Russian nuclear arsenals, while still far too high, would not be anywhere near as low as they currently are."[58] Even if all other hurdles can be conquered, the issue of verifications can dissolve any security treaty.[59] This is why the claim by Clarke and Knake that verification of any cyber agreement seems to be an impossible task is so demoralizing.[60] Goldsmith explains that the issue of verification is directly connected to the issue of attribution – when it is hard

[57] P. W. Singer and Allan Friedman, "Cult of the Cyber Offensive," Foreign Policy, January 15, 2014, http://www.foreignpolicy.com/articles/2014/01/15/cult_of_the_cyber_offensive_first_strike_advantage.
[58] Thomas Graham and Keith Hansen, Spy Satellites: And Other Intelligence Technologies That Changed History (University of Washington Press, 2007), 13.
[59] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 10.
[60] Clarke, Cyber War, 220.

to figure out who is behind an attack, it is hard to come up with verifications to stop cyber-attacks. Thus, in order to overcome the issue of verifications, the international community has to figure out a way to identify these attacks and whom they belong to. This fact exists in complete contrast with the nuclear realm, as intent to weaponize nuclear technology is foreseeable and confirmable (sometimes even preventable) due to the nonproliferation regime that deems verification as a high priority task – a role which is filled by the IAEA. Additionally, the international community has been strengthening the inspection capabilities of the IAEA with the IAEA Information Circulars (INFCIRCS) 153 (Comprehensive Safeguard Agreement) and 540 (the Additional Protocol). These INFCIRCS focused on facilities, materials, or both, with tangible verification techniques that just do not exist in the cyber paradigm.

Now that we looked at the differences between the two paradigms and the debates surrounding the 21st century battlefield, I will attempt to address the original question of what is preventing the international community from adopting an NPT type treaty to reduce the threat of cyber war. As highlighted above, it appears that managing the nuclear threat is quite different from what managing the cyber threat will be. It is my hypothesis that the biggest hurdle to an NPT type cyber treaty is the different types of threats each paradigm presents. Accordingly, the purpose of this paper is to address the question of how states balance *internal* and *external* threats, and how that differs by regime type. My hypothesis is outlined in the preceding chapter, yet not much research has been done on the subject in order to support or disprove my hypothesis. I will study the question by looking at the language of major cyber security treaty proposals from the United States, the European Union, the Russian Federation, the People's Republic of China, and their allies in order to ascertain the intent of these proposals. I will also use the analysis of the language from the NPT as the

'control' group in order to demonstrate the intent of treaties where a common external threat to the major players in the international arena exists. I will utilize democracy rating resources (e.g. democracyranking.org and economist intelligence unit) in order to demonstrate how the threat perception is different depending on the regime type.

Part III: The Enemy

Using ideas originally outlined by Kenneth Waltz and Hans Morgenthau, Steven David explains the realist arguments as they pertain to the international arena in his work entitled *Explaining Third World Alignment*. He writes that "international politics," just like human nature, "focuses on power, interests, and rationality."[61] David continues by writing that realists see "clear hierarchies of issues, with survival being the most important."[62] Survival is seen as the most important of the hierarchies as the international arena is "anarchical" or a "self-help" system.[63]

In order to understand the dangers that the cyber paradigm presents to different regimes, we must first understand their political structure. In their book *The Dictator's Handbook* by Bruce Bueno de Mesquita and Alastair Smith, the authors identify three groups of people within the political landscape (and even structures of publicly traded corporations), which they call the three political dimensions: the nominal selectorate, the real selectorate, and the winning coalition. Bueno de Mesquita and Smith define the nominal selectorate as people with at least some legal right to choose their leader. In the U.S., for example, this would include all adults ages eighteen and over. The real selectorate is a group which consists of people who actually choose their leader. A good example of this group would be the senior members of the royal Saudi family. Lastly, the winning coalition is the most important of these groups. These are the people who actually keep the leadership in power and their support is vital to the survival of the regime. The winning coalition within the United States is vastly larger than that of, for example, Cuba. Fundamentally, the nominal selectorate is the pool of potential support for the leader; the

[61] Steven R. David, "Explaining Third World Alignment," World Politics 43, no. 02 (January 1991): 236, doi:10.2307/2010472.
[62] David, "Explaining Third World Alignment," 237.
[63] Robert O. Keohane, ed., Neorealism and Its Critics, The Political Economy of International Change (New York: Columbia University Press, 1986), 98–101.

real selectorate includes those whose support is truly influential; and the winning coalition extends only to those essential supporters without whom the leader would be finished. A simple way to think of these groups is: interchangeables, influential, and essentials."[64] It is important to note that Bueno de Mesquita and Smith apply their assessment to both democratic and authoritarian regimes. This is important because we must understand why authoritarian regimes are prone to perceive the need of the state as secondary to their own maintenance of power.

The leaders of authoritarian regimes are more likely to choose regime survival over what is best for the state in the event of an impending dual threat from the cyber paradigm. This probability is based on the fact that the winning coalition within the authoritarian regimes is vastly smaller than that within the democratic regimes, creating a disproportionately smaller percentage of the general population to whom the leader must cater to in order to remain in power. Bueno de Mesquita and Smith underscore this point by writing that the "[d]ifferences in the size of these groups across states, businesses, and any other organization […] decide almost everything that happens in politics – what leaders can do, what they can and can't get away with, to whom they answer, and the relative qualities of life that everyone under them enjoys (or too often doesn't enjoy)."[65] The authors add that "the best way to stay in power is to keep the coalition small and, crucially, to make sure that everyone in it knows that there are plenty of replacements for them."[66] The merits themselves will not keep the leader in power for long. It may, however, it is not the most determining factor. The more important factor is loyalty from the coalition that is keeping the ruler in power. Consequently, the paradoxical problem resides in

[64] Bruce Bueno de Mesquita and Alastair Smith, The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics (New York: PublicAffairs, 2011), 4–5.
[65] Ibid., 7.
[66] Ibid., 61.

the fact that the smaller the coalition of the ruler, the bigger the opposition movement against him can potentially be. This creates a larger portion of the population that is *willing* to fight the leadership once the movement against the regime gains momentum and attempts to reach a critical mass. This is due to the fact that a successful leader puts his essential supporters before the needs of the people. Bueno de Mesquita and Smith write that "[m]ore often than not, the coalition's members get paid at the cost of the rest of society […] Eventually things get bad enough that some of the people tire of their burden. They too can threaten the survival of their leader. […] Although not as omnipresent as the threat posed by the risk of coalition defection, if the people take to the streets en masse then they may succeed in overwhelming the power of the state."[67] All that is needed for the feelings of neglect, anger, and general disillusionment towards the regime to become a movement is "a tipping point, at which life in the future under the existing government is expected to be sufficiently bad that it is worth their while to risk the undoubted costs of rebellion."[68]

However, this opposition movement against authoritarian leaders is often fractured and weak. Natasha Ezrow and Erica Frantz, authors of *Dictators and Dictatorships* write that "[i]n all dictatorships, there exist individuals who do not support the regime. Key to the regime's survival is, ensuring that these individuals do not unify, and become so organizationally robust, that they threaten the regime's hold on power."[69] This is where it helps to have a catalyst like cyber technology in order to unite and organize the fractured opposition groups behind an issue or multiple issues.

---

[67] Ibid., 195.
[68] Ibid., 196.
[69] Natasha M. Ezrow, Dictators and Dictatorships: Understanding Authoritarian Regimes and Their Leaders (New York: Continuum, 2011), 56.

Through the Internet and social media (Facebook, Twitter, Youtube, etc.), the cyber paradigm becomes the essential threat to authoritarian regimes by providing the tools for easier mobilization by the public. According to Bueno de Mesquita and Smith,

> "[t]o come to power a challenger need only do three things. First, he must remove the incumbent. Second, he needs to seize the apparatus of government. Third, he needs to form a coalition of supporters sufficient to sustain him as the new incumbent. Each of these actions involves its own unique challenges. *The relative ease with which they can be accomplished differs between democracies and autocracies*."[70]

I will concentrate on the first requirement as it pertains to the internal threat that emerges from the cyber paradigm. There are multiple fronts of opposition, including civilian and student, which are often fragmented in their numbers and their goals. These fragmented coalitions may at first demand individual policy changes, but those can morph into demands of regime change as the fragmented coalitions unite.[71] With the advent of social media, it has become substantially more efficient to organize these coalitions. The tools allow for quick organization of students, the general populous, etc. and are hard to suppress without eliciting additional anger – may it be an organic mobilizations of the tools or a state sponsored event. The recipe for revolution involves a coalition that represents a small fraction of the populous, a 'tipping point,' and a 'catalyst.' This concept is best illustrated by looking at the empirical examples of this mechanism at work around the world.

If you know the name Mohamed Bouazizi, then you know he was the tipping point that sparked the movement across the Middle East known as the Arab Spring. As the breadwinner for

[70] Bueno de Mesquita and Smith, The Dictator's Handbook, 23.
[71] R. H. Dix, "The Breakdown of Authoritarian Regimes," Political Research Quarterly 35, no. 4 (December 1, 1982): 566, doi:10.1177/106591298203500407.

his family, Bouazizi, a college educated unemployed street vendor, supported his mother and six siblings by selling fruits and vegetables on the market in a town called Sidi Bouzid, Tunisia. In December 2010, Bouazizi was confronted by the police for not having a license to sell his goods on the market. The police asked Bouazizi to hand over his merchant cart, and when he refused, the policewoman slapped him.[72] Publicly humiliated and angered, Bouazizi walked to the government building and set himself on fire. By doing so, Bouazizi unknowingly ignited the already heated passion and anger shared by his townspeople against the government over corruption, inequality, censorship, and joblessness. Despite Tunisia's strict web censorship laws, the protests in Sidi Bouzid, which erupted that same day, were captured by cell phones and shared online. Fanned by online Internet tools, the protests spread throughout the country calling for the resignation of their President, Zine El Abidine Ben Ali. About a month after the incident, when the armed forces refused to crack down on the protests, Ben Ali was forced to flee to Saudi Arabia in exile after 23 years in power.

Meanwhile, protests spread across multiple borders to Egypt, Libya, Yemen, Syria, Bahrain, Saudi Arabia, Morocco, Algeria, Jordan, Oman, and Kuwait. In Egypt, the mass mobilization of protesters continued for eighteen days before President Hosni Mubarak was forced to resign after 29 years in power. In Libya, the protests turned violent after security forces opened fire on protesters in Benghazi. This event turned simple anti-government protests into a deadly civil war with anti-Gaddafi armed forces receiving support from NATO forces. The civil war and NATO intervention ended with the capture and execution of Muammar Gaddafi. The National Transitional Council, which led the revolt, promised to rebuild Libya as a pluralist and

[72] N. P. R. Staff, "The Arab Spring: A Year Of Revolution," NPR.org, accessed April 9, 2014, http://www.npr.org/2011/12/17/143897126/the-arab-spring-a-year-of-revolution.

democratic state after being under a 42 year authoritarian rule.[73] In Yemen, President Ali Abdullah Saleh promised not to seek reelection after demonstrations erupted calling for his resignation. However, his promise did not appease protesters as their numbers swelled and protests multiplied. President Saleh's security forces cracked down on the protesters leaving hundreds, if not thousands, dead. After being gravely injured in a bombing, and upon returning from abroad after receiving treatments for his serious injuries, President Saleh ultimately signed a deal in November 2011 to hand over his presidency to his deputy. Mr. Saleh's attempt to resist pressure is commendable but is not as impressive as Bashar al-Assad's fight for survival at the throne. Assad's response to the protests in Syria was predictable: a violent security force crack down upon protesters. After security forces opened fire on demonstrators demanding Assad's resignation, the protestors increased in numbers and locations. Assad's government branded the protesters as "terrorists" and "armed criminal gangs"[74] and unleashed a ruthless effort to squash the movement, to no avail. Opposition supporters took up arms and fought back, facilitating the transition of the conflict into a sectarian civil war. The tide of war swung back and forth between the Assad administration and the opposition forces. The West's hesitation to supply heavy arms to the opposition with links to al-Qaeda, coupled with Russian support for Assad, helped keep Assad in power. Pressure on Assad grew dramatically, however, after a chemical weapons attack near Damascus left hundreds of Syrians dead, forcing Syria to destroy its chemical weapons stockpiles after an international outcry.[75] The conflict is currently at a stalemate with President Assad refusing to relinquish his power while more than 146,000 Syrian's paid with their lives.[76]

---

[73] "Arab Uprising: Country by Country," BBC News, accessed April 10, 2014, http://www.bbc.com/news/world-12482311.
[74] Ibid.
[75] Ibid.
[76] Noah Rayman, "Report: More Than 146,000 People Killed in Syrian Civil War | TIME," TIME.com, accessed April 10, 2014, http://time.com/24077/syria-death-toll/.

It is clear that in all the countries involved in the Arab Spring, a tipping point existed in one form or another (e.g. unemployment, inequality, repression, etc.). This is what caused the initial spark, but the catalyst that fanned the flames was the various forms of social media. Recent research conducted by Philip Howard, an associate professor in communication at the University of Washington, suggests that "social media played a central role in shaping political debates in the Arab Spring," and that "social media has carried inspiring stories of protests across international borders."[77] According to Howard, "social media carried a cascade of messages about freedom and democracy across North Africa and the Middle East, and helped raise expectations for the success of political uprising […] [p]eople who shared interest in democracy built extensive social networks and organized political action. Social media became a critical part of the toolkit for greater freedom."[78] Howard's research indicates that a week prior to Mubarak's resignation, for example, the rate of tweets grew 9,900%, from 2,300 a day to 230,000 a day – imagine the mobilization potential for a movement. What makes this equation even more complex for the autocrats is the fact that the efforts to shut down the Internet during the height of the protests in Egypt backfired as people who could no longer follow the events through social media took to the streets, creating further momentum against the regime. Howard concludes that "people throughout the region were drawn into an extended conversation about social uprising. The success of demands for political change in Egypt and Tunisia led individuals in other countries to pick up the conversation. It helped create discussion across the region."[79] The ability to organize and share information increased citizens' ability to affect domestic politics in highly

[77] "New Study Quantifies Use of Social Media in Arab Spring | UW Today," accessed April 10, 2014, http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/.
[78] Ibid.
[79] Ibid.

censored environments. The reach and ease with which information can be shared on the Internet is the real power (and threat) of the cyber paradigm to the internal stability of authoritarian regimes via mobilization against the regime, delegitimization of the regime, and cross border exposure of the regimes' (often atrocious) actions.

The Protests are not limited to the Middle East and North Africa however. Another example that demonstrates the potential internal threats posed by the cyber paradigm through social media are the recent revelations by the Associated Press that the US Agency for International Development (USAid) engineered a program similar to Twitter. ZunZuneo, named after a slang name for a Cuban hummingbird's tweet, was "intended to encourage 'flash mobs' in Cuba, emulating social media-based protests that had been occurring organically in countries such as Iran, the Philippines and Moldova."[80] To circumvent Cuba's strict control of the Internet and information, the 'Cuban Twitter' would use cellphone text messaging in order to "renegotiate the balance of power between the state and society."[81] At its peak, the program's 40,000 subscribers were never aware that ZunZuneo was created by the US government. In fact, "in order to conceal the true nature of the social-media network," Paul Lewis and Dan Roberts of The Guardian reported, "[e]xtensive efforts were undertaken." These efforts include the use of offshore bank accounts, front companies, overseas servers, and "[m]ock ad banners [which would] give it the appearance of a commercial enterprise."[82] The hazard that this program poses to authoritarian regimes is clearly summarized in The Guardian publication:

---

[80] Paul Lewis and Dan Roberts, "White House Denies 'Cuban Twitter' ZunZuneo Programme Was Covert," The Guardian, April 3, 2014, sec. World news, http://www.theguardian.com/world/2014/apr/03/white-house-cuban-twitter-zunzuneo-covert.
[81] Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government," The Guardian, April 3, 2014, sec. World news, http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.
[82] Lewis and Roberts, "White House Denies 'Cuban Twitter' ZunZuneo Programme Was Covert."

> "Documents show the US government planned to build a subscriber base through 'non-controversial content': news messages on soccer, music, and hurricane updates. Later when the network reached a critical mass of subscribers, perhaps hundreds of thousands, operators would introduce political content aimed at inspiring Cubans to organize 'smart mobs' – mass gatherings called at a moment's notice that might trigger a Cuban spring […]."[83]

An additional example of the threats that social media poses to non-democratic regimes comes from Turkey where the government recently blocked access to both Twitter and YouTube after a recording was circulated on both social media sites in which Turkish top officials "were heard discussing a plot to establish a justification for military strikes in Syria."[84] The Turkish government cited national security concerns when bans occurred, and the 'crackdown' didn't stop there as officials further suggested that "a broader crackdown on the Internet may be coming."[85] Prime Minister Tayyip Erdogan's efforts to suppress the information from slipping out was too late and therefore futile due to the very nature of online content and the fact that Twitter and YouTube do not comprise the entire Internet.

There are also examples of preemptive subversion of cyber technology by autocratic regimes. The most recent example of cyber technology subversion used in a conflict occurred just months ago during the Russian invasion of Ukraine's territory of Crimea. The conflict arose when on November 21, 2013; Ukrainian President Viktor Yanukovych's government announced the decision to seek closer cooperation with Moscow by abandoning planned economic cooperation with the European Union. Protests erupted promptly and within a week attracted 300,000 protesters. The parliament imposed harsh anti-protest laws, which attracted more protesters to the streets. Predictably, street clashes and casualties soon followed. On February 22, Yanukovych was forced to

[83] Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government."
[84] Tim Arango, "Recordings, Posted Online, Rattle Officials in Turkey," The New York Times, March 27, 2014, http://www.nytimes.com/2014/03/28/world/europe/high-level-leaks-rattle-turkey-officials.html.
[85] Ibid.

flee out of the country after a political coup. According to USA Today, on February 28 "[a]rmed men in Russian military uniforms [took] control of key airports in Crimea. Russian marines [surrounded] a Ukraine coast guard base in Sevastopol."[86] What followed was a complete takeover of the Crimean peninsula by Russian forces. Crimean local parliament voted to join Russia on March 6, and scheduled a referendum – which was overwhelmingly passed on March 16. The conclusion to this story is not yet clear. What is clear, however, is that the Russian Federation was concerned about the 'wrong' information regarding its annexation of Crimea spilling out of the area. On February 28, right as armed men in Russian military uniforms were taking over strategically important airports in Crimea, the largest telecom provider in Ukraine called 'Ukrtelcom' said that "unidentified people seized telecommunications nodes and destroyed cables, effectively severing data and voice connectivity between Crime and the rest of Ukraine."[87] This effectively brought down most phone lines and Internet services in Crimea. At the same time, Russia ramped up the propaganda machine within the peninsula.

What we have learned from previous pages is that the internal threat cyber technology poses to authoritarian regimes is real and immediate. If we view the world through a realist's lens and assume that a non-democratic state's or an authoritarian state leader's primary concern is to survive, we can safely conclude that threat(s) to the state or the regime will be resisted. However, if multiple threats arise (both internal and external), a choice must be made. It is far more likely for an authoritarian leader to act in *his* own interest of staying in power in contrast to a democratic state which is more likely to act in state's best interest. This sentiment is echoed by

[86] "Timeline: Key Events in Ukraine," accessed April 14, 2014, http://www.usatoday.com/story/news/nation-now/2014/03/06/ukraine-russia-timeline-obama/6127545/.
[87] "Saboteurs Bring down Phone and Internet Services in Crimea," UPI, accessed April 14, 2014, http://www.upi.com/Top_News/World-News/2014/02/28/Telecom-services-sabotaged-in-Ukraines-Crimea-region/7611393621345/.

David when he writes that "since the dominant goal of Third World leaders is to stay in power, they will sometimes protect themselves at the expense of the interest of the state.[88] Thus, the cyber-dual-threat nature poses a dilemma for the authoritarian regimes around the world. One can make a case that a low-level, political cyber war is already taking place. Attacks on the political pillars of authoritarian regimes has, is, and will continue to occur leaving authoritarian regimes helpless to respond in kind with effective political attacks on democratic systems. The only recourse left for authoritarian regimes is that of cyber attacks against apolitical hard targets as described by Clarke and Knake. The question then becomes whether or not the authoritarian regimes' inherent bias towards preventing internal threats precludes the creation of a meaningful international treaty for the cyberspace.

[88] David, "Explaining Third World Alignment," 236.

Part IV: The Data

In this section, I will examine the weight of internal and external threat perception and its impact on the development of an international cyber treaty by analyzing the support of or opposition to existing cyber treaty proposals and their language by regime type. First, it is important to highlight the language of a successful treaty, the NPT, as it pertains to the nuclear paradigm, a clear external threat as noted in the introduction of this paper. The NPT is considered to be the most successful arms control treaty in history, boasting 189 signatories. As mentioned previously, the NPT is a grand bargain between the nuclear states and the non-nuclear states. The non-nuclear states agreed to give up their ambitions of acquiring nuclear weapons, while the nuclear states agreed to complete disarmament of existing nuclear arms. All treaty members maintained the "inalienable right" to seek nuclear material for peaceful purposes. The following is the breakdown of the articles and their intent via the treaty language. Articles I, II, and III address the 'non-proliferation' pillar of the treaty through the following language:

> "Each nuclear-weapon State Party to the Treaty undertakes not to transfer to any recipient whatsoever nuclear weapons […] or control over such weapons or explosive devices, or indirectly; and not in any way to assist, encourage, or induce any non-nuclear-weapon State to manufacture or otherwise acquire nuclear weapons. […] Each non-nuclear-weapons State Party to the Treaty undertakes no to receive the transfer from any transferor whatsoever of nuclear weapons[;] […] not to manufacture or otherwise acquire nuclear weapons[;] […] and not to seek or receive any assistance in the manufacture of nuclear weapons or other nuclear explosive devices. […] Each Non-nuclear-weapon State Party to the Treaty undertakes to accept safeguards, as set forth in an agreement to be negotiated and concluded with the International Atomic Energy Agency […] for the exclusive purpose of verification of the fulfilment of its obligations assumed under this Treaty with a view to preventing diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices."[89]

Articles IV and V address the 'peaceful use of nuclear energy' pillar of the treaty through the following language:

> "Nothing in this Treaty shall be interpreted as affecting the inalienable right of all the Parties of the Treaty to develop research, production and use of nuclear energy for peaceful purposes without discrimination and in conformity with Articles I and II of this Treaty. All the Parties of the Treaty undertake to facilitate, and

[89] Available: http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf, accessed April 24, 2014

> have the right to participate in the fullest possible exchange of equipment, materials and scientific and technological information for the peaceful uses of nuclear energy."[90]

Article VI addresses the 'disarmament' pillar of the treaty through the following language:

> "Each of the Parties to the Treaty undertakes *to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament*, and on a treaty on general and complete disarmament under strict and effective international control" (emphasis added).[91]

Notice that the language is straight forward and uncompromising until reaching Article VI where the language becomes considerably more ambiguous. Considering that this document was drafted during the height of the Cold War, the language is clearly intended to minimize or eliminate any external threat emanating from the nuclear paradigm while allowing for the nuclear states the room to eliminate their arsenal in a balanced way.

In *Interpreting the Nuclear Non-Proliferation Treaty, Daniel Joyner* addresses the issue of disarmament by the nuclear-weapon states. The treaty does not enforce the disarmament pillar nor does it provide a timeline for the disarmament process. To demonstrate the manipulation of this loophole, Joyner points out that "evidence of *arms control* efforts is often tendered by nuclear weapon states, and in particular the United States, in order to attempt to show compliance with the *disarmament* requirements of Article VI."[92] He further elaborates by drawing a clear distinction between 'arms control' and 'disarmament' by explaining that arms control efforts seek to effect a limitation or reduction in weapon technologies, while the object of disarmament is the complete elimination of weapons from national arsenals.[93] The grand bargain between the nuclear states and the non-nuclear states will not come to fruition so long as external

[90] Ibid
[91] Ibid
[92] Joyner, Interpreting the Nuclear Non-Proliferation Treaty, 37.
[93] Ibid., 36.

threats persist or are perceived by the nuclear superpowers against one another. Despite this, the NPT provides the network necessary to strengthen international security and protect states from the external threat of nuclear weapons confrontation.

There are many success stories of the NPT in recent history. According to the United Nations Office for Disarmament Affairs, Argentina, Brazil, and South Africa gave up their nuclear weapons programs and joined the NPT in 1995, 1998, and 1991, respectively. This is significant as each additional country joining the nuclear club increases the likelihood of a nuclear confrontation (or a terrorist group getting its hands on poorly secured nuclear material). On the same token, in his book *Disarmament Sketches*, Ambassador Thomas Graham Jr. paints a grim alternative present without the NPT:

> "A result of the spread of nuclear weapons from one nation to five between 1945 and 1964, and the increasing accessibility of the technology, there were predictions in the Kennedy administration that by the end of the 1970s there would be 25-30 avowed nuclear weapon states … such a development could likely have led to 50-60 nuclear weapon states today, creating an intolerable *national and international situation*. The IAEA estimates that the present time some 70 nations have the capability to build nuclear weapons. *If such proliferation had occurred, every confrontation, no matter how small, would raise the specter of nuclear war.* And it would be impossible to keep these weapons out of the hands of terrorists, religious cults, and criminal organizations" (emphasis added).[94]

Furthermore, countries suspected of pursuing a nuclear weapons program while being members of the NPT, or that leave the NPT to pursue nuclear weapons, are exposed to the possibility of severe sanctions imposed by the collective international community. North Korea and Iran, for instance, are both currently experiencing crippling international sanctions that are wreaking havoc on both economies. The threat of a united international community, coupled with the power of sanctions, serves as a deterrent for states from contemplating withdrawal from the treaty. Given the clear focus of the treaty language, the NPT is clearly intended for the

[94] Graham, Disarmament Sketches: Three Decades of Arms Control and International Law, 326.

purpose of minimizing the external nuclear threat within international community. I will now look at the cyber paradigm.

It is no secret that information or data pertaining to the cyber paradigm is closely guarded by states and, therefore, is not easily accessible. This reality limits the scholarly research potential in the field. However, certain documents exist that provide a foundation for analyzing intent through treaty language.

First, I analyzed a product of the World Conference on International Telecommunications (WCIT), which took place in Dubai, UAE in 2012. The WCIT was assembled by the International Telecommunication Union (ITU), a specialized United Nations agency for information and communication technologies (ICTs). The ITU has 193 member states, and its membership includes ICT regulators, leading academic institutions, and approximately 700 private companies. The WCIT is described on the ITU website as a "landmark conference [that] reviewed the International Telecommunications Regulations (ITRs), which serve as the *binding global treaty* designed to facilitate international interconnection and interoperability of information and communication services, as well as ensuring their efficiency and widespread public usefulness and availability" (emphasis added).[95]

Second, I evaluated the 2011 proposal submitted by China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations General Assembly (UNGA). Submitted during

[95] "World Conference on International Telecommunications (WCIT-12)," ITU, accessed April 21, 2014, http://www.itu.int/en/wcit-12/Pages/default.aspx.

the 66th session of the UNGA, the proposal outlined the *International Code of Conduct for Information Security*.

The third document I examined was the Russian-drafted *Yekaterinburg Declaration* approved by the Shanghai Cooperation Organization (SCO). The SCO is comprised of the following member states: China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. Additionally, Afghanistan, India, Iran, Mongolia, and Pakistan have the observer status within the SCO (this, however, means that those states cannot vote nor submit proposals).

The United States provided the fourth document for examination. The document entitled *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* was released by the Obama administration in May 2011 and it offers a vision for Internet cooperation from the United States' perspective. President Barack Obama introduces the document by writing that "[t]his is not the first time my Administration has addressed the policy challenges surrounding these technologies, but it is the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues. And so this strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and abroad to *understand our priorities*, and how we can come together to preserve the character of cyberspace and reduce the threats we face" (emphasis added).[96]

[96] United States, "International Strategy for Cyberspace," May 2011, 3, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Lastly, I studied the European Commission's Joint Communication entitled *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace*. The European Commission has a substantial role within the European Union (EU) and is able to propose new legislation to the European Parliament and to the Council of the European Union. According to its website, the Commission "has the right of initiative to propose laws for adoption […] [and] [o]nce EU legislation has been adopted, the Commission ensures that it is correctly applied by the EU member countries." Thus, this Joint Communication will be viewed as the official representation of the European Union's priorities.

The *Final Acts of the World Conference on International Telecommunications* was published in 2012 and consists of fourteen articles. The purpose and scope of the regulations are defined in Article I:

> "[t]here Regulations establish general principles which relate to the provision and operation of international telecommunication services offered to the public[,] […] contain provisions applicable to those operating agencies, authorized or recognized by a Member State, to establish, operate and engage in international telecommunications services to the public, […] [t]hese Regulations are established with a view to facilitating global interconnection and interoperability of telecommunication facilities and to promoting the harmonious development and efficient operation of technical facilities, as well as the efficiency, usefulness and availability to the public of international telecommunication services […]" and that "[t]he Member States, where appropriate, shall cooperate in implementing these Regulations."[97]

The document even goes as far as mentioning the states' firm commitment to implement the regulations addressed within in a way which will not conflict with their "human rights obligations."[98] However, the language that follows is slippery and contains loopholes which can be exploited by states in order to actually infringe on the human rights of the citizenry if such an opportunity were to arise.

[97] "World Conference on International Telecommunications (WCIT-12)," 2–3.
[98] Ibid., 3.

Articles VI and VII are of most concern. Article VI deals with the security and robustness of networks:

> "Member States shall individually and collectively endeavor to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public."[99]

Two phrases are problematic in Article VI: 1) 'collectively endeavor,' and 2) 'to ensure the security.' Working backwards through the sentence containing these phrases, one realizes that human rights violations, or at least violations of democratic values, are permitted to occur in the name of 'security.' Depending on what is considered a 'national security concern,' the state may use the term to justify Internet censorship or suppression. In fact, 'national security' is exactly what Turkey's government cited when it decided to ban YouTube after audio files detailing the false flag operation discussed by the senior Turkish government, military, and intelligence officials were leaked, as noted in Part III of this paper. The Guardian article reported that "[a] source at the prime minister's office told Reuters that the government had taken action against YouTube after the leak of the voice recordings created a 'national security issue.' The source noted that Turkey was in talks with the video-sharing platform and may lift the ban if YouTube agreed to remove the content."[100] An even bigger problem lies in the words 'collective endeavor.' If all signatory parties to the treaty are the 'collective,' this means that the states which hold democratic values in high regard within the 'collective' must compromise their

[99] Ibid., 10.
[100] Constanze Letsch, "Turkey Blocks YouTube amid 'National Security' Concerns," The Guardian, March 28, 2014, sec. World news, http://www.theguardian.com/world/2014/mar/27/google-youtube-ban-turkey-erdogan.

values by potentially cooperating with less democratic states in order to satisfy the terms of this treaty *even though* the states may use the pretext of 'security' to censor the Internet.

Article VII deals with unsolicited bulk electronic communications:

> "Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services […] [and] Member States are encouraged to cooperate in that sense."[101]

Here, the problematic language lies in the phrases 'necessary measures,' 'unsolicited bulk electronic communications,' and 'cooperate.' 'Unsolicited bulk electronic communications' generally refers to spam, however, the danger is that in order to control the content, states can label any electronic communication as spam, thus applying 'necessary measures' when convenient. Since 'necessary measures' is a vague term, this could mean blocking content. Even worse, the signatories would have to cooperate with each other in this process, which poses the same issue as outlined in Article VI in reference to 'collective action.'

The European Commission issued a press release following the vote on the treaty which stated that "[i]n the opinion of EU participants, the final text risked threatening the future of the open internet and internet freedoms, as well as having the potential to undermine future economic growth. The EU was concerned about this possible harm not only within the EU, but globally, including in developing countries."[102] The United States similarly expressed its concerns. United States Ambassador Terry Kramer, Head of Delegation to the WCIT,

[101] "World Conference on International Telecommunications (WCIT-12)," 10.
[102] "No Change to Telecoms and Internet Governance - EU Member States amongst Dozens Not Signing Proposed New International Telecommunications Regulations (ITR) Treaty, Remain 100% Committed to Open Internet" (European Commission, 22 2012), http://europa.eu/rapid/press-release_MEMO-12-991_en.htm.

specifically spoke about the U.S. concerns about spam, among other things, stating that "spam is a form of content and that regulating it inevitably opens the door to regulation of other forms of content, including political and cultural speech"[103] However, the Russian Federation's perspective on this issue was outlined a year prior to the WCIT by then Russian Prime Minister Vladimir Putin who met with the head of the ITU and was quoted as saying that it is important to establish "international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union."[104]

Realizing the language concerns hidden within the potentially problematic WCIT treaty, I next examined whether or not such concerns were driven by the voting regimes. To do so, it is helpful to break down the votes for and against the treaty while adding the democracy rating variable for each voting country. The complete dataset of the votes submitted by Members States of the ITU was forwarded to Mike Masnick, editor of the Techdirt.com, by a reporter named Dave Brustein. The data for democracy ratings for the year 2013 is courtesy of Globaldemocracyranking.org, which utilized raw data from the Freedomhouse.org, World Economic Forum, and Transparency International, and assessed the following variables (weighted) in order to come up with their democracy rankings: Political rights – 25%, civil liberties – 25%, global gender gap report – 25%, press freedom – 10%, corruption perceptions index – 10%, change of the head of government in the last 13 years (peaceful) – 2.5%, political party change in the head of government in the last 13 years (peaceful) – 2.5%. Available in Appendix 1 is a table that utilizes both data sets and organizes the signatory and non-signatory

[103] Bureau of Public Affairs Department Of State. The Office of Website Management, "World Conference on International Telecommunications," Remarks|Remarks, U.S. Department of State, (December 13, 2012), http://www.state.gov/e/eb/rls/rm/2012/202040.htm.
[104] Jerry Brito, "The Case Against Letting the U.N. Govern the Internet," Time, accessed May 20, 2014, http://techland.time.com/2012/02/13/the-case-against-letting-the-united-nations-govern-the-internet/.

states in different columns, accompanied by their democracy rating scores[105] (when available, otherwise left blank). At the end of the table, I provide the average democracy rating (ADR) for the signatory and the non-signatory states.

Appendix 1 illustrates a correlation between the democracy rating of a state and vote for or against the WCIT treaty. In particular, the ADR of the signatory nations is 50.57, while the ADR of the non-signatory nations is 71.02. In order to further substantiate these findings, I used another democracy rating report in conjunction with the data provided by Dave Brustein (Appendix 2). *The Economist Intelligence Unit's Index of Democracy 2012: Democracy at a Standstill*

> "is based on the ratings for 60 indicators grouped in five categories: electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture. Each category has a rating on a 0 to 10 scale, and the overall index of democracy is the simple average of the five category indexes. […] The index values are used to place countries within one of four types of regimes: 1) Full democracies – scores of 8-10; 2) Flawed democracies – score of 6 to 7.9; 3) Hybrid regimes – score of 4 to 5.9; 4) Authoritarian regimes – scores below 4."[106]

The ADR of the signatory nations as shown in Appendix 2 is 4.81, while the ADR of the non-signatory nations is 7.43. Appendix 1 data demonstrates a slightly smaller divide in the ADR between signatories and non-signatories of the treaty as compared to Appendix 2 (Appendix1 = 33.64% , Appendix 2 = 42.81% difference). However, the differences are meaningful in both ADR calculations. The data from both Appendices is plotted in Figures 1, 2, 3, and 4.

[105] "Global Democracy Ranking – Democracy Ranking 2013."
[106] Economist Intelligence Unit, The Economist Intelligence Unit's Index of Democracy 2012: Democracy at a Standstill (The Economist), 26–27, accessed April 23, 2014, https://portoncv.gov.cv/dhub/porton.por_global.open_file?p_doc_id=1034.

Both figures contain outliers within the data (e.g., any data point that is more than two standard deviations from the mean). In Figures 1 and 2, for example, the Republic of Korea, Uruguay, Yemen, Armenia, Kenya, and Malawi are all considered outliers. In Figure 3, Armenia, Belarus, and Gambia are all considered outliers. When the averages are adjusted for removing the outliers, there is little difference: the ADR for signatories' in Appendix 1 falls to 50.17 while the ADR of non-signatories rise to 72.72. In Appendix 2, the ADR for signatories' stays the same while the non-signatories see an increase to 7.67. After adjusting for the outliers, the data from Appendix 2 shows that three 'full democracies,' as defined by The Economist Intelligence Unit's Index of Democracy, signed the treaty while none of the authoritarian regimes within the given data refused to sign the treaty. Additionally, all nations with the democracy rating below 4.71 (Kenya) signed the treaty and all nations with the democracy rating above 8.17 (Mauritius & Uruguay) refused to sign the treaty. In Appendix 1, countries with democracy ratings below 54.1 (India) signed the treaty while countries with democracy ratings above 70.2 (Argentina) refused to sign the treaty. It is also important to add that the United States and Europe specifically cited the "significant threat to the 'open Internet'" as a point of concern within the proposed language and the reason for not supporting the WCIT treaty.[107] Below are scatterplots of the data in Figures 1, 2, 3, and 4; the data points that include the names and ratings of the countries are outliers.

[107] Eric Pfanner, "Citing Internet Standoff, U.S. Rejects International Telecommunications Treaty," The New York Times, December 13, 2012, sec. Technology, http://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html.

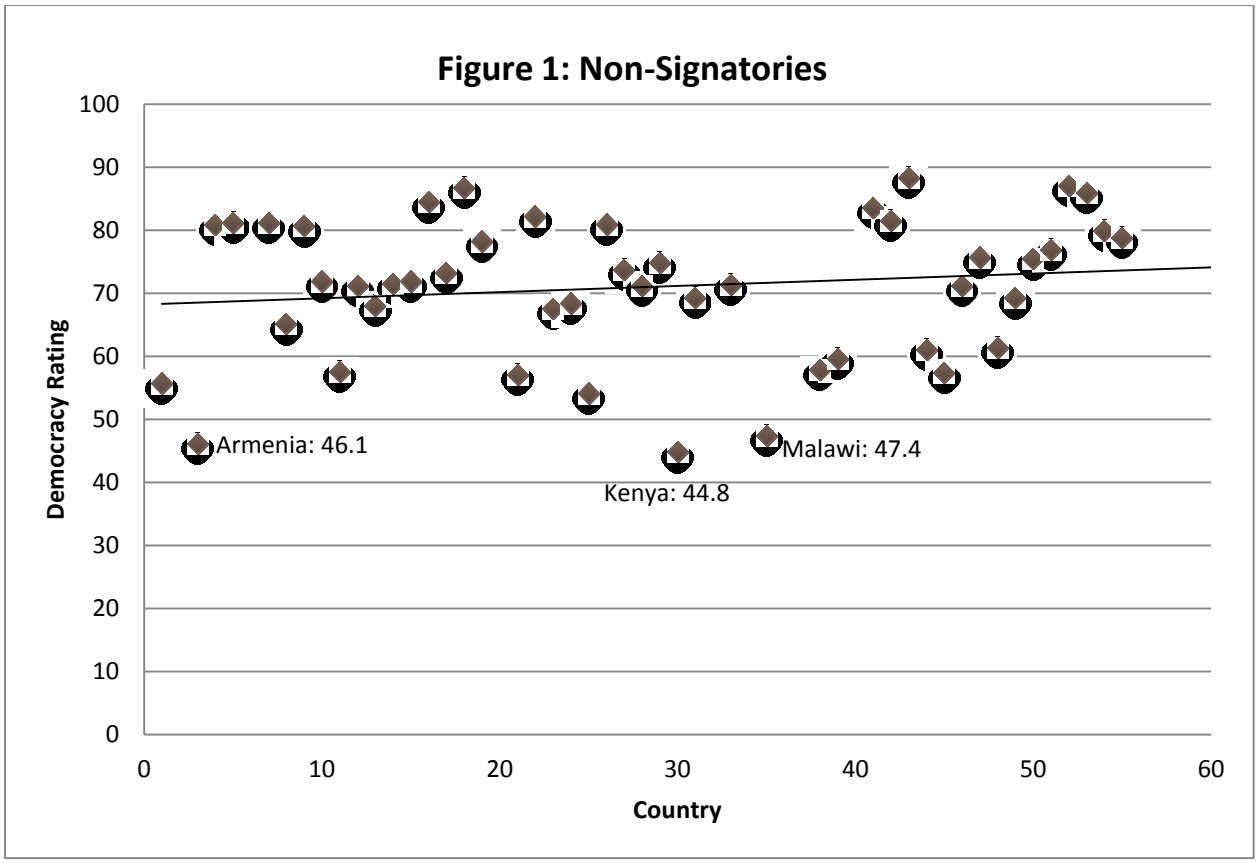


Figure 1: Non-Signatories
Democracy Rating
Country
Armenia: 46.1
Kenya: 44.8
Malawi: 47.4

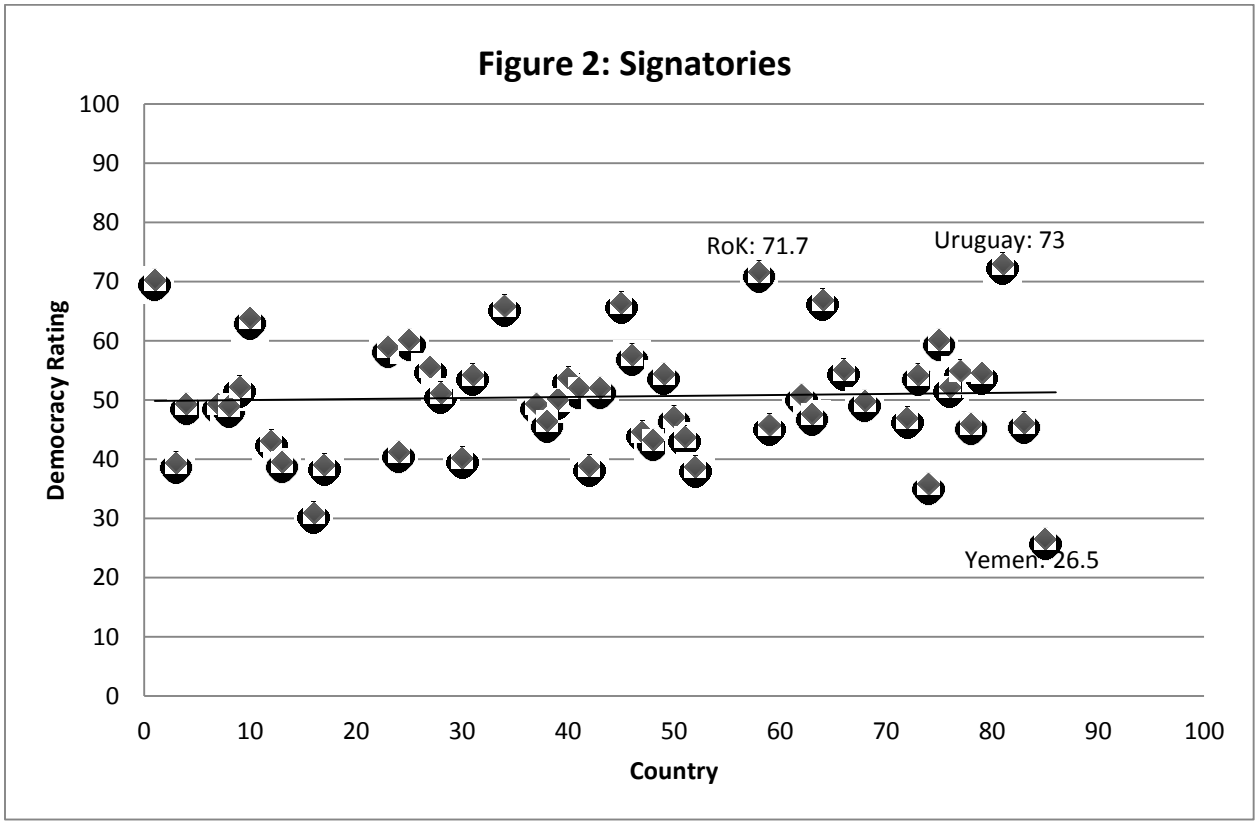


Figure 2: Signatories
Democracy Rating
Country
RoK: 71.7
Uruguay: 73
Yemen: 26.5

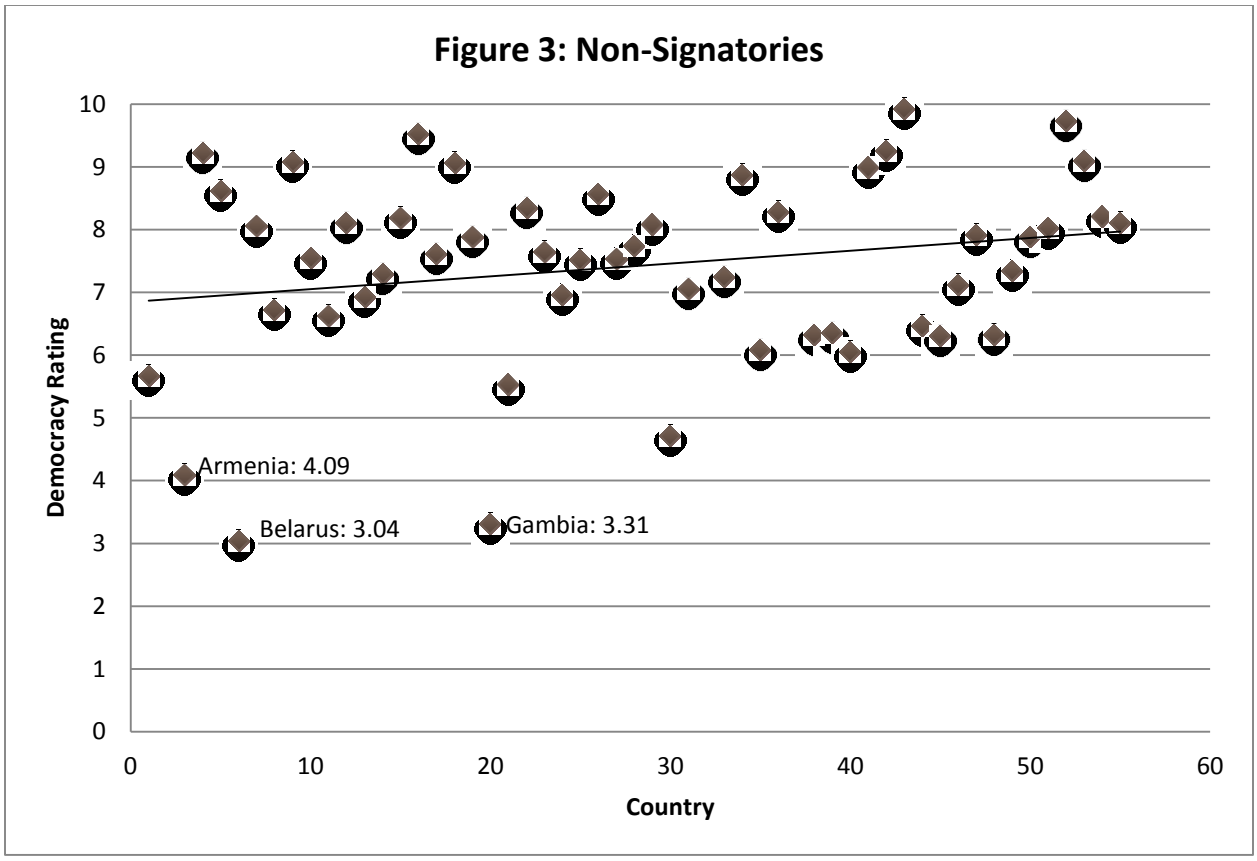


Figure 3: Non-Signatories
Democracy Rating
Country
Armenia: 4.09
Belarus: 3.04
Gambia: 3.31
0
1
2
3
4
5
6
7
8
9
10
0
10
20
30
40
50
60

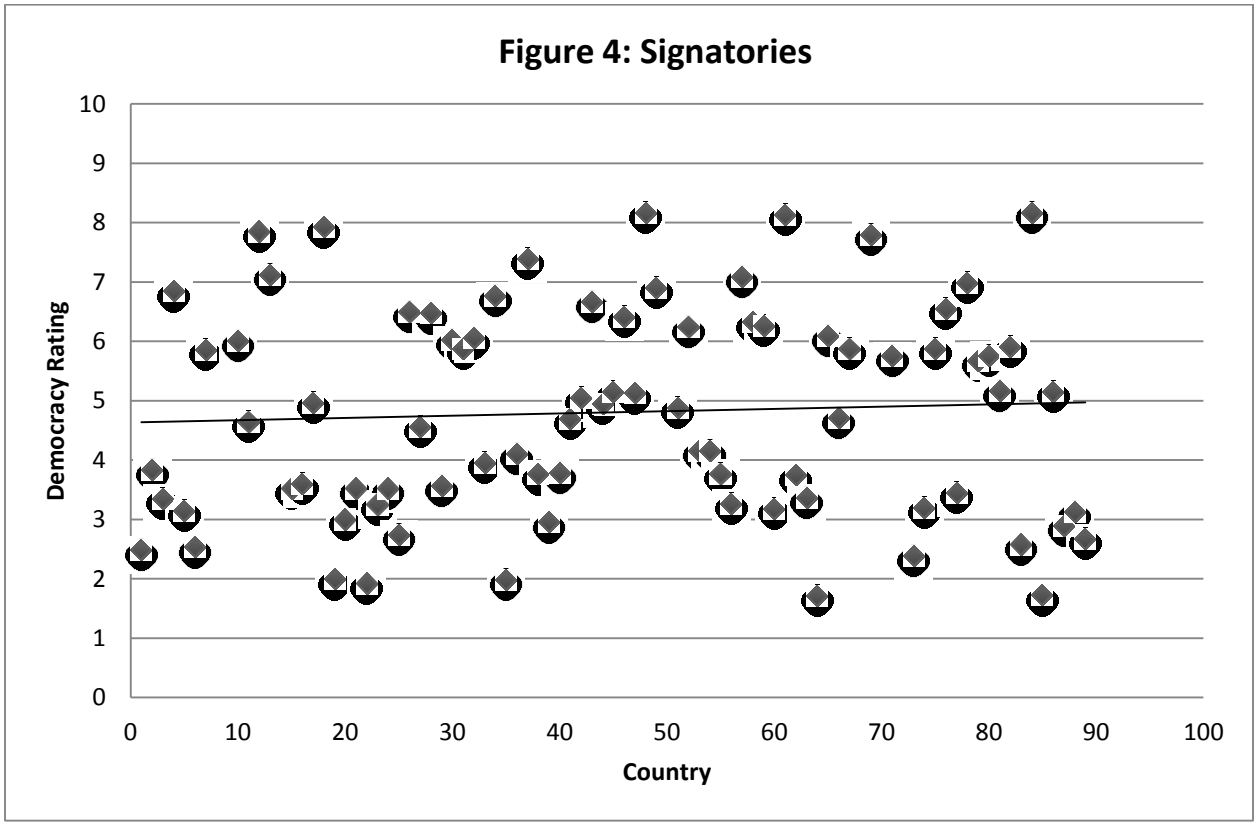
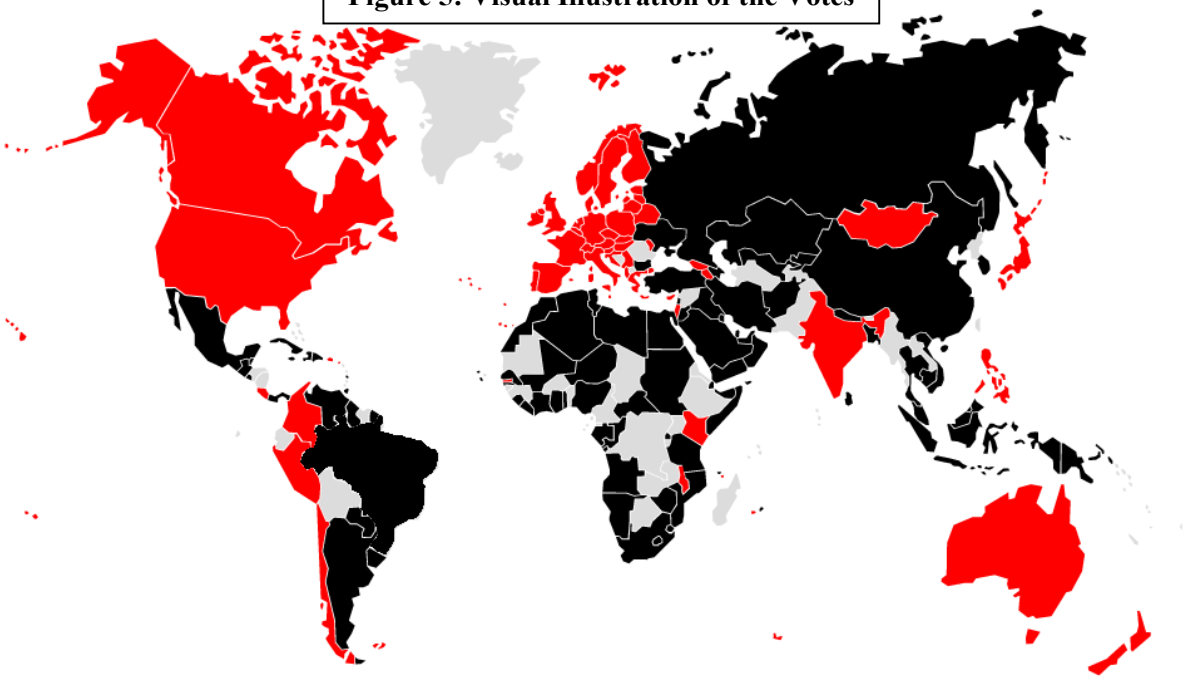


Figure 4: Signatories
Democracy Rating
Country
0
1
2
3
4
5
6
7
8
9
10
0
10
20
30
40
50
60
70
80
90
100

Figure 5[108] is a useful visual representation of the vote breakdown, which illustrates a clear divide between the East and the West, democracies and non-democracies.

Figure 5: Visual Illustration of the Votes



*Map courtesy of Techdirt.com – Slightly edited to include Brazil's vote (Red=Against, Black= For, Gray=No Vote)

Perhaps in anticipation of resistance from the West, the East has been working on regional agreements in order to advance its interests pertaining to the subject of the Internet. When looking at the 2011 proposal submitted by China, the Russian Federation, Tajikistan, and Uzbekistan entitled *International Code of Conduct for Information Security*, it is important to establish the respective countries democracy rankings. In assessing this document, I will use The Economist Index of Democracy report as it includes the most extensive rating for the applicable countries. The ratings are as flows:

1) Russia = 3.74
2) China = 3
3) Tajikistan = 2.51
4) Uzbekistan = 1.72

[108] "Who Signed The ITU WCIT Treaty... And Who Didn't | Techdirt," Techdirt., accessed April 23, 2014, https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml.

Notice that according to The Economist definition noted above (e.g., authoritarian regimes score 4 or below), all four nations are considered authoritarian regimes by the data. The *International Code of Conduct for Information Security* proposal states that

> "The purpose of the present code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviors and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being, with the objective of maintaining international stability and security. Adherence to the code is voluntary and open to all States."[109]

The code is broken down into eleven sections, four of which raise enormous red flags. Section (a) asks states to be mindful of "human rights and fundamental freedoms" and asks states to "respect […] the diversity of history, culture and social systems of all countries[.]"[110] This could be understood to say that countries which are by nature not democratic due to a variety of reasons should not be held to the same standard of expectations in regards to, for example, Internet freedoms and, thus, can conduct censorship mechanisms freely. Perhaps an argument can be made for such a claim, though it is harder to justify when in section (j) of the code states pledge "[t]o bolster bilateral, regional and international cooperation, promote the important role of the United Nations in formulating international norms, peaceful settlements of international disputes and *improvements in international cooperation in the field of information security*, and enhance coordination among relevant international organizations" (emphasis added).[111] The language here suggests that states that perceive democratic values inherently different would pledge to cooperate in the field of information security, which can perhaps mean censorship of the Internet. The language in sections (b) and (c) is vague enough to support this concern.

[109] China et al., "International Code of Conduct for Information Security" (United Nations, General Assembly, September 14, 2011), 4, undocs.org/A/66/359.
[110] Ibid.
[111] Ibid., 5.

Section (b) states that nations pledge "[n]ot to use information and communications technologies […] to [...] proliferate *information weapons* or related technologies" (emphasis added). This section can directly challenge the free flow of information within the cyber sphere. Along the same lines, section (c) targets "criminal and terrorist activities that use information and communication technologies" as well as aims to curb "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment[.]"[112] Again, 'terrorist activities,' 'extremism,' and the word 'undermines' can be stretched to mean anything – including, as demonstrated by the Turkish government, any information that challenges or damages the legitimacy of the ruling party within an authoritarian state. The Chinese Ambassador for Disarmament Affairs Wang Qun explained the reasons for submitting the code as an attempt to launch "an open and transparent process for developing, within the framework of the UN, international norms and rules for information and cyberspace security, which, [China hopes] will prompt countries to act responsibly and constructively in information and cyberspace and address concerns of all parties in a balanced way."[113] Based on the language, however, it is hard to believe that the *International Code of Conduct for Information Security* is anything other than an attempt by authoritarian regimes to shield themselves from the internal threat that the cyber sphere inherently poses.

Examining the third document, the Russian-drafted *Yekaterinburg Declaration* approved by the SCO, a recognizable pattern emerges. First, all the members of the SCO score below 4 in The Economist Index of Democracy report, except for Kyrgyzstan which scored 4.69. This

[112] Ibid., 4.
[113] Timothy Fransworth, "China and Russia Submit Cyber Proposal," Arms Control Association, November 2011, http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

means that five out of six regimes within the SCO are authoritarian and one is considered a hybrid regime:

1) Kyrgyzstan = 4.69
2) Russia = 3.74
3) China = 3
4) Kazakhstan = 2.95
5) Tajikistan = 2.51
6) Uzbekistan = 1.72

Second, under the *Yekaterinsburg Declaration* section VII "[t]he SCO member states stress the significance of the issue of ensuring international information security as one of the key elements of the common system of international security."[114] The SCO includes 'information terrorism' in the list of 'major international information security threats'[115] as specified in the *Yekaterinsburg Declaration*. The definition of 'information terrorism' clearly broadens the definition of general cyber security as it identifies threats emanating from

> "terrorist organizations and individuals involved in terrorist activities acting unlawfully through information resources […] [and is] characterized by the use of information networks by terrorist organizations to carry out terrorist activities and recruit new supporters; destructive impact on information resources leading to disruption of public order; control or blocking of mass media channels; use of the internet or other information networks for terrorist propaganda, creating an atmosphere of fear and panic in the society, as well as other negative impacts on the information resources."[116]

Again, international information security takes on a broader definition with words like 'information terrorism,' which can be stretched to include any person or organization which challenges the state's power through the cyber paradigm. In contrast, the United States provides a definition for 'information security' that is very different from that of the SCO and is specific to protect information within government agencies without the potential for overreach. The

[114] "Саммит ШОС '13 » Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization," accessed April 24, 2014, http://www.scosummit2013.org/en/documents/ekaterinburgskaya-deklaratsiya-glav-gosudarstv-chlenov-shanhayskoy-organizatsii-sotrudnichestva/.
[115] Shanghai Cooperation Organization website, "Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security," 2 Dec 2008, http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, accessed 05 Apr 2014.
[116] Ibid.

Federal Information Security Management Act (FISMA) was enacted in 2002 as Title III of the E-Government Act of 2002 and defines the term 'information security' as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction[.]"[117] The contrasting differences do not stop with FISMA.

The Obama administration's document entitled *International Strategy for Cyberspace* provides a glimpse at the United States' vision for international cooperation in cyberspace. In it, the United States outlines a goal to "work internationally to promote an open, interoperable, secure, and reliable information and communication infrastructure that supports international trade and commerce, strengthen international security, and *foster free expression* and innovation" (emphasis added).[118] Additionally, the document outlines cyberspace norms that includes 'upholding fundamental freedoms' – of expression and association – and 'valuing privacy' – the protection from arbitrary or unlawful state interference with individual's privacy when they use the Internet. The document expands on the concept of 'prioritizing openness and innovation of the Internet' through the following language:

> "The ability to distribute information efficiently on the Internet is at the very core of modern consumer, business, political, scientific, and educational activity. Governments around the globe recognize the value of the Internet; however, many of them place arbitrary restrictions on the free flow of information or use it to suppress dissent or opposition activities. The method and enforcement of these restrictions vary widely across countries, as do their justification, but we should not allow the Internet's governance or technical architecture to be reengineered to accommodate decisions that violate fundamental freedoms or unnecessarily stifle innovation. Effective, inclusive Internet governance can help ensure acts grossly outside international norms of acceptable network management are not compounded by a technical or governance structure that would enable them. *Preserving, enhancing, and increasing access to an open, global Internet is a clear policy priority*. The United States will continue to advance these goals […]" (emphasis added).[119]

[117] U.S. House. 107th Congress, 1st Session. H.R. 2458, Washington, Government Printing Office, 2002, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, accessed 24 Apr 2014.
[118] United States, "International Strategy for Cyberspace," 8.
[119] Ibid., 21.

Obviously, the language in the *International Strategy for Cyberspace* is vague and light on details, but it is not the same vagueness that plagued any previous document pertaining to cyberspace examined in this paper. The language in this document clearly demonstrates that the United States does not perceive an internal threat residing within the cyber paradigm while at the same time making it clear that it does not know how to minimizing the external threat. It is also important to note that the United States is rated as a full democracy according to The Economist Index of Democracy with a rating of 8.11.

Lastly, the European Commission's Joint Communication entitled *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace* is the final document examined in this paper and has striking similarities to the document provided by the Obama Administration. The 28 nation union receives an ADR of 7.94, giving it a classification of a flawed democracy (but is extremely close to a full democracy). The *Cybersecurity Strategy of the European Union* states that

> "[a]n open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies – most strikingly during the Arab Spring. For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace."[120]

The European Union's values, norms, and laws are emphasized as transferable to cyberspace. The protection of fundamental rights, freedoms of expression, and privacy is part of those values. The Joint Communication states that "[c]ybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of

[120] "Global Democracy Ranking – Democracy Ranking 2013.", accessed April 15, 2014

the European Union and EU core values." Very similar to The United States' *International Strategy for Cyberspace*, the *Cybersecurity Strategy of the European Union* emphasizes open and free Internet, thereby demonstrating that the internal threat to the member states' regime is external and not internal in nature. The external threat concerns are evident in both the *International Strategy for Cyberspace* and the *Cybersecurity Strategy of the European Union* precise and pointed language.

Part V: Conclusion

The purpose of this paper was to address the question of why an NPT type cyber treaty has not materialized by looking at how states balance *internal* and *external* threats, and how that differs by regime type. This is an important question to confront as determining what stands in the way of progress towards a goal that will strengthen peace between nations will allow us to work towards finding solutions to ameliorate said obstacles and pave the way for a safer international climate. In evaluating the language, data, and empirical evidence outlined in this paper, I constructed a relationship between the prioritization of threats and state regime types. My research illustrates that there is a clear correlation between the threat perception and regime types. Correlation, however, does not equal causation. Accordingly, one cannot conclude with certainty that a nation balances perceived threats in a certain order or that it would sign a treaty with imperfect language *because* of its regime type. There are far too many other variables that may explain this correlation besides the one highlighted in this paper. As further agreements and proposals are introduced by the international community, we will have a clearer picture of the intentions of states, which will either support or refute my conclusions. Further scholarly research is required for this purpose in this ever evolving subject that is currently in its infancy.

What can be concluded from this paper, however, is that even though substantial time has not been dedicated by international actors to confront the issue of cyber warfare, time is not the foremost obstacle to crafting the treaty for cyberspace. In fact, I would argue that leaving the differences in threat perceptions based on regime types unchallenged or unresolved would delay any cyber treaty indefinitely. The empirical evidence supports the fact that non-democratic states have reasons to fear, and indeed do fear, the very nature of cyberspace and the internal threat it poses. The language within the *Final Acts of the World Conference on International*

Telecommunications, the *International Code of Conduct for Information Security*, the *Yekaterinburg Declaration*, the *International Strategy for Cyberspace*, and the *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace* demonstrates that non-democratic regimes indeed do strive for greater control over the medium in order to protect themselves from threats that emanate from internal forces. It is also clear that there have been great attempts to redefine cyber warfare by less democratic regimes. As Tom Gjelten, author of *Internet Peace vs. Internet Freedom*, writes "[w]hile peace accords and disarmament agreements are attractive, democracies have reason to proceed cautiously in this area, precisely because of differences in the way cyber attacks are being defined in international forums."[121] If states balance internal and external threats differently and thus prevent an agreement on who the real enemy is, then the international community will have a very hard time agreeing on the language within any future cyber treaty.

Further research should focus on other variables that fit into this equation. For example, we should understand why three full democracies (the Republic of Korea, Mauritius, and Uruguay) signed the WCIT treaty. Perhaps by uncovering the variables involved in states' decision making, we can uncover other factors that can be used in assessment of this topic. Additionally, the reasons behind why states considered 'outliers' in this study voted uncharacteristically, or not as predicted, should be further examined and explained. Furthermore, as other proposals and agreements are introduced, scholars should attempt to assess the language of these documents and their sources of support and opposition in order to confirm or disprove the findings in this paper.

[121] Tom Gjelten, "Internet Peace vs. Internet Freedom," ARMY Magazine, March 2011, 30–31.

Even though causation is not directly proven in this paper, taken together with the empirical evidence which supports the quantitative data, a case can be made for the fact that non-democracies are more likely to seek greater control over the cyber paradigm through international institutions and agreements in order to minimize the internal threat the medium poses. This strategy is counter, and sometimes even hostile, to that of democratic states. How, then, can an international cyber treaty come into existence without the inclusion of internal political security for authoritarian regimes? The struggle and debate between authoritarian and democratic regimes over this dilemma will continue. The difference in cultures and regime structures of democracies and non-democracies should not prevent international cooperation on the subject of cyber security. States have to figure out a way to work together for a safer future that includes the cyber paradigm.

Appendix I

Signatories	Democracy Rating (2013)	Non-Signatories	Democracy Rating (2013)	Non-Participants
Afghanistan		Albania	55.7	Antigua & Barbuda
Algeria		Andorra		Bahamas
Angola		Armenia	46.1	Bolivia
Argentina	70.2	Australia	80.8	Bosnia and Herzegovina
Azerbaijan		Austria	81.2	Cameroon
Bahrain	39.4	Belarus		Chad
Bangladesh	49.3	Belgium	81.1	Congo (D.R.)
Barbados		Bulgaria	65.1	Dominica
Belize		Canada	80.6	DPRK
Benin	49.3	Chile	71.9	Ecuador
Bhutan	48.9	Colombia	57.5	Equatorial Guinea
Botswana	52.3	Costa Rica	71.1	Eritrea
Brazil	63.8	Croatia	68	Ethiopia
Brunei Darussalam		Cyprus	71.5	Fiji
Burkina Faso	43.1	Czech Republic	71.9	Grenada
Burundi	39.5	Denmark	84.4	Guinea
Cambodia		Estonia	73.2	Guinea-Bissau
Cape Verde		Finland	86.7	Honduras
Central African	31	France	78.2	Hong Kong, China
China	39.1	Gambia		Iceland
Comoros		Georgia	57.1	Kiribati
Congo		Germany	82.2	Laos
Cote d'Ivoire		Greece	67.5	Macao, China
Cuba		Hungary	68.4	Macedonia
Djibouti		India	54.1	Madagascar
Dominican Republic	58.9	Ireland	80.9	Maldives
Egypt	41.2	Israel	73.7	Mauritania
El Salvador	60.1	Italy	71.2	Micronesia
Gabon		Japan	74.8	Monaco
Ghana	55.5	Kenya	44.8	Myanmar
Guatemala	51.2	Latvia	69.3	Nauru
Guyana		Liechtenstein		Nicaragua
Haiti	40.2	Lithuania	71.3	Pakistan
Indonesia	54.2	Luxembourg		Romania
Iran		Malawi	47.4	Samoa
Iraq		Malta		San Marino
Jamaica	65.9	Marshall Islands		São Tomé and Príncipe
Jordan		Moldova	57.8	Seychelles
Kazakhstan		Mongolia	59.6	Solomon Islands
Kuwait	49.3	Montenegro		St. Kitts and Nevis
Kyrgyzstan	46.4	Netherlands	83.5	St. Vincent and the Grenadines
Lebanon	50.2	New Zealand	81.5	Suriname
Lesotho	53.8	Norway	88.3	Syria
Liberia	52	Peru	61	Tajikistan
Libya	38.9	Philippines	57.3	Timor-Leste
Malaysia	52	Poland	71.1	Tonga
Mali		Portugal	75.7	Turkmenistan
Mauritius	66.4	Serbia	61.4	Tuvalu
Mexico	57.7	Slovak Republic	69.2	Vanuatu
Morocco	44.6	Slovenia	75.4	Vatican
Mozambique	43.2	Spain	76.9	Zambia
Namibia	54.4	Sweden	87	
Nepal	47.2	Switzerland	85.9	

Signatories	Democracy Rating (2013)	Non-Signatories	Democracy Rating (2013)	Non-Participants
Niger	43.8	United Kingdom	79.9	
Nigeria	38.7	United States	78.8	
Oman				
Panama				
Papua New Guinea				
Paraguay				
Qatar				
Republic of Korea	71.7			
Russia	45.8			
Rwanda				
Saudi Arabia				
Senegal	50.8			
Sierra Leone	47.6			
Singapore	66.9			
Somalia				
South Africa	55.1			
South Sudan				
Sri Lanka	49.8			
St. Lucia				
Sudan				
Swaziland				
Tanzania	47			
Thailand	54.2			
Togo	35.8			
Trinidad & Tobago	60.1			
Tunisia	52.3			
Turkey	54.9			
Uganda	45.9			
Ukraine	54.5			
United Arab Emirates				
Uruguay	73			
Uzbekistan				
Venezuela	46.1			
Vietnam				
Yemen	26.5			
Zimbabwe				
ADR	**50.57**		**71.02**	

*Data courtesy of Globaldemocracyranking.org & Dave Brustein via Techdirt.com

Appendix II

Signatories	Democracy Rating (2012)	Non-Signatories	Democracy Rating (2012)	Non-Participants
Afghanistan	2.48	Albania	5.67	Antigua & Barbuda
Algeria	3.83	Andorra		Bahamas
Angola	3.35	Armenia	4.09	Bolivia
Argentina	6.84	Australia	9.22	Bosnia and Herzegovina
Azerbaijan	3.15	Austria	8.62	Cameroon
Bahrain	2.53	Belarus	3.04	Chad
Bangladesh	5.86	Belgium	8.05	Congo (D.R.)
Barbados		Bulgaria	6.72	Dominica
Belize		Canada	9.08	DPRK
Benin	6	Chile	7.54	Ecuador
Bhutan	4.65	Colombia	6.63	Equatorial Guinea
Botswana	7.85	Costa Rica	8.1	Eritrea
Brazil	7.12	Croatia	6.93	Ethiopia
Brunei Darussalam		Cyprus	7.29	Fiji
Burkina Faso	3.52	Czech Republic	8.19	Grenada
Burundi	3.6	Denmark	9.52	Guinea
Cambodia	4.96	Estonia	7.61	Guinea-Bissau
Cape Verde	7.92	Finland	9.06	Honduras
Central African Republic	1.99	France	7.88	Hong Kong, China
China	3	Gambia	3.31	Iceland
Comoros	3.52	Georgia	5.53	Kiribati
Congo	1.92	Germany	8.34	Laos
Cote d'Ivoire	3.25	Greece	7.65	Macao, China
Cuba	3.52	Hungary	6.96	Macedonia
Djibouti	2.74	India	7.52	Madagascar
Dominican Republic	6.49	Ireland	8.56	Maldives
Egypt	4.56	Israel	7.53	Mauritania
El Salvador	6.47	Italy	7.74	Micronesia
Gabon	3.56	Japan	8.08	Monaco
Ghana	6.02	Kenya	4.71	Myanmar
Guatemala	5.88	Latvia	7.05	Nauru
Guyana	6.05	Liechtenstein		Nicaragua
Haiti	3.96	Lithuania	7.24	Pakistan
Indonesia	6.76	Luxembourg	8.88	Romania
Iran	1.98	Malawi	6.08	Samoa
Iraq	4.1	Malta	8.28	San Marino
Jamaica	7.39	Marshall Islands		São Tomé and Príncipe
Jordan	3.76	Moldova	6.32	Seychelles
Kazakhstan	2.95	Mongolia	6.35	Solomon Islands
Kuwait	3.78	Montenegro	6.05	St. Kitts and Nevis
Kyrgyzstan	4.69	Netherlands	8.99	St. Vincent and the Grenadines
Lebanon	5.05	New Zealand	9.26	Suriname
Lesotho	6.66	Norway	9.93	Syria
Liberia	4.95	Peru	6.47	Tajikistan
Libya	5.15	Philippines	6.3	Timor-Leste
Malaysia	6.41	Poland	7.12	Tonga
Mali	5.12	Portugal	7.92	Turkmenistan
Mauritius	8.17	Serbia	6.33	Tuvalu
Mexico	6.9	Slovak Republic	7.35	Vanuatu
Morocco		Slovenia	7.88	Vatican

Signatories	Democracy Rating (2012)	Non-Signatories	Democracy Rating (2012)	Non-Participants
Mozambique	4.88	Spain	8.02	Zambia
Namibia	6.24	Sweden	9.73	
Nepal	4.16	Switzerland	9.09	
Niger	4.16	United Kingdom	8.21	
Nigeria	3.77	United States	8.11	
Oman	3.26			
Panama	7.08			
Papua New Guinea	6.32			
Paraguay	6.26			
Qatar	3.18			
Republic of Korea	8.13			
Russia	3.74			
Rwanda	3.36			
Saudi Arabia	1.71			
Senegal	6.09			
Sierra Leone	4.71			
Singapore	5.88			
Somalia				
South Africa	7.79			
South Sudan				
Sri Lanka	5.75			
St. Lucia				
Sudan	2.38			
Swaziland	3.2			
Tanzania	5.88			
Thailand	6.55			
Togo	3.45			
Trinidad & Tobago	6.99			
Tunisia	5.67			
Turkey	5.76			
Uganda	5.16			
Ukraine	5.91			
United Arab Emirates	2.58			
Uruguay	8.17			
Uzbekistan	1.72			
Venezuela	5.15			
Vietnam	2.89			
Yemen	3.12			
Zimbabwe	2.67			
ADR	**4.81**		**7.43**	

*Data courtesy of The Economist Intelligence Unit's Index of Democracy 2012: Democracy at a Standstill & Dave Brustein via Techdirt.com