Spring 4-27-2018

An Analysis Of International Agreements Over Cybersecurity

Lucas Ashbaugh
University of Maine, lucasashbaugh@gmail.com

AN ANALYSIS OF INTERNATIONAL AGREEMENTS OVER CYBERSECURITY

By

Lucas Ashbaugh

B.S. University of Maine, 2016

A THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Arts

(in Global Policy)

The Graduate School

The University of Maine

May 2018

Advisory Committee

Seth Singleton, Adjunct Professor of International Relations, Advisor

Frank Appunn, Professor of Information Technology, Thomas College and InfraGard Maine Chapter President

Kenneth Hillas, Adjunct Professor of International Affairs and Retired Senior Foreign Service Officer

Kristin Vekasi, Assistant Professor of Political Science and Assistant Professor of International Affairs

AN ANALYSIS OF INTERNATIONAL AGREEMENTS OVER CYBERSECURITY

By Lucas Ashbaugh

Advisor: Dr. Seth Singleton

An Abstract of the Thesis Presented
in Partial Fulfillment of the Requirements for the
Degree of Master of Arts
(in Global Policy)
May 2018

Research into the international agreements that increase cooperation over cybersecurity challenges is severely lacking. This is a necessary next step for bridging diplomatic challenges over cybersecurity. This work aspires to be push the bounds of research into these agreements and offer a tool that future researchers can rely on. For this research I created, and made publicly available, the International Cybersecurity Cooperation Dataset (ICCD), which contains over 350 international cybersecurity agreements and pertinent metadata. Each agreement is marked per which subtopics within cybersecurity related agreements it covers. These typologies are:

- Discussion and Dialogue
- Research
- Confidence Building Measures
- Incident Response
- Crime
- Capacity Building
- Activity Limiting
- Defense
- Terrorism

Drawing on ICCD and R for summary statistics and significance tests, as well as some quantitative insights, this research explores the relationship between different agreements, organizations, and other possibly related factors. The most significant takeaways from this research are:

1. Governments view cybersecurity in terms of relative advantages and are hesitant to engage competitors with agreements over topics like incident response and capacity building.

2. Authoritarian governments are involved with agreements over controlling or projecting state power and government authority while democratic governments focus on resilience and defense.

3. There are two groupings of authoritarian governments, those with high technical capabilities and those without. Technically capable governments focus on agreements over terrorism, and they also often end up participating in activity limiting agreements. Those without are preoccupied with agreements over criminal activity.

4. Discussion and dialogue agreements tend to accompany agreements over additional topics about one fifth of the time. While policy-makers shouldn't create a hard rule out of this statistic, it does possibly strengthen an optimistic hypothesis that dialogue consistently leads to agreements.

Hopefully this research invigorates researchers' interest in studying and understanding when cooperation over cybersecurity is successful or not. Policy-makers will need this knowledge if they are to achieve their goals in an environment that is rapidly increasing in state actors and complexity

DEDICATION

Even though my mom will most likely find this report itself boring, the accomplishment it speaks to, the high hopes for the future it represents, and the mere fact that I'm the author, will be anything but to her. Anyone that knows my mom knows that her ambitions for me, and the sacrifices she's made, go beyond what anyone can articulate. The fact that I've successfully navigated seven years of higher education could not have been possible without her heroic level of effort and active support.

This report stands as the culmination of the entirety of my academic and professional experience to date, and with it, I'm ambitious to start a fulfilling career, in which I hope that I can initiate the long process of matching the time and effort she's devoted to me. Thank you mom, I couldn't have done it without you.

ACKNOWLEDGMENTS

Dr. Seth Singleton – Professor Singleton has a robust academic background, having served as the dean of institutions in the US and Vietnam, and having taught at a much broader range of institutions spanning everywhere from Tanzania, to Russia, and more. Beyond his teaching, he has held grants from the National Council on Soviet and East European Research, the Rockefeller Foundation, the Fulbright program, and more. Professor Singleton graciously accepted to serve as my committee chair. As a long time security studies expert with a deep familiarity of nuclear arms control and U.S.-Soviet relations, his willingness to approach the new age security challenge of cyber security and serve as the head of my thesis committee was much appreciated. Our collaboration over this project was a bit of a 'melding of generations', applying conventional wisdom, knowledge, and experience to the dynamic and novel topic of cybersecurity as an international security concern. He guided this manuscript through multiple iterations and helped take what was originally a fledgling idea and frame it as a practical research project that can offer actionable results for policy makers. Without his attentive guidance and support, ICCD and this research would not have been possible.

Dr. Frank Appunn – Dr. Appunn is an educator on computer security and information technology at Thomas College. He is also a Certified Information Systems Security Professional (CISSP) and is highly active in the security community, volunteering his time at public/private partnerships actively contributing within the security community towards helping tackle some of the nation's most daunting cybersecurity challenges. His interdisciplinary and cross-institutional role in this project is exemplary of the exact types of

solutions that are needed to amply address cybersecurity as an international security concern moving forward. His oversight and technical fluency provided this research with a technical attunement that many similar projects all too often lack.

Kenneth Hillas – Professor Hillas is an accomplished, now retired, Senior Foreign Service officer. He has previously worked on special assignments involving conflict resolution, as well as having served in Prague, Moscow, Rome, Pretoria, Warsaw, and Washington; among many places. Beyond his career in the State Department he has taught courses on foreign policy at the National War College and continues to teach at the University of Maine. Regarding this project, his mastery and practical experience in diplomacy has helped apply context and nuance to this research.

Dr. Kristin Vekasi – Professor Vekasi is an experienced international political economist and professor. She teaches a range of classes covering economics and political science and has worked as a visiting Research Fellow at the University of Tokyo and a Fulbright Fellow at Tohoku University. She is an expert on North East Asia and has spent years conducting research in China and Japan. In the context of this thesis, she contributes her in-depth knowledge of the North East Asian region along with her superior knowledge of analytical methods towards helping me correctly draw conclusions.

Center for Systemic Peace – The underlying dataset that makes this research possible, the International Cybersecurity Cooperation Dataset (ICCD), is significantly enhanced by its inclusion of data points from the Center for Systemic Peace's Polity IV Annual Time-Series. The Center's willingness to grant me permission to include their polity data within ICCD while opening it up for a Creative Commons license will have a lasting impact on enabling future researchers to have important additional insights that would otherwise not be possible. (*See Appendix A for explicit written permission.*)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND DEFINITIONS

CBM – Confidence Building Measure

Cyber Attack – A cyber operation that is significant enough to prompt a government to claim it has been the victim of an armed attack under international law. The threshold for this is purposefully undefined by governments, hence it is not defined here.

Cybercrime – Traditional crime that is enhanced using digital technology, or maliciously abusing a digital device to operate in a way that is inconsistent with how it was designed to operate.

Cybersecurity – Ensuring that electronically automated devices are only used as they were intended.

Cyberspace – For the purposes of this research, taking into account previous academic debate over the topic, this is defined as anything involved in the collection, movement, sharing, or analysis of data through partially or fully electronically automated methods.

GGE – Governmental Group of Experts

IANA - Internet Assigned Numbers Authority

ICANN - Internet Corporation for Assigned Names and Numbers

ICCD – International Cybersecurity Cooperation Dataset

IETF – Internet Engineering Task Force

Information Security – The concept that there is a broader domain of information and dialogue within a country which governments have a sovereign right to control and protect.

ITU – (United Nations) International Telecommunications Union

Multistakeholder – A governance structure that not only involves multiple governments, but all key stakeholders, including members of the private sector and other interested parties.

NATO – North Atlantic Treaty Organization

NATO CCD COE – NATO Cooperative Cyber Defence Centre of Excellence

Protocol – A standardized technical process for achieving a specific digital task, often formalized by a whitepaper.

Public-Private Partnership – A forum/organization that facilitates dialogue and coordination between government and private sector activities.

SCO – Shanghai Cooperation Organization

UN – United Nations

Volatile – Only stored for a brief period of time before being permanently deleted, many network logs are considered 'volatile' as they are not stored long term or recoverable after a certain date.

Vulnerability – A flaw in a device/software that allows for someone to use or influence the item in a way that it was not intended.

INDEX

CHAPTER 1: INTRODUCTION

"We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here" (Barlow, 1996). Twenty years ago, John Perry Barlow's Declaration of the Independence of Cyberspace basked in governments' limited reach and the absence of sovereignty in cyberspace, a dynamic that continues to define the domain. The Internet's decentralized, international, open, and rapidly evolving nature (Strickling, Hill, 2017) has made traditional government approaches obsolete in managing the challenges inherent with cyberspace. Yet, while Barlow was correct that cyberspace is devoid of matter, it nevertheless relies on physical infrastructure, serves humans who live in sovereign territories, and depends on law abiding companies to make devices. It is at these control points that governments stake their claims, and where international cooperation has a chance of success.

This research aims to comprehensively understand international agreements over cybersecurity. In order to do this, I created the International Cybersecurity Cooperation Database (ICCD), which I use to explore what topics governments are working towards cooperating over, and how they are approaching these challenges. ICCD attempts to include every publicly accessible international cybersecurity agreement between two or more governments up until 2018. Each agreement has been marked as to what specific cybersecurity subtopics it pertains to: Discussion and Dialogue, Research, Confidence Building Measures, Incident Response, Cybercrime, Capacity Building, Defense, Activity Limiting, and Terrorism. Additionally, ICCD includes

authoritarian/democratic (polity), internet penetration rate (IPR), and high technology export data about the participants in each entry in an attempt to understand some of the influencing factors surrounding these agreements. Whereas there have been numerous studies on 'cyber conflict', this has not been matched sufficiently with studies of cooperation over those same challenges. This research aims to change that.

With this cooperation-oriented vision in mind, this research works towards three primary goals:

1. Offer a full picture of cyberspace and relevant diplomatic challenges, and present the current state of international cooperation over cybersecurity.
2. Identify patterns in existing international cybersecurity agreements that can assist governments in identifying future opportunities, and offer a tool for future researchers exploring this topic.
3. Identify areas of cooperation that are lacking and offer explanations.

Governments have a long way to go towards attaining a level of international cooperation that achieves their cybersecurity goals, yet this isn't for lack of trying. Governments around the world have turned towards a plethora of multilateral, multistakeholder, and bilateral forums in an effort to meaningfully engage each other over a diverse set of topics. These efforts have culminated in a great number of agreements, joint statements, frameworks, declarations, forums, and more. Yet attention and analysis on these efforts has been lacking, with the predominant focus remaining on 'cyber conflicts' and offensive operations. This report hopes to shift the dialogue towards a cooperation-oriented emphasis. Of course it is still useful to understand cyber conflicts, but the reward for understanding what contributes towards a successful agreement offers a more practical and immediate solution to many nations' foreign policy cybersecurity challenges. This

is especially true considering experts' ambivalence over the efficacy of deterrence techniques in cyberspace (Borghard, Lonergan, 2018). By scrutinizing previous international cooperation over cybersecurity, researchers can leverage this knowledge to guide future efforts, which is precisely what this report sets out to do.

In recent years governments have made a notably more significant effort towards cooperating, yet cybersecurity issues are expected to become increasingly destabilizing and cyberspace more conflict ridden (Healey, 2017). Recent cyber operations have experimented with increasingly destructive goals, like the attempt at not only crippling Saudi Aramco's production capabilities, but also at crippling the fail-safe mechanism that prevents an explosive disaster (Groll, 2017). This loosening of norms, along with the looming influx of additional governments who will soon have offensive cybersecurity capabilities, makes abundantly clear why cooperation over these challenges needs to be pursued, and soon. It's about time that thirty years of cybersecurity ignorance and shocking 'wake up calls' comes to an end (Healey, 2013).

CHAPTER 2: CYBERSPACE AND RELEVANT DIPLOMATIC CHALLENGES

A large factor of what makes cybersecurity so challenging to cooperate over is the uniqueness of the cyberspace domain, combining aspects from all of the traditionally considered domains along with new aspects. Its basic functionality and governance structure are so counter intuitive to how traditional international affairs operates that it often makes traditional strategies and approaches weak or entirely self-defeating. For anyone looking to forge meaningful cooperation over cybersecurity, there is a necessary base understanding.

Defining 'cyberspace' is a lively debated topic among practitioners and academics, but for the purposes of this study, I use the following definition:

> *Anything involved in the collection, handling, movement, sharing, or analysis of data through partially or fully electronically automated methods.*

'Cyberspace' resides on physical infrastructure that is set up as a series of recursive webs, a 'network of networks'. Each network connects to an even larger geographic network. Then, when very large connections must be made to connect different regions, high bandwidth cables are run between some of the most top level networks in order to connect them as well. While avoiding the nuances of transportation infrastructure, looking at cyberspace through the context of the traditional land domain, its structure can be compared with that of a national interstate. At its furthest points small local and private roads branch outwards from increasingly larger roads, with those largest avenues connecting to a network of national highways. Just like roads, different municipalities manage their portions with different rules and with varying degrees of maintenance. Also similar to roads, a washout at one point prompts drivers to find alternative routes to their intended destination. However this analogy becomes less useful as it is applied to

the more specific aspects of cyberspace. This description has only been for the 'physical' infrastructure the Internet resides on.

There is also a logical layer, which dictates which protocols devices use, or rather - which languages they speak. The 'World Wide Web' is a network of devices that speak the same language, Hypertext Transfer Protocol (HTTP). Yet, there are other logical networks that run off different protocols, for example the anonymous The Onion Router (Tor) network. These various 'logical networks' can be easily understood by comparing them to a stereotypical dirty college student's laundry bin. While there is one physical bin that holds all of the clothes, the student knows there are really two piles of clothes in the bin at any given moment. While the 'clean' and 'dirty' piles may get somewhat mixed up within this single laundry bin, they are very importantly two logically different piles. 'Cyberspace' encompasses all networks running on the Internet's physical infrastructure, even though some protocols may not have the technical capability to interact with one another.

Where most readers most likely aren't interested in an introductory networking lesson, this information allows for relevant insights. First off, each smaller network doesn't have to choose to connect to other networks and participate in the global Internet. On a national level, North Korea would be an extreme example of this; although the government does currently maintain two connections itself (Reuters, 2017). Also, drawing lessons from the traditional sea domain and the ocean, this giant network of networks has no central authority or point of control. Yes, networks operate within the territory of a sovereign government, but there is no inherent international jurisdiction mechanism. Data often crosses a multitude of static jurisdictions before reaching its intended recipient. For both the ocean and the Internet, governments can set their own rules within the parts they control, but experience real difficulties extending their

sovereignty past that point. A relevant example of such rule setting would be China's Great Firewall. Within China there is tight surveillance and a control of unfolding dialogues on the Chinese Internet. However, no one in any other country is directly affected by this, unless of course, they're trying to communicate with someone or something in China.

Unique to the Internet is that fact that the more devices that are connected to it, the more value it gains. The larger it is the more valuable it is. Without this dynamic, many authoritarian governments might otherwise be content not connecting to the international Internet, only maintaining a gated national network. However, this dynamic means that citizens want to have access to more online resources, which are often hosted in foreign countries, and therefore there's a demand to allow a certain amount of openness. This mix of a demand for openness versus governments' control over certain segments of the Internet produces many different governmental approaches for managing their Internet infrastructures. Likewise, as countries' connectivities increase, so do their vulnerabilities to malicious cyber activity (Brantly, 2016). Interestingly though, this doesn't necessarily have an equal influence on their offensive capabilities. North Korea maintains a clear asymmetric advantage in that it maintains competent offensive capabilities but has a rather small cyberspace attack vector for its enemies to target. On the opposite end of the spectrum, Estonia's highly Internet reliant society was the target of one of the world's most famous cyber attacks in 2007 called the Bronze Soldier Incident, when Russian patriotic hackers (enabled, or at least unfettered, by the Russian government) targeted the country with denial of service operations in anger because the Estonian government decided to move a famous Soviet war hero statue (Healey, 2013).

The Internet's internationally connected nature, and most countries' desires to continue their participation in an internationally connected Internet, means that countries must either bridge

their policy disagreements or learn to accept unwanted activity online. In one more extreme example, this dynamic can be seen in the U.S.-Chinese disagreements on cyber enabled theft. While this is a point of extreme tension for both sides (Ashbaugh, 2018), their need to participate in the Internet overcomes this negative aspect. Similarly, transnational crime benefits extraordinarily from the Internet. While the League of Arab States may deem gambling illegal (League of Arab States, 2010), Arab citizens can still relatively easily access gambling websites hosted in other parts of the world. The Internet enables criminals to commit criminal activity without being in the same country as their target, therefore not being accountable to that government's laws. This happened when Yevgeniy Nikulin stole 117 million LinkedIn user accounts all the way from Russia. Yevgeniy Nikulin has only been held accountable for his actions due to a cybercrime agreement between the United States and Czech Republic (Farivar, 2018). Along with many other malign activities, the Internet enables terrorist organizations to communicate and recruit through their own custom forums and social media, identity theft to be automated and information sold anonymously, and child exploitation and sex trafficking to be coordinated across borders. Many of these criminal activities are possible without cyberspace, but are enhanced by new technologies. Fortunately, this is an area where, at least in theory, governments agree on a need for cooperation. However, reaching an encompassing international consensus on what is illegal is politically fraught for everything but the most egregious crimes. This level of cooperation requires 'dual criminality', meaning that to avoid 'safe havens' unwanted activity must be punishable in all cooperating nations. Additionally, there's a need for 'mutual legal assistance' (MLA) agreements. Below is a brief excerpt from Pedro Verdelho, demonstrating how mutual legal assistance works (Verdelho, 2008):

> "In the beginning of 2005, a Norwegian citizen (let's call him A.T.) attacked a bank in Oslo. He intended to steal money and he did so effectively. During his action, a police officer was killed. A.T. ran away and could never be found in Norway. Some days later, police found and searched his home and computer and discovered that A.T. was the owner of an email account from a provider in the United Kingdom. International cooperation was required from British authorities which asked the provider to put this email account under surveillance. One day, A.T. used his account to send an email message. In the United Kingdom, police asked the ISP information about the IP address where the communication came from and it was found that it came from Spain."

This scenario also highlights another challenge involved with cybercrime, the volatility and inaccessibility of evidence. Cybercrime, such as the above example, scatters evidence across borders, making it difficult for an investigative authority to obtain. Additionally, much of this evidence is often volatile, as many organizations store logs and other pertinent data for only a specified (often brief) amount of time. If international cooperation were to move at its traditional slow pace, the evidence would be gone before a case could be made against a criminal. To solve this, most cybersecurity mutual legal assistance agreements contain a clause for legal proceedings between cooperating parties about ceasing data immediately upon request and then holding it for a longer period of time until international mechanisms can catch up to legally obtain the evidence.

Another area where international connectivity creates a lot of friction is in the spread of information. Liberal democracies overwhelmingly champion the idea of cybersecurity and achieving an "open, free, secure" Internet (Australian Government, 2017). This concept is opposed by Russia and China, particularly over the idea of 'cybersecurity', which implies the

technical security of devices. While China and Russia acknowledge this concept, they're more focused on the idea of 'information security' and a national 'information space'. This has much less to do with the security of infrastructure and devices, and everything to do with controlling available information and users' dialogues online. In 2017 alone, the Russian government's media and censorship branch, the Roskomnadzor[1], blocked 244 web pages daily, and an Internet user was attacked or threatened every six days (Meuza, 2018). In Chinese Internet censorship, the government's goal is in shaping public discourse and public consciousness, not in catching every dissident. The goal is to foster an environment where there is no demand for dissenting information in the first place (Chen, Yang, 2018).

This competition between these ideologies of freedom of speech and government guided speech and information have had a tangible impact between the competing governments and their respective private industries. Recently Apple was forced into moving the private keys that secure their Chinese users' accounts so that they are stored within China where they can be accessed by Chinese authorities, effectively surrendering any privacy Chinese citizens might have been granted by Apple accounts prior (Nellis, Cadell, 2018). Similar demands from the Chinese government that compromise privacy are common. The United States has been struggling with Russian efforts to sabotage the dialogue surrounding the 2016 elections (Director of National Intelligence, 2017). This can almost be considered ironic as Russia's large fear of losing control of its domestic dialogue online (Giles, 2013) was precisely what they tried to do in their operations against the United States.

[1] The Federal Service for the supervision of communications and mass media.

These incompatible ideologies about how the Internet should be tend to stunt progress towards further international cooperation. Among these ideologies are even more specific state and regional perspectives. At a conference in Hamburg in 2011, representatives were given a chance to share their perspectives, and many of these didn't align terribly well (Institute for Peace Research and Security Policy at the University of Hamburg, 2011). Possibly most interesting is the different states insistence on varying terms and definitions:

- United States

  International laws and norms should be solidified for cyberspace through the OSCE, G8, or OECD. This viewpoint emphasizes the fact that offline laws apply online, especially when it pertains to human rights. Additionally there's a strong belief in the efficacy of multistakeholder approaches. This viewpoint stresses the individual, as well as the interests of private firms, in playing a major influencing role in making decisions.

- Russia

  The Internet is dominated by US owned technology giants like Microsoft, Cisco, Apple, Amazon, etc., leading to a 'digital disparity'[2] between participants in the Internet. These companies, which promote U.S. values and are ultimately responsible to the U.S. government, unfairly impose their will on the Internet. States should have full sovereignty over their 'information space' including "the state of its security and the data contained". By referencing the data contained, this means content and censorship if necessary.

[2] Note that this is not a reference to the ITU's 'digital disparity' term.

- China

  Governments need to maintain a leading role in cyberspace, and the Chinese government is committed to "strengthening information and cybersecurity from new angles". Due to the Internet's connectedness, it is in no one's interest to use this space as a battlefield. "China does not see itself as one of the "cyber-powers" but rather as a major information and communication technology (ICT) user, who is facing severe challenges in cyberspace".

These three statements alone are illustrative of the rather complicated and frustrating situation these nations see themselves in. Both Russia and China assert their concept of needing to secure an 'information space', which is contradictory to the US's (and Europe's) push for policies that privilege the individual over the state. The US's calls for norms were met with resistance and frustration over the sole US stewardship of Internet Assigned Numbers Authority (IANA) and the preeminence of American technology companies. This sole stewardship was later transferred to a multilateral governance structure in 2016. Russia's frustration with the lack of diversity in technology companies speaks to a broader supply chain security concern. Russia and China both feel a need to produce their own devices and software so as to not have to source these from a country they have a competitive relationship with. While not listed here, in that same document France heavily emphasizes the idea that cyber diplomacy should be multistakeholder, which is exactly inverse of the Chinese perspective that governments need to maintain a leading role in cyberspace. Just from these brief statements, it's easy to see why progress is so difficult on a global scale. In one definitional example, the International Telecommunications Union (ITU) only officially adopted a working definition of cybersecurity in 2008 (ITU, 2010). The ITU's focus on definitions shouldn't be interpreted as bad. It demonstrates that challenges are rampant

even down to the most basic language involved in unfolding diplomatic efforts over cybersecurity.

Sovereignty and governance are a strong point of contention (DeNardis, 2014), and this debate directly affects international cooperation over cybersecurity issues. As Laura DeNardis humorously explains, “protocols are politics by other means”, with political impacts. Protocols are agreed upon standards of operation that individuals, companies, and governments agree to use. In a non-technical example, a common protocol is to say “hello” and “goodbye” during a phone call to avoid confusion, this same idea holds true to technical protocols. There is no law that two computers must use the same protocols. However if they don’t, they lose the ability to communicate as they then can’t understand each other, diminishing their value.

Protocols, and other standards in cyberspace, are mostly dictated by technocratic NGOs and multi-governmental organizations (MGOs); which is a significant departure from historical international-issues, because it marginalizes the role of most governments. The Internet Engineering Task Force (IETF) is a lead NGO in cyberspace which is run completely by volunteers. While there is no recognized authority on establishing technical protocols, the IETF is perhaps the closest thing to one, and these protocols often have strong policy impacts.

While seemingly apolitical, the fact that the IETF is run by volunteers introduces political challenges. Often, companies like IBM and other tech giants will sponsor representatives to work on ongoing projects through the IETF, giving them, and the more technological advanced countries these companies come from, a larger say in these politically critical standards. This multi-stakeholder consensus approach diminishes the ultimate authority of participating governments. Both of these aspects frustrate the Chinese and Russian governments. This

structure tends to keep developing countries out of the process, and bars anyone who can't afford to fly around the world to all of the needed international conferences from contributing to the IETF. This barrier has been something Brazil has previously been very vocal on within the Organization of American States (REMJA, 2015), advocating for figuring out a structure which doesn't disadvantage potential participants with less resources.

The Internet Corporation of Assigned Names and Numbers (ICANN) was transferred from US stewardship to a multi-stakeholder stewardship in 2016. It serves as the authority for top level domains (ex: .com, .edu., .uk, .cn, etc…) and other Internet backbone nomenclatures. Names and numbers online are of specific interest, because while the Internet is a diffuse and decentralized structure, there absolutely must be agreement on the individual assignment of names and numbers. If there are duplicates, the network can't function properly.

Such lack of governmental control, and existing competition for increased power in Internet governance, makes cooperation over many cybersecurity issues more difficult. It means that nothing can be enforced throughout the entire Internet unless there is an international consensus or a pertinent non-governmental organization such as ICANN makes the decision, a process which often ignores the requests of certain governments and communities.

The United Nations International Telecommunications Union (ITU) has also become a global leader in making decisions. As a branch of the UN, they are arguably the most equitable in giving each government a say. The ITU is mostly used as a forum for implementing technical standards across countries, increasing global penetration rates, and for convening governments to find areas of increased cooperation or for joint research. In one example they helped Arab countries set and meet better cybersecurity standards for themselves (ITU, 2017). However, the

ITU's international nature forces it to avoid contentious cybersecurity topics, which it often defines as "questions of cybercrime, national defense and security, and legal or policy issues" (ITU, 2010).

Also crucially important is the immense clout that the private sector holds in cyberspace and regarding cybersecurity, and more specifically the clout of U.S. companies. Whereas other countries have their own competencies as well and are starting to challenge this, notably China and their hardware, U.S. private sector influence is still very strong. Cyberspace is possibly the only domain in which sovereign governments are ambitious to enforce their jurisdiction but loath to provide defense for their citizens or hold a strict monopoly on power. While governments defend their own governmental assets, they leave it up to private entities to defend themselves, only involving themselves when a severe case warranting their attention arises. This stems from the impracticality of governments having the resources to amply defend the overwhelming number of private networks out there. Addressing this, public-private partnerships have had some success. These organizations facilitate meetings and events for information and best practice sharing between governments and the private sector. Some rather successful examples have been the United State's Infragard and the European Union's 'Public-Private Partnership' (sometimes referred to as P3). Within the United States some policy makers dislike the idea of being responsible for defense of private networks in certain instances, and there has been discussion of ceding that authority to the private sector.

'Active cyber defense' measures are a spectrum of activities that span everything from information gathering on an attacker to actually disrupting their computer systems all together (Hoffman, Levite, 2017). The United States has released documentation preliminarily exploring 'active cyber defense' measures, commonly known as 'attacking back' (Chesney, 2017). This

would empower private companies to take things into their own hands and punch back. However, removing the government's monopoly on initiating offensive operations has drawn a lot of criticism. Many are skeptical about the competence of the private sector to be able to do this, and about the consequences of the common yet legally complicated scenario where the attacker is in a different country, meaning that a counter operation from a private source might break another nation's laws.

Because cyberspace is a domain constructed by humans, the companies that produce the devices it was constructed with have a certain amount of clout. The fact of the matter is that it's hard for governments to make any meaningful progress over cybersecurity topics without engaging large technology firms. Say for example, governments are looking to alter encryption standards. Without having RSA[3] (a dominant encryption company) and other large technology companies in the discussion, it's hard to make any progress beyond statements and recommendations. Yet governments have other levers to pull. A company's nationality grants its respective government a certain amount of power. In this specific example with RSA, the U.S. National Security Agency (NSA) gave RSA encryption tools to incorporate into their products, supposedly with the veiled (or not disclosed but explicitly agreed) intent that it would allow them to more easily crack RSA's encryption (Chabrow, 2014). Yet, no matter how governments chose to engage private companies, it remains clear that private companies' cooperation is needed for governments to reach goals.

This decentralized, overlapping, and murky governance of the global Internet makes implementing cooperative agreements over cyberspace a particular challenge. Bilateral

[3] RSA is named after the encryption standard 'RSA', which is named after its creators Ron Rivest, Adi Shamir, and Leonard Adleman, the company's name is the abbreviation 'RSA' and not the spelt out version of the standard.

agreements often only work at addressing specific concerns of interactions between the two negotiating governments. Multilateral international agreements are often hard to get a final consensus on, and even when a consensus is reached, seeing to it that the terms of an agreement are properly implemented throughout the entirety of a country's highly decentralized cybersecurity organizations is daunting. Regional organizations seem to be the preferred option that balances these challenges, yet even then they are often non-binding or minimum in their requirements. It is hard to enforce agreements among such decentralized national and international structures.

While there are already huge challenges over topics like cybercrime, competing perspectives, and Internet governance things are about to get much more complicated. As more and more governments work to develop their offensive capabilities, it's expected that there will be a sharp increase in the number of actors in cyberspace. Unlike other domains, less talented actors are more dangerous, as they don't have the resources (and in some cases desire) to run precise operations. This year Lebanon ran a rather broad spyware operation targeting cell phones looking to capture video data (Reuters, 2018). Ethiopia also ran an espionage campaign against Ethiopian dissidents in the US and UK (Marczak, Alexander, McKune, Scott-Railton, Ron Deibert, 2017).

This influx of offensively capable states has the possibility to significantly weaken international stability. However, there is evidence to suggest that states have shown a certain level of restraint in cyberspace, and that possibly this increase of offensively capable states may not be as destabilizing as some might assume. Recent research by Brandon Valeriano and Ryan Maness has shown that governments, without the explicit deterrence of others, choose to restrain themselves from using information and communications technolgies (ICTs) offensively in the frivolous way many previously expected (Valeriano, Maness, 2015). Similarly, building on

previous research (Axelrod, Iliev, 2014), Brent Maheux explains that when the matter at hand is of a ‘Cyberwarfare’ or ‘Political’ natures, an attacker resorts to using malware only when the stakes are high and of a clear ‘Cyberwarfare’ intention (Maheux, 2014). As examples he offers the highly sophisticated U.S./Israeli Stuxnet virus that targeted the hardware at the Iranian Natanz nuclear facility in 2010 and the Flame spyware that spread across the Middle East is 2012. This is significant in that there are a many circumstances where a possible attacker decides against an attack. However this restraint is considered by some experts to be merely wishful thinking, or ephemeral as more governments come into play.

Many possible reasons could be causing this restraint, and most likely it is a combination of reasons. One possible influence is the fear of ‘blowback’. Blowback is the idea that once an attack leveraging a new vulnerability is used, the government that used it immediately loses control of it. This might result in other governments copying this attack and finding the same vulnerabilities in the original attacker, and attacking back using the same methods. Whether or not this fear truly influences governments’ decisions, current evidence suggests it is a rational fear. Leyla Bilge and Tudor Dumitras demonstrated that once a vulnerability is disclosed, “the number of malware variants exploiting them increases 183–85,000 times and the number of attacks increases 2–100,000 times” (Bilge, Dumitras, 2012). Additionally, these numbers suggest that an attack that uses a new vulnerability very well might cause collateral damage. This could mean that other organizations in different industries and countries with the same vulnerability may be harmed, and the original attacking country might be to blame for not properly considering the collateral damage of their actions (Schmitt, 2017).

This idea, the idea that governments restrain themselves due to a bundle of various risk factors, seems well demonstrated in historical instances. However, it is consistently challenged by

indiscriminate operations such as North Korea's WannaCry ransomware and the Russian NotPetya malware that the U.S. executive branch deemed the 'biggest cyber attack in history'. Nevertheless, there is still a compelling case to be made that governments refrain from using cyber attacks even when they would accompany kinetic violence because of fear of the repercussions. Jason Healey explains that U.S. forces in Libya refrained entirely or partially from deploying cyber means along with their kinetic actions (Healey, 2013). Overall, world leaders might be nervous to break the existing norms against practicing 'cyber restraint'. Richard Clarke explains that:

> "the Bush Administration was apparently unwilling to destroy Saddam Hussein's financial assets by cracking into the networks of banks in Iraq and other countries. The capability to do so existed, but government lawyers feared that raiding bank accounts would be seen by other nations as a violation of international law, and viewed as a precedent. The counsels also feared unintended consequences if the U.S. cyber bank robberies hit the wrong accounts or took out entire financial institutions." (Clarke, 2011)

The idea of risk in cyberspace is poorly defined and elusive. Yet while it is hard to fully understand and grasp, 'risk' in cyberspace is clearly an overwhelming influence on governments and a critically important consideration. Governments with new offensive capabilities may or may not demonstrate this same level of restraint, but many other governments would rather not wait and find out. There has been a vigorous revival of dialogue around the matter of 'confidence building measures' (CBMs), which famously contributed towards ratcheting down Cold War tensions that might have otherwise had nuclear consequences (Helsinki Final Act, 1975). However the environment in which CBMs are being negotiated is notably different from previously famous confidence and trust building gestures and agreements. Agreements such as

the Anti-Ballistic Missile Treaty, Prevention of Incidents In and Over High Seas Agreement, and Limited Nuclear Test Ban were all negotiated in a bipolar NATO versus Warsaw Pact environment, strikingly different from today's multi-polar world. Many post Cold War Agreements, like the Open Skies Treaty and Convention on Cluster Munitions, have asserted a multi-polar emphasis. These were all treaties. Confience and trust efforts as they currently relate to cyberspace are not treaties at all. Many of them are merely frameworks that governments may use as a tool, and the strongest of them are non-binding voluntary norms such as refraining from targeting computer emergency response teams and not allowing illegal activity to operate out of a government's sovereign territory when they have the ability to stop it.

The Cold War produced extensive literature focused on CBM theory and how to best contribute towards CBMs. This work included Osgood's Graduated Reciprocation in Tension-reduction (GRIT) Theory (Goldstein, Freeman, 1990) calling for unilateral benign actions without need of reciprocation from an adversary, or Axelrod's 'tit-for-tat' approach of simply mimicking an adversary's moves in ratcheting up or down hostilities (Axelrod, 1981). No similar theory has been produced on CBMs regarding cybersecurity. These bipolar focused theories aren't tested for multilateral efforts, and considering all of the challenges involved in international cooperation over cybersecurity, it's easy to understand why reaching meaningful CBMs is a daunting task.

With all of these diplomatic challenges, obtaining a better understanding of what contributes towards implementing a successful cybersecurity cooperative activity is both timely and necessary to ensure future progress.

CHAPTER 3: CURRENT STATE OF INTERNATONAL COOPERATION

The current state of international cooperation over cybersecurity is, at best, frail. However, these prevailing agreements are the culmination of particularly burdensome work on behalf of those championing such efforts, and provide a useful groundwork for continued cooperation.

This slow pace is no surprise as norm building has always been a slow and repetitive process. Establishing a collective expectation for proper behavior (Finnemore, 2018) takes time and refinement. Likewise, policy has traditionally lagged behind technology. Considering the compounding influences of rapidly evolving technologies and gruelingly slow norm building processes, it's impressive that agreements have made it as far as they have.

Since 2003 the United Nations General Assembly has maintained a Governmental Group of Experts (GGE) (UN, 2003) who have been devoted to research into "Information and Telecommunications in the Context of International Security". Over the years this multinational group has explored viewpoints and concerns from UN members, all the while producing the occasional report. The most prominent of these was the 2013 report, which many policy makers viewed as the first truly global assertion that international laws apply in cyberspace. Equally as important, this agreements was followed by a 2015 report (UN, 2015) which got all members to agree to a set of 'voluntary non-binding norms'. The achievements of these two documents are seen by many as the most comprehensive international agreements over cybersecurity to date, specifically citing the voluntary-norms that were established:

- States shouldn't allow their territory to be used for 'internationally wrongful acts'
- States must not use proxies to commit 'internationally wrongful acts'

- States should not conduct or support activity to harm authorized emergency response teams
- A State should not conduct or knowingly support activity contrary to its obligations under international law that intentionally damages critical infrastructure *('International Law' referring to numerous prior G7/G8, G20, and UN agreements)*

The degree to which these norms have been followed seems rather pessimistic. Russia has been caught red-handed supporting their well known Cozy Bears proxy group (Reuters, 2018) and Iran has been exposed for maintaining a strong relationship with criminal organizations it sometimes calls on to do favors for the state (Anderson, Sadjadpour, 2017). North Korea's WannaCry ransomware was blatantly indiscriminate in 2017, crippling some hospital systems (critical infrastructure) in the UK. Further still, 'international law' is a tenuous concept in cyberspace, which is most clearly defined by the Tallinn Manual that is not even officially ratified by any government (Schmitt, Vihul, 2013). The concept of international law in cyberspace is highly contentious. Following their 2015 report, the UN GGE continued its work towards further progress, yet it was unable to reach a consensus and offer a report in 2017 due to a disagreement over a clause that asserted that international law applies in cyberspace. The debate over the applicability of international law in cyberspace remains because some governments, Cuba among them, want the ability to use asymmetric cyber capabilities without dealing with the consequences of their actions being considered an armed attack (Sukumar, 2017). Likewise, governments like Russia and China are hesitant to adopt international laws that would qualify cyber operations as attacks because that would mean victims might have a legal right to respond, which is counter to many Western countries that advocate for this because of this very reason.

While much of the hype around cybersecurity tends to gravitate towards complex state backed operations, the bulk of malicious activity online is in fact cybercrime. The Council of Europe's 2001 Budapest Convention, commonly known as the Convention on Cybercrime, is perhaps the most successful international agreement over this challenge. The convention is open to anyone and acts as a joint mutual legal assistance and extradition agreement between members. The agreement targets blatant criminal activity that every country can agree to as detrimental. It aims "to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation" (Council of Europe, 2001). The agreement covers everything from minimum sentencing to data retention and procedural law. The Convention on Cybercrime has been a relative success, yet many countries haven't signed it, limiting its authority. Russia and China haven't signed the document, and many nations from other regions haven't ratified the document yet. The Economic Community of West African States (ECOWAS) has attempted a similar document, but it doesn't serve as an extradition treaty, requiring every member to forge such an agreement with every other participating member if there is any chance of it being useful, which hasn't happened so far (Orji, 2015).

Less ambitious yet more uniformly subscribed to has been the (former) G8's 24/7 Contact Network. This open agreement merely requires participating states to appoint a specific department within the government to act as the authority on cybersecurity which foreign governments can contact. This department is then charged with running a permanent office that can accept communications for clarifying communications or increasing cooperation (G8, 1997).

The Organization for Security and Cooperation in Europe (OSCE) has also become an important player. The unique history of the OSCE in facilitating confidence building measures sets them

apart as possibly qualified to facilitate this once again, but this time with respect to cybersecurity. In 2013 the OSCE released a set of original transparency measures members could pursue. This was bolstered further in 2016 by the release of sixteen cyber confidence building measures (CBMs) that countries could consider (OSCE, 2016). At the moment, while these CBMs are useful suggestions, there has been little initiative by any member to see them actually implemented. In general, governments have leaned more towards the previously mentioned non-binding voluntary norms as opposed to any more serious CBMs.

The Coordinating Center Computer Emergency Response Team (CC-CERT) was originally a US Defense Advanced Research Projects Agency funded incident response organization. However as the Internet expanded, it also expanded to become the coordinating authority for over two hundred CERTs around the world. These CERTs focus on acting as first responders to technical incidents, like when the City of Atlanta's public resources were held hostage by ransomware (Romo, 2018). Additionally, most CERTs participate in the Forum of Incident Response and Security Teams (FIRST network), a cooperative platform for emergency incident teams around the world. Above all else, CERTs retain their autonomy, often sharing similar organizational structures but coming from vastly different environments and maintaining what can sometimes be a rather loose communication network. For example, while the US-CERT has been granted national authority for its activities, many other CERTs have merely assumed such a role in their respective countries and operate in a sort of legal vacuum (Choucri, Madnick, Ferwerda, 2014). While CERTs or the FIRST network don't match the definition of an agreement for ICCD, they're important to mention as they fill what would otherwise be a large gap in needed international cooperation. CERTs cooperate over non-politically contentious technical and procedural matters such as sharing vulnerability information about common products. The

FIRST network is a multistakeholder organization, consisting of teams from most nations as well as regional and market specific teams (Amazon SIRT, MSCERT, Huawei PSIRT, etc..). A corporation or special interest group often funds the CERT which focuses on it, such as Amazon funding the Amazon SIRT or the special interest U.S. Industrial Control Systems CERT.

Worth mentioning are the North Atlantic Treaty Organization (NATO) cyber defense bloc and the Shanghai Cooperation Organization1 (SCO) information security bloc. While it wouldn't be fully accurate to describe them as competitors, it's clear that they disagree on even the most basic of definitions. Beliefs and ideologies of individual liberties versus state rights often clash in international forums like the UN, but are areas of agreement among members of NATO and the SCO.

NATO declared at their 2014 Wales Summit that a cyber attack could be as harmful as a physical attack, and therefore declared its right to consider a cyber attack as triggering its Article 5 mutual defense clause, warranting an armed response (NATO, 2014). NATO has avoided defining this any more specifically, leaning toward a 'strategic ambiguity' policy that allows them to take possibly qualifying incidents on a case by case basis. Taking their stance a step further, NATO declared cyberspace an operational domain at their 2016 Warsaw summit, asserting it will work to maintain "freedom of action and decision" in cyberspace (NATO, 2016). Beyond these agreements, most NATO members participate in the NATO Cooperative Cyber Defense Center Of Excellence (NATO CCD COE), which was established in Tallinn, Estonia, following the denial of service attack that targeted Estonia in 2007. Through this organization, a group of lawyers produced the acclaimed Tallinn Manual 2.0 that aims to lay out what the international law of cyberwarfare should be, although this work hasn't been officially endorsed by any governments (NATO CCD COE, 2013). The NATO CCD COE's mandate has been recently

expanded to include training and education (NATO, CCD COE, 2018), Japan has been accepted as a member as well.

The Shanghai Cooperation Organization[4] (SCO) is another organization which member governments have used to pursue their cybersecurity goals through. In 2008 the SCO released the 'Agreement among the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security'. This document emphasized cooperation over ensuring their concept of information security, specifically listing the "dissemination of information harmful to social and political, social and economic systems" as a perceived prioritized threat (Shanghai Cooperation Organization, 2009). The definition of 'harmful' is dubiously broad here allowing states to subjectively deem content 'harmful' when in reality it is merely dissenting. SCO members have repeatedly looked to assert an 'international code of conduct' through the UN. They introduced the idea once in 2011 and then again in 2015. While many countries can consistently agree on working towards defining 'responsible state behavior' in cyberspace, the SCO members' proposal was rather one sided. It looked to reaffirm the UN's commitment to state sovereignty, therefore legitimizing censorship and freedom of expression abuses in cyberspace, and denying other countries the ability to take action against such activities. Furthermore, it tried to emphasize a multilateral Internet governance system, based only on governments, which ran opposite to many liberal democracies' pushes for a multistakeholder system (NATO CCD COE, 2015).

[4] China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan were SCO members when most of the agreements pertinent to this research were agreed upon. India and Pakistan have now since joined as well.

CHAPTER 4: METHODOLOGY

Before I can identify patterns in existing agreements, and areas and types of agreements that are lacking, I need to explain what process led to these conclusions and why certain methodological decisions were made. This section describes how data was collected and turned into usable information. Anyone who replicates this research through repeating these processes and decisions should arrive at the same results. Additionally, just as with any study, there are a few biases discussed that future researchers may hopefully be able to eliminate or mitigate more effectively.

International Cybersecurity Cooperation Dataset (ICCD)

This paper is the result of a preliminary analysis of the International Cybersecurity Cooperation Dataset (ICCD). ICCD contains over 350 entries. It is a best effort attempt at cataloging all international cybersecurity agreements between governments ('agreements' are defined later in this section). ICCD contains metadata about each agreement, and marks each entry so that they can be sorted by which subtopic within cybersecurity each pertains to. These subtopics are referred to as 'typologies'. ICCD also includes additional data on 'related variables', describing the governments involved in each agreement, to illustrate a fuller picture.

Sources

This dataset sourced a limited number of documents from the Carnegie Endowment for International Peace Cyber Norms Index and the NATO Cooperative Cyber Defense Center of Excellence (NATO CCDCOE) INCYDER Dataset. Yet, these datasets only aim to provide the most signifigant documents within their respective scopes, as opposed to a comprehensive approach. Also, both of these datasets use their own typologies and are missing categories I thought important. Given these realities, the main source of dataset entries are primary documents and sources that were found using a Google search. A Google search was conducted for every existing country using the key words: “cybersecurity” and “agreement”. Additional tailored online searches were conducted to find documents that were referenced in previously collected documents or sources.

Data

Each source was scrutinized and then entered into ICCD along with the typologies it pertained to, related correlating variables, and the appropriate metadata. ICCD looks to enable research and analysis with a focus on existing international cybersecurity agreements. This ultimately led to the decision to construct the dataset with one entry per agreement. Some alternatives to this were constructing the dataset by country or organization. However to do so by country would not only result in over 10,000 entries, it would also only be useful for countries which have pursued agreements often enough to generate enough data to draw conclusions from. Similarly, organizing the dataset by organization would have faced the same challenges, and made comparisons between bilateral and multilateral/multistakeholder agreement difficult. For these

reasons, and keeping true to the focus of the dataset being on agreements and activities, not countries, the dataset was constructed by agreements.

ICCD can be thought of as two separate datasets (divided into separate sheets), one for bilateral and one for multilateral/multistakeholder agreements. This is because the two types of agreements benefit from being compared with different types of influencing data. For example, the range in polity[5] between the two participating countries when considering bilateral agreements is revealing, while doing the same for agreements brokered through organizations as broad as the United Nations is rather useless because all types of political systems are represented.

For each entry into ICCD, the following data is listed:

- **Title** - The title of the source. Sometimes these titles are altered slightly upon entry into the database for readability, however the essence of the title is always respected.
- **Date** - This is the beginning date of the cooperative activity or agreement. The date of ratification is used when multiple dates are supplied.
- **Organization** - When applicable, this denotes what international organization this agreement was brokered in.
- **Description** - Each entry was read in entirety and a brief qualitative description was supplied. In instances when a larger document covered multiple topics, the description and research efforts only focus on those parts that are pertinent to cybersecurity. Text was quoted

[5] The Center for Systemic Peace graciously gave their explicit written consent (Appendix B) to allow some of their polity data to be included in ICCD.

in instances where information was presented in a concise enough way to quote within the dataset.

- **Typology** - Every entry was assigned typologies pertaining to the agreements, this was often multiple typologies. These typologies were:
  - **Discussion and Dialogue** - This activity requires the least commitment from parties and just involves agreeing on future discussion and dialogue to exchange viewpoints and opinions. This includes forums, conferences, dialogues, high level meetings, agreements on future meetings for further discussion, and in many cases working groups.
  - **Research** - This activity pertains to research into social science information surrounding cybersecurity as well as technical research (often agreements are not terribly articulate on clarifying this). This includes surveying parties, establishing expert groups, and academic/multistakeholder studies.
  - **Confidence Building Measures** - These measures include information sharing, voluntary norms, points of contact and hotlines, and some capacity building efforts when the clear purpose is to establish confidence and trust to prevent destabilizing activities from harming relations. To avoid definitional challenges, this research does not require a certain amount of competitiveness or an adversarial relationship to be present for something to be considered a confidence building measure. The decision to define this typology so broadly was due to known high profile cases of close allies having distrust in one another, for instance as a results of the post-Snowden revelations when U.S. operators were revealed to have aggressively pursued targets, even when they were on European networks, without notifying these allies.

- **Incident Response** - This pertains to coordinating across government agencies how to best handle incidents. While CERTs and CSIRTs clearly fill this role, this study focuses specifically on governments and their agreements involving this. These agreements often blur the lines between governments and their CERTs. In some instances governments agree to enhance their CERTs' cooperation with one another. Considering government involvements in these agreements, these instances were included under this category.
- **Cybercrime** - While criminal activity is defined differently across the globe, this category applies to any agreement to manage and deal with activity that is deemed illegal by a given government. This activity also includes dealing with victims of criminal activity (such as child protection agreements).
- **Capacity Building** - This activity pertains to efforts to increase offensive and defensive capabilities through training, cooperation, or providing equipment. This often deals with protecting critical infrastructure, but can also deal with offensive capabilities. Notably, countries often agree to build capacity in 3rd countries, yet it is often unclear if they reference this in a security or development context. When a clear development context (absent of any cybersecurity context) can be discerned, the potential entry is excluded.
- **Activity Limiting** - This broad title references when governments agree to refrain from certain activities. Most commonly this is seen in agreeing to refrain from theft "for commercial gain". However agreeing not to target CERTs and CSIRTs, as well as other activity limiting, is sometimes mentioned.
- **Defense** - This looks at mutual defense, or cooperative defensive agreements. While capacity building may sometimes improve a country's defensive posture, these activities look at mutually pursuing strong cooperative defense activities.

- **Terrorism** - This research does not define terrorism. However when countries use terms such as ‘extremism’ or ‘terrorism’, those agreements qualify for this typology.

- **Link** - A link is provided to every source, which is usually a primary document or government site. All of these links were ‘live’ at the construction of ICCD, although it is possible that some may become ‘dead’ in the future.
- **Bi / Multi** - This marks if the cooperative activity was bilateral, marked by a ’B’, or multilateral/multistakeholder, ‘M’.
- **Countries** - This lists the countries involved in alphabetical order.
- **Notes** - When there was a complication, additional source, or other need for commentary, a note is provided.

Additionally, correlating variables were added to each entry, pulling from different datasets from the same year as the initial ICCD entry. The variables aim to provide related pertinent data that may offer a wider perspective regarding these cooperative activities. These variables are described below, along with their source:

- **Variable:** Polity

  Source: Center for Systemic Peace

  Dataset: Polity IV Annual Time-Series, 1800-2016

  Link: http://www.systemicpeace.org/inscrdata.html

  Description: ‘Polity’ is a quantitative value derived from quantifying a country’s ‘democracy’ score and ‘authoritarian’ score, and subtracting the latter from the former. This provides an idea of what type of government is in place. It should be noted that the underlying theory that led to the creation of ‘authoritarian’ and ‘democracy’ scores proposed that these are not opposites and that they can coexist. Polity is a popular tool

within the research community and still provides an insight into the type of government in place.

- **Variable:** Internet Penetration Rate

  Source: World Bank

  Dataset: Internet World Stats

  Link: https://data.worldbank.org/indicator/IT.NET.USER.ZS

  Description: 'Internet Penetration Rate' (IPR) is a measure of what percentage of a country is able to access the Internet. It is often used to facilitate a discussion on how much Internet infrastructure a country has. While useful, it should be noted that 'having access' to the Internet is entirely different from being able to use it. A variety of challenges like monetary costs, language barriers, and technical fluency often prevent those who 'have access' from using the Internet. In fact, half of the world isn't even connected to the Internet, and of the 'connected' half many are unable to use it. That being said, rolling out the infrastructure is a mandatory first step in connecting people to the Internet and is therefore a useful measure (ITU, 2018).

- **Variable:** High Technology Export Percentage

  Source: World Bank

  Dataset: High-technology exports (% of manufactured exports)

  Link: https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?view=chart

  Description: This variable tracks what percentage of exports are classified as being 'high technology'. For the purposes of ICCD, it is used as a proxy variable for the technical capability of a country. This is not a perfect measure by any means, as there is often a disconnect between what a country is exporting and what it is capable of. However it is

the best fit given the alternative proxy variables. Including this variable is important because there is often a disconnect between how much Internet infrastructure a country has and how technically capable it is, especially with less developed and developing countries.

Restricting Research Scope

International agreements over cyberspace and cybersecurity challenges represent a broad and blurry spectrum. These activities range from: international multistakeholder discussion forums, expert groups, voluntary norms, joint statements, explicit agreements, and many other types. While explicit agreements and signed documents clearly belong in this dataset, defining a cut-off for 'loose form' cooperative activities is much more challenging. Most difficult to differentiate are forums, conferences, and dialogues. Without a set scope, this dataset would quickly become a collection of every international government event pertaining to technology ever held, which is well beyond the scope and resources of this research. For this research, a loose form cooperative activity was included if the present government representatives had the authority and intention to make new commitments or progress directly on behalf of their government. For example, while the U.S.-Germany Cyber Bilateral Meetings consistently affirm commitments, the Sino-European Cyber Dialogues tend to only be focused on a continued discussion that doesn't share this intention and produces no such results. This distinction is sufficient for most cooperative activities, yet it benefits from clarification regarding research activities. A report pertaining to cybersecurity doesn't in itself qualify for entry into ICCD. For research activities to count, governments had to agree to conduct such research in order to make some form of tangible

progress or commitment from governments. For example, the ITU's research in 2010 on definitions and terminology was intended to secure much needed universal terminologies that governments could agree upon and work from. Therefore, this has been included in ICCD. On the other hand, the special topic reports that the ITU puts out throughout the course of its regular operations, while inherently international due to the organization, are not included if they make no direct effort at attaining progress or commitments where they had been previously lacking.

Additionally, defining a scope requires making decisions as to what challenges pertain to 'cybersecurity', a process that inherently involves excluding certain topics. Notably, anything relating to the topic of privacy was not included in this dataset. While privacy defines laws for what people and organizations are permitted to keep secret or share within the bounds of the law, security deals with mitigating and managing activities that breach laws and in many instances access secret information. This means that numerous agreements such as the EU General Data Protection Regulation (GDPR), the US Clarifying Legal Overseas Use of Data (CLOUD) Act, and the ECOWAS Supplementary Personal Data Protection Act are not included in this dataset. This is a clear opportunity for future research.

Definitional Challenges

When constructing ICCD, there were two possible methods for flagging entries for typologies. One method was to review each potential source to properly enter it into the dataset based on the qualitative features the source possessed. The other was to strictly search for the use of specific language. Given the acute definitional barriers this field still experiences, as well as possible

translation issues, a qualitative review of each source was picked as the method for flagging entries for typologies.

Additionally, while this method provides a more accurate representation than alternatives, it also relies heavily on context. This requires making a best effort at distinguishing 'capacity building' in a cybersecurity context versus a development and connectivity context. Other challenging instances of this can be found in statements which cover many topics, including topics such as cybersecurity, counter-terrorism, and research. All of these items have different meanings inside, and outside, the context of cybersecurity. This was often very challenging. Many UN documents like to include the following phrase in their opening sections: "Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes". Some organizations start an international agreement with an exhaustive list of that forum's previous agreements, even if the listed items are more or less unrelated to the focus of the present agreement. These references were not considered for ICCD as these lists are so commonplace that they would dilute ICCD significantly.

Biases

Inaccessible Information

Most challenging to this research is the difficulty in finding the ICCD data. Governments often do a poor job releasing information about their cooperative activity over cybersecurity. There are many instances when there was sufficient information about a third meeting or agreement, but finding the prior instances was highly difficult or impossible. Coupling this is the possibility that many governments may not want their exact efforts fully disclosed for what they deem as

security reasons. There are likely instances of close cooperation between staunch allies that are not available to the public. This lack of information could bias data away from more serious military and intelligence cooperation being well represented in ICCD.

Language Barrier

These cooperative activities are sourced from a variety of languages. While Google translate is able to assist with plain text information that is found in a different language, this barrier still prevents searching for these activities in countries' official languages or in documents that were only scanned and put online. For the purposes of the ICCD, agreements in English were included.

Missing Bilateral Data

At times data was unavailable, especially in agreements that were reached in 2017 or in recent years. This means that an analysis of all of the polity scores for the entirety of the bilateral data will be less than the total quantity of agreements. As with any quantitative study, more data would be preferable and improve the accuracy of this study's results. In the future, it would be appropriate for researchers to replicate these methods, given new additional data, to see if the same conclusions are still reached.

Unequal Country Representation

There is no way around it, some countries are just more active in pursuing cybersecurity agreements. China and the United States are obvious examples of this. While this does affect the data, it doesn't degrade its utility. The matter of fact is that some governments have unequal clout and interest in cyberspace, and until this changes, these findings drawn from ICCD will

continue to be valuable. Additionally, the sheer quantity of agreements included in ICCD and its attempt at being fully inclusive tries to mitigate the risk of over-representation of certain countries in the data.

Quantity Versus Quality

This research focuses on leveraging ICCD to facilitate a quantitative analysis because it is the first time a quantitative approach has been possible for the topic of international cybersecurity agreements. With that in mind, readers should practice a healthy skepticism that quantity doesn't determine the quality or efficacy of the included agreements. This research never asserts that one agreement is necessarily better or more effective than another. However, the quantity of agreements does provide insights, such as suggesting where governments are placing their priorities, or where agreements have been easier to achieve. In a domain where governments are struggling to enforce a basic set of norms and sets of acceptable behavior, quantity and repetition of agreements is valuable information.

Analysis Tools Used

Using ICCD, RStudio was used to facilitate a series of analysis. These analyses have been sorted below alphabetically by the tools used to achieve them, followed by a purpose and explanation.

- *ANOVA* - An 'analysis of variance' (ANOVA) test confirms that the means of multiple categorized groups of numbers are in fact statistically significantly different from each other. In this instance an ANOVA test would communicate if the chosen typologies are statistically

different from another, or if there's a chance that they are possibly [mathematically] the same.

- *Average Polity And Range*- Any bilateral agreement has two polity scores, one from each government involved, combining these gives an average polity. Over the aggregate of all of the bilateral agreements, especially once sorted by typology, this provides useful insights, along with the range.
- *Average Internet Penetration Rate and Range* - Any bilateral agreement has two internet penetration rate (IPR) scores, one from each government involved, combining these gives an average IPR. Over the aggregate of all of the bilateral agreements, especially once sorted by typology, this provides useful insights, along with the range.
- *Average Tech Capacity And Range* - Any bilateral agreement has two high technology export percentages, one from each government involved, combining these gives an average high technology export. Over the aggregate of all of the bilateral agreements, especially once sorted by typology, this provides useful insights, along with the range.
- *count* - A simple count of the number of agreements that pertain to each typology. This can reveal which agreements are most popular or easiest to achieve. Also, sorting quantities by organizations in multilateral/multistakeholder data offers insights into each organization.

CHAPTER 5: HYPOTHESES

As a final step before exploring patterns in existing agreements and areas that are lacking, it's useful to lay out what we might reasonably expect to see in our results. These expectations are presented as a series of hypothesis. This study's focus is not restricted to these hypothesis, yet it is still important to compare the results against expected results.

H1 - Discussion and dialogue agreements are the most common.

Due to the fact that mere discussion is the lowest form of commitment, it's easy to understand why this would be expected to be the most popular form of agreement in both bilateral and multilateral/multistakeholder settings.

H2 - Different forums are preferred for different typologies of agreements.

It's commonly accepted knowledge that different governments look towards different forums to reach their cybersecurity objectives. This is seen in Russia's and China's repeated attempts to use the UN, but it is also shown inversely, like when the G8 was used to establish a network of contact points. This agreement was presumably because this network was acutely needed to keep incidents or misunderstandings from spiraling up the escalation ladder, a result no one wanted.

H3 - Activity limiting agreements are more common among disparate governments.

It seems that cyberspace favors authoritarian regimes that leverage it against their less nimble democratic peers. For this reason, it makes sense that activity limiting agreements take place mainly between dissimilar governments. The exception to this is when like-

minded governments create agreements in the spirit of norm building. However, it is expected that it is more common for governments to reach these agreements with the intent of addressing a practical problem instead of just doing so in a norm building way.

H4 - Countries with lower IPRs are less likely to pursue international cybersecurity agreements.

The idea here is that these agreements aren't a foreign policy priority for countries that have less Internet infrastructure. Countries with less infrastructure are less likely to seek agreements because the Internet isn't as important to them.

H5 - Incident response agreements are common across different governments just as cooperation between CERTs is.

Much of the language involved in international agreements frames incident response agreements as an easy way to find mutual ground. It's well known that the majority of threats online come from criminals and other more baseline threats that aren't state actors, hence doing things like increasing coordination between CERTs is a win-win for everyone involved. Due to their agreeableness, these can be expected to be fairly common.

H6 - Confidence building measures span widely across polity cores and geographies.

Traditional CBMs have a history of bringing together democratic and authoritarian governments to contribute towards a greater peace. Not only are CBMs expected to span a variety of different activities, but they will span geographies due to the distance between some of the world's leading competitive nations.

CHAPTER 6: IDENTIFYING PATTERNS IN EXISTING AGREEMENTS

While ICCD allows for an abundance of summary statistics and analyses, some in particular are deserving of attention. In this section I'll engage each hypothesis as a backboard for a broader discussion of the most important patterns and anomalies that ICCD has brought to light.

Quantity most definitely doesn't speak to any measure of quality, however it does signal which typologies are easiest to agree on and suggests the priorities of different governments. To begin, an easy pattern to look for is which kinds of agreements are most abundant. This brings us to our first hypothesis:

H1 - Discussion and dialogue agreements are the most common.

Status: Not False

Discussion and Dialogue is clearly the most sought out agreement in bilateral and multilateral/multistakeholder settings. In fact, 79% of all bilateral agreements make some formal

Number and Percentage Representation Out of Total of Each Typology (Bilateral)

Typologies	Discussion And Dialogue	Research	Confidence Building Measures	Incident Response	Crime	Capacity Building	Activity Limiting	Defense	Terrorism
Count	66	16	24	17	25	37	14	7	10
Percentage of Total	79%	19%	29%	20%	30%	44%	17%	8%	12%

Table 1 – Number and Percentage Representation Out of Total of Each Typology (Bilateral)

commitment to pursue further discussion, an abundance that soars above all other typologies. However that begs a more rudimentary question - are these typologies even statistically distinct from each other? An ANOVA test proves that the answer is a resounding no, with an F-Value of 1.527 and a Pr(>F)-Value of 0.144. Yet, while that might be a matter of concern in most experiments, in this context that may actually be a good thing. The fact that these typologies

cannot be determined to be fully distinct from one another speaks to just how often one agreement addresses multiple typologies, signaling that governments are more often than not open to pursuing multiple objectives simultaneously in a bilateral setting. But in what combinations?

Number of Instances When Agreements of Different Typologies Accompany Each Other (Bilateral)

	Discussion And Dialogue	Research	Confidence Building Measures	Incident Response	Crime	Capacity Building	Activity Limiting	Defense	Terrorism	Totals
Discussion and Dialogue	66	11	17	12	23	27	11	4	8	179
Research	11	16	7	8	6	12	4	2	2	68
Confidence Building Measures	17	7	24	8	11	13	4	5	2	91
Incident Response	12	8	8	17	6	14	3	3	2	73
Crime	23	6	11	6	25	14	8	2	10	105
Capacity Building	27	12	13	14	14	37	6	5	5	133
Activity Limiting	11	4	4	3	8	6	14	1	2	53
Defense	4	2	5	3	2	5	1	7	0	29
Terrorism	8	2	4	2	10	5	2	0	10	43
Totals	179	68	93	73	105	133	53	29	41	

Table 2 – Number of Instances When Agreements of Different Typologies Accompany Each Other (Bilateral)

Discussion and dialogue is apparently often bundled with other types of agreements and is the overlapping factor here. When that typology is removed from the ANOVA test, statistical significance between the categories improves noticeably with an F-Value of 0.849 and a Pr(>F)-Value of 0.547. However, excluding discussion and dialogue would be a mistake as its prevalence suggests there is some driving cause as to why it's common with other agreements. One possible reason might be that the typology is fundamentally different from the others. Whereas every other typology covers a subject matter, discussion and dialogue is an activity. This is not necessarily bad, and it's clearly a prominent enough item in agreements to warrant

being its own typology, but it does mean that in comparison to the other typologies there's an 'apples and oranges' scenario.

At first glance discussion and dialogue is most commonly observed along with capacity building, cybercrime, and confidence building measure bilateral agreements. However, it remains unclear if this is because it substantively has a reason to be present with these other typologies, or if this is only because these other three typologies are the other most common typologies. With the exception of the defense typology (at 14%), discussion and dialogue is consistently present with 16% to 22% of every bilateral typology. Most likely there is another underlying reason why discussion and dialogue is present in roughly one fifth of every typology.

To investigate this further I compared these bilateral findings to their multilateral/multistakeholder counterparts. Immediately a comparison of the ANOVA tests show that the results are very different. The multilateral/multistakholder typology ANOVA test is highly statistically distinct with an F-Value of 10.8 and a Pr(>F)-Value of 4.6e-15, meaning that the amount of overlap we had previously witnessed in bilateral instances is not seen in the multilateral/multistakeholder data at all. Although, interestingly we do see that there is still roughly one fifth of all typologies being present along with the discussion and dialogue typology (except activity limiting at 13%). Similarly, the multilateral/multistakeholder data also has cybercrime, capacity building, and confidence building measures as the next most abundant agreements and they're also most often paired with discussion and dialogue.

Number of Instances When Agreements of Different Typologies Accompany Each Other (Multi)

	Discussion And Dialogue	Research	Confidence Building Measures	Incident Response	Crime	Capacity Building	Activity Limiting	Defense	Terrorism	Totals
Discussion and Dialogue	227	47	71	52	105	86	4	12	56	660
Research	47	61	25	21	23	26	1	3	12	219
Confidence Building Measures	71	25	89	37	42	53	5	8	12	342
Incident Response	52	21	37	70	32	51	2	9	20	294
Crime	105	23	42	32	140	46	4	1	57	450
Capacity Building	86	26	53	51	46	108	4	12	27	413
Activity Limiting	4	1	5	2	4	4	7	0	5	32
Defense	12	3	8	9	1	12	0	13	1	59
Terrorism	56	12	34	20	57	27	5	1	76	288
Totals	660	219	364	294	450	413	32	59	266	

Table 3 – Number of Instances When Agreements of Different Typologies Accompany Each Other (Multi)

There's no clear answer to this one fifth phenomena. While this would need to demonstrated in further research to discover a causal mechanism, these results suggest that discussion and dialogue agreements are fruitful roughly one fifth of the time, with little regard as to the typologies or governments involved. The presence of a discussion and dialogue agreement is evidence that these bundled results happen in a forum where it's not a given that discussion on cybersecurity will happen on an ongoing basis without an agreement, so possibly these bundled results speak more about the forums they come out of than the efforts that create them. No matter the reasons, it seems one fifth of discussion and dialogue agreements result in another type of agreement as well. Of course no one should adopt this statistic as a hard rule, but it does illustrate an optimistic picture of diplomatic efforts. The consequences of such a finding are that if policy makers commit themselves to putting their heads together and hashing things out, there is a proven history of reaching further agreements, and this may be a useful tactic moving forward.

Also insightful is the fact that the multilateral/multistakeholder data in ICCD is highly statistically significant while the bilateral data isn't statistically significant at all. This demonstrates that there is a heavy overlap of typologies in the bilateral data while there is much less in the multilateral/multistakeholder data. Practically speaking, it would seem that bilateral approaches are more suitable for addressing multiple topics of agreement simultaneously, while agreements that involve more governments tend to be more precise and focus more on one component. This makes sense, but what typologies are addressed through which organizations? This leads to the next hypothesis:

H2 - Different forums are preferred for different typologies of agreements.

Status: Not False

As the previous ANOVA test hints at, different typologies are addressed individually in multilateral/multistakeholder settings, and they are often addressed through different forums. The quantity of international agreements should definitely be taken with a grain of salt as different organizations move at different paces and vary in how often they produce tangible agreements. So if one organization has one more agreement than another, that doesn't communicate anything useful. However, viewing the quantities more broadly and the quantities as rough generalizations, we can clearly identify a few trends.

Organizations With The Highest Number of Agreements of Each Typology (Multi)

Discussion And Dialogue	Research	Confidence Building Measures	Incident Response	Crime	Capacity Building	Activity Limiting	Defense	Terrorism
OAS 39	EU 17	EU 16	EU 21	OAS 39	EU 24	G7 3	NATO 10	OAS 13
UN 26	UN 13	OSCE 12	ITU 9	EU 23	NATO 14	UN 2	EU 3	UN 12
EU 24	ITU 9	G8/G7 9	ASEAN 8	G8/G7 14	ITU 13	G20 1	ASEAN 1	G7/G8 11
ASEAN 17	APEC 6	ASEAN 8	NATO 7	ASEAN 9	ASEAN 11	-	-	EU 10
ITU 15	BRICS 3	ITU 8	APEC 6	ITU 10	G8/G7 10	-	-	[TIE]

Table 4 – Organizations With The Highest Number of Agreements of Each Typology (multi) - *('TIE' used when multiple entries have same quantity)*

One pattern is when the United Nations is used. The UN has been successful in serving as a forum for discussion and dialogue and research pertaining to how different members view cybersecurity issues. This is reflected in the annual recurrence of agreements to discuss and look further into the matter that went on for nearly twenty years starting in 1998. Additionally, governments seem to feel comfortable denouncing terrorism through the UN, and agreeing on how to combat terrorists' use of communications technologies. This ability to agree is most likely rooted in how loosely defined the term terrorism is. While the Shanghai Cooperation Organization includes the idea of 'information terrorism', this is not present in other organizations' agreements. The two UN activity limiting agreements come from the UN GGE documents. These were difficult to negotiate and represent progress in themselves. However in comparison to other forums, the UN doesn't seem to be a preferred forum for activity limiting agreements.

The G8/G7 and G20 are the only other forums that have been used for multilateral/multistakeholder activity limiting agreements, which is a markedly different approach than going through the UN. These instances suggest that world leaders understand that their most important activity limiting commitments will be from other world leaders and competing governments. Possibly these leader felt that if they could solidify certain activity limiting agreements with other world leaders, they could build a coalition to enforce these norms in cyberspace.

By far, regional forums seem to dominate many of these multilateral/multistakeholder agreements. The EU and ASEAN both have a strong presence in most typologies, although ASEAN seems to shy away from some of the typologies that require a strong political commitment like Defense. Europe's solidarity through NATO is apparent as they seem to be the only organization willing to take on firm defense commitments. The Organization of American States seems to have a judicial focus as it is present in discussion and dialogue, cybercrime, and terrorism. A look at the Organization of American States documents reveals that the organization has found a niche for facilitating judicial cooperation in the Americas in the absence of any equivalent premier agreement like Europe's Budapest Convention[6], although some Western Hemisphere countries have signed that as well. These findings seem to align and confirm with how experts view these organizations being utilized. What still remains unexplored is how governments' efforts are manifesting in bilateral agreements.

[6] Better known as the European Commission's 'Convention on Cybercrime'

H3 - Activity limiting agreements are more common among disparate governments.

Status: Not False

Activity limiting agreements are sort of the 'odd one out' within this field of study, especially the bilateral agreements. While many of the other agreement typologies involve governments finding common ground and trying to build on that for further progress, activity limiting agreements aren't always as good hearted. Some of them are anticipatory and out of good will, but many of them tend to be reactive after a buildup of tensions. For example, many of the bilateral activity limiting agreements involving the Chinese government could more appropriately be described as a having been stop-gap measures for near diplomatic crises. For the purposes of this study those instances would still be considered a priority to the Chinese government though, if at the very least the priority was calming down infuriated peer governments. This typology would benefit from a more nuanced approach that aims to keep this anticipatory versus reactive context in mind, but considering it is already a slimly populated typology, doing so in this study would only hinder the resulting findings. Plus, activity limiting doesn't always take place in such a hostile environment. There are instances when governments have agreed not to attack CERTs without any looming diplomatic crisis. These circumstances in no way disqualify the typology from this research, but they do offer an important context.

Distribution of Average Polity Scores of Governments
. Participating In Agreements Per Typology (Bilateral)

Typology	Minimum	First Quartile	Median	Mean	Third Quartile	Max
Discussion and Dialogue	0.5	3.125	9	7.13	10	10
Research	3	8.5	9	8.611	10	10
CBMs	0.5	1.5	9	6.58	10	10
Incident Response	3	9	9.5	8.9	10	10
Crime	0.5	1.5	8.25	5.725	9.625	10
Capacity Building	0.5	4	9.5	7.5	10	10
Activity Limiting	-1.5	1.25	1.5	3	4.375	9
Defense	3	9	10	8.7	10	10
Terrorism	0.5	1.25	1.5	3.125	3.375	9

Table 5 – Distribution of Average Polity Scores of Governments Participating In Agreements Per Typology (Bilateral)

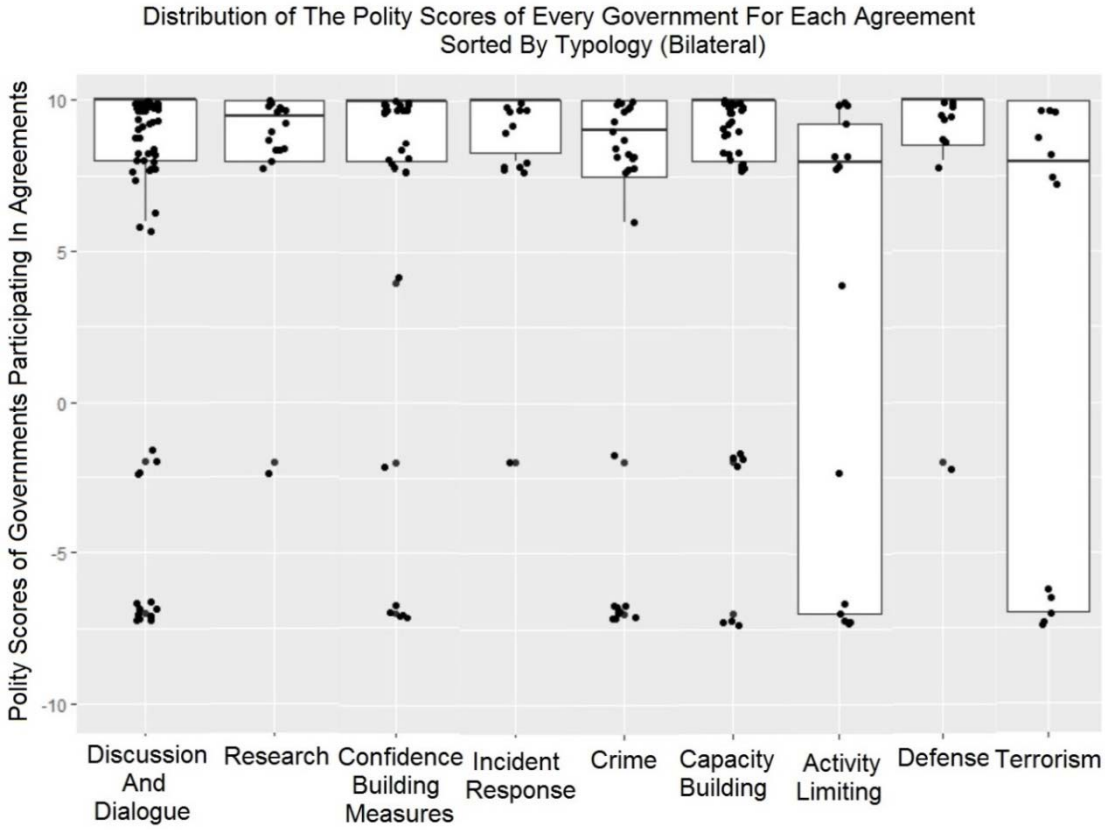


Figure 1 – Distribution of The Polity Scores of Every Government For Each Agreements Sorted By Typology (Bilateral)

The distribution of polity scores within activity limiting sticks out from other typologies. Activity limiting and terrorism skew much more heavily towards authoritarian participants than most other typologies. Along with these low polity means, cybercrime also has a comparatively low mean, demonstrating that these are higher priorities for authoritarian governments. All of these categories focus on the rights and legal powers of a given government and reinforce the common viewpoint that lower polity countries tend to worry about domestic instability. Equally revealing are where the highest polity means exist, which speak to what more democratic governments pursue.

Compared to authoritarian priorities, high polity governments are more involved with bilateral agreements over incident response and defending themselves. The mean average polity of agreements in the defense typology is the second highest of all the typologies. It also has one of the highest minimum values in its range out of the entirety of ICCD, meaning that the low point of its polity range is higher.

Looking beyond the average polities, viewing the distribution of high polity scores before they are averaged with their respective low polity scores reveals a more nuanced finding. The averages suggest incident response and defending themselves are the highest priorities of liberal democracies, but the averaged numbers are affected by the outlying authoritarian governments. The un-averaged scores show that democracies are also heavily engaged in confidence building measures, capacity building, and discussion and dialogue. It's good to see that these typologies have a heavy enough engagement with authoritarian governments to skew their average results, especially when it comes to discussion and dialogue and confidence building measures.

The difference between the average results and the un-averaged polity scores makes it clear that even though these typologies might not be liberal democracies' high foreign policy priorities, it is still more so a priority for them than their authoritarian counterparts. The discussion and dialogue typology has the most authoritarian participants out of every typology, yet because of the heavy representation of liberal democracies, its statistics are still heavily skewed upwards. The fact that discussion and dialogue is an activity and not a subject matter most likely explains why it is so easily dominated by democratic participation who might value dialogue and openness more highly, but the same can't be said for capacity building or confidence building measures (CMBs).

Most likely the skew with the confidence building measures typology is based in definitional challenges. Where this study might classify information sharing between two friendly governments as a CBM, the context of their relationship might mean that such an agreement possibly leans more towards a defense or [non existent in this study] intelligence agreement. Quantitative findings from the CBM typology seem to have suffered from the open definition used in the process of constructing ICCD. Future research may look to more appropriately sort that category.

The upwards skew of the capacity building typology has no such excuse. If anything, a more open definition that might include development efforts would shift it downwards, and this is not the case. Even including an above average number of negative polity scores, the typology still skews dramatically towards the top. Capacity building is not only a priority of liberal democracies – it happens most often exclusively between liberal democracies, just like the incident response typology.

From a practical standpoint these varied priorities between democracies and authoritarian governments prove very tough for policy makers. Many liberal democracies are convinced of the efficacy of multistakeholder institutions, but it would appear that not only do opponents of this idea disagree with this assertion, but it actually runs against the grain of their highest foreign policy priorities. Additionally, liberal democracies seem focused on forging agreements among themselves, which runs counter to how governments usually approach transnational issues.

H4 - Countries with lower IPRs are less likely to pursue international cybersecurity agreements.

Status: False

While 'lower' is a subjective term without a defined threshold, this statement still rings untrue. Every bilateral entry in ICCD has two IPR values, one from the higher country, and one from the llower, after a quick look of the distribution of 'high' and 'low' IPR pairs, the majority of IPRs volved in these agreements falls below 80%. Rising powers like China and India are active in seeking out these agreements, therefore to claim that lower IPR countries don't pursue these agreements would be excluding some of the world's most important players in cyberspace. Interestingly though, there is a gap roughly between the 50% to 60% IPR range. Possibly there is some sort of threshold here. I already explored the differences between authoritarian and democratic governments, and this IPR gap could be related.

It’s not surprising that lower IPR countries participate along with higher IPR countries, especially since we already know that an IPR doesn’t necessarily speak to a government’s offensive capabilities.

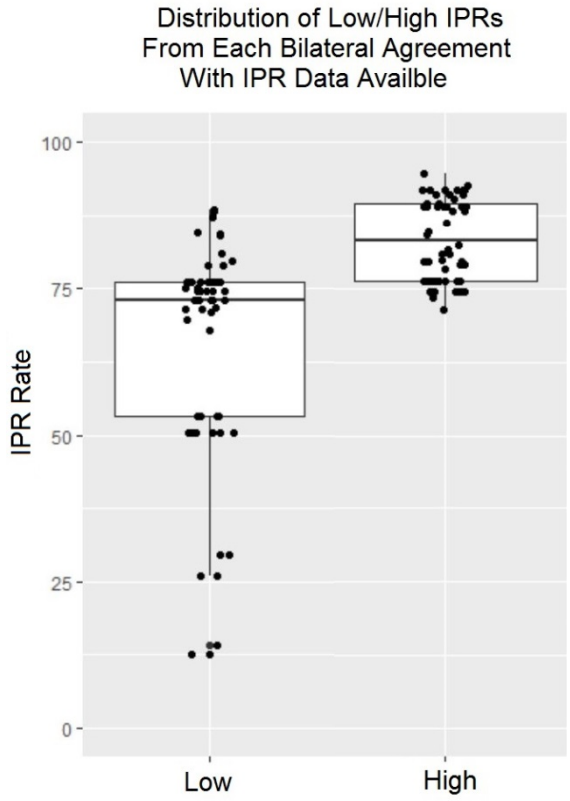


Figure 2 – Distribution of Low/High IPRs From Each Bilateral Agreements With IPR Data Available

Distribution of Internet Penetration Rates of Countries Participating In Agreements Per Typology (Bilateral)

Typology	Minimum	First Quartile	Median	Mean	Third Quartile	Max
Discussion and Dialogue	44.28	64.69	77.78	73.41	82.08	90.12
Research	52.51	52.86	77.1	70.25	80.34	85.48
CBMs	52.86	64.69	77.78	73.42	81.93	90.12
Incident Response	52.21	74.39	77.98	74.14	82.21	90.12
Crime	46.04	62.43	64.69	69.62	81.05	90.12
Capacity Building	52.51	67.11	80.43	75.82	82.89	90.12
Activity Limiting	52.86	61.86	63.24	65.53	71.15	82.1
Defense	76.3	78.19	79.59	79.75	81.36	83.28
Terrorism	62.43	64.12	64.69	68.49	69.04	82.21

Table 6 – Distribution of Internet Penetration Rates of Countries Participating In Agreements Per Typology (Bilateral)

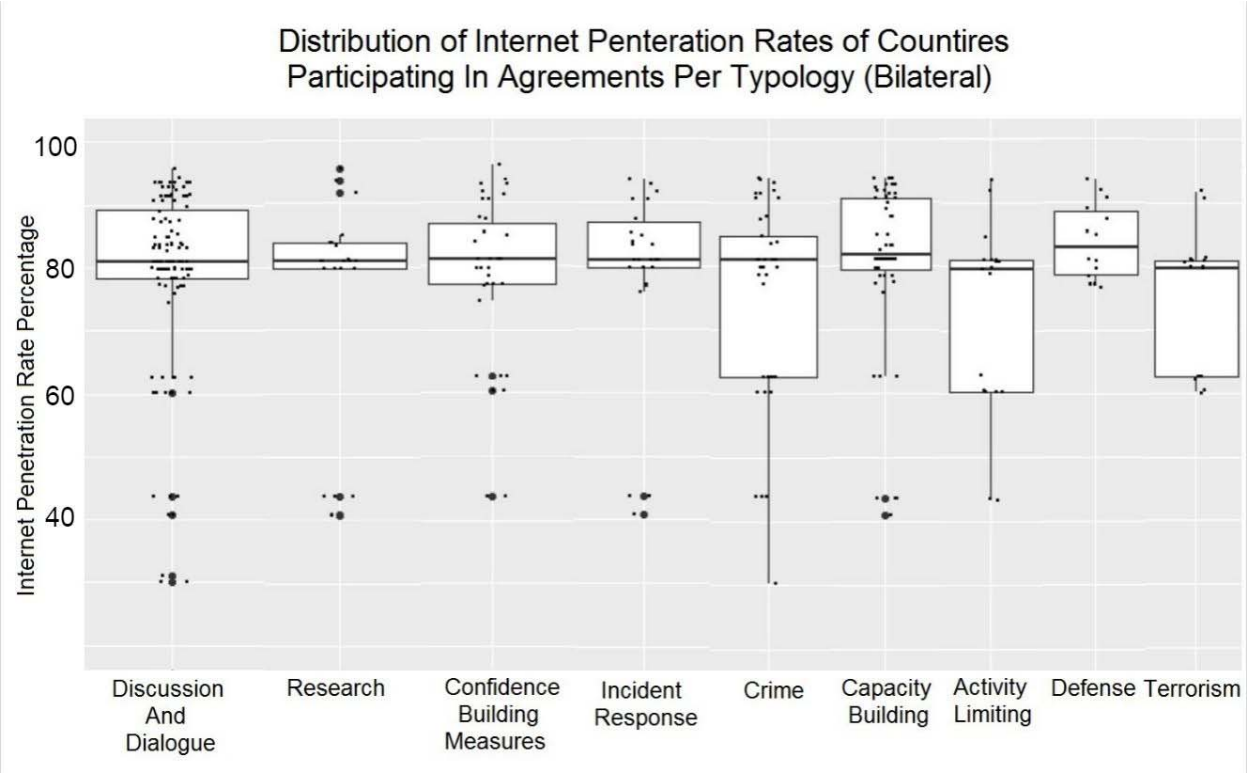


Figure 3 – Distribution of Internet Penetration Rates of Countries Participating In Agreements Per Typology (Bilateral)

Yet there is much more here to be discovered beyond simple trends with the IPRs. By laying out the IPRs, high tech exports, and polity scores of each typology, the data becomes much more revealing. ICCD already revealed the difference in priorities between democratic and authoritarian governments. Relating those insights with these findings offers further understanding. It turns out that the terrorism, activity limiting, and cybercrime typologies have the three lowest IPRs as well. So while IPR is no predictor of government participation in international cybersecurity agreements, lower IPRs do generally tend to occur among more authoritarian governments.

Distribution of High Technology Export Percentages of Countries Participating In Agreements Per Typology (Bilateral)

Typology	Minimum	First Quartile	Median	Mean	Third Quartile	Max
Discussion and Dialogue	10.27	15.24	17.59	19.39	22.42	43.7
Research	13.55	15.57	18.8	20.85	21.84	43.7
CBMs	13.55	16.23	17.89	19.79	22.37	43.7
Incident Response	13.55	16.95	17.89	20.81	22.92	43.7
Crime	12.02	15.5	17.46	19.37	22.47	43.7
Capacity Building	13.5	15.5	17.78	20.86	22.47	43.7
Activity Limiting	13.55	17.89	22.27	22.13	22.92	43.7
Defense	16.95	17.21	18.43	22.49	21.95	43.7
Terrorism	17.37	21.17	22.47	21.29	22.47	22.92

Table 7 – Distribution of High Technology Export Percentages of Countries Participating In Agreements Per Typology (Bilateral)

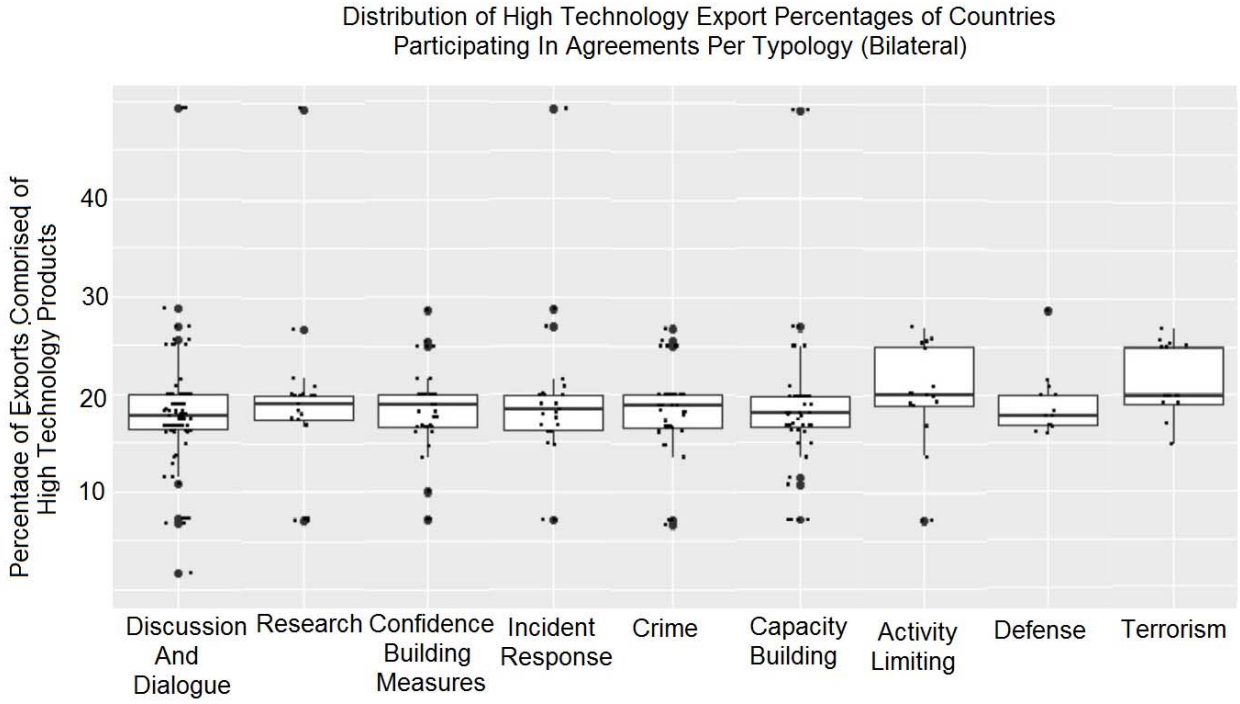


Figure 4 – Distribution of High Technology Export Percentages of Countries Participating In Agreements Per Typology (Bilateral)

Sorting agreement typologies by the high technology exports of the governments who participated in them outlines two different groups. The terrorism and activity limiting typologies have very high means, while the cybercrime typology has the lowest. Considering this in the context of the 50% to 60% IPR gap of the bilateral agreements (Figure 1.1), there may be a tangible threshold distinguishing these two authoritarian groups from one another. This possibility that IPRs and polity scores are related should be an area of focus for future research. These findings suggest that there are two categories of authoritarian governments with distinct foreign policy priorities in cyberspace, those that are highly technically capable and those that are not.

The correlation of activity limiting agreements with high technology export statistics suggests that high technology exports possibly correlate with whichever metrics governments use to identify possible threats. It may be possible for democratic countries to proactively spot authoritarian governments that will become aggressive in cyberspace by using a process that at least in some way involves tracking their high technology exports. Then they may be able to proactively enter activity limiting agreements before these impending aggressive governments grow into their full potential. Inversely, authoritarian governments that have issues with aggressive democracies will be seen as a greater threat and have more diplomatic leverage once they gain further technical expertise and their economy matures to show this.

If researchers were able to prove any sort of causation between IPRs, polity scores, and high tech exports, democracies may gain additional development and foreign policy tools to achieve democracy and human rights promotion. This finding is also useful in that it is now clear that authoritarian governments with relatively lower high technology exports are most likely interested in pursuing agreements over cybercrime. Democracies could offer these less capable authoritarian governments basic cybercrime cooperation in exchange for achieving some of their own foreign policy objectives.

H5 and H6 are discussed in the following section.

Recapping Patterns

- Discussion and dialogue agreements are not only the most common, they tend to accompany agreements in additional typologies roughly one fifth of the time. This should not be considered a hard rule, but does suggest a reason to stay optimistic about diplomatic efforts.
- Bilateral agreements are much better suited for addressing multiple topics to agree on simultaneously, while agreements involving more than two governments are usually narrowly focused.
- The United Nations is good for facilitating dialogue, researching various viewpoints, and counter terrorism activities, although terrorism in cyberspace is loosely defined.
- Regional agreements are very prominent forums for pursuing international cybersecurity agreements.
- Authoritarian regimes focus on projecting or managing state power and maintaining control through the terrorism, cybercrime, and activity limiting typologies.
- Democracies maintain a defensive focus through the capacity building, defense, and incident response typologies.
- Authoritarian governments are divided into two groups, one with high technical capability, and one without. Those with high technical capabilities participate in the activity limiting and terrorism typology more while those without prioritize cybercrime agreements.

CHAPTER 7: IDENTIFYING AREAS OF COOPERATION THAT ARE LACKING

Just as important as identifying trends is reading between the lines and understanding what's not taking place. Forging international agreements over cybersecurity is daunting work, yet there is a lot of room for improvement that has gone unnoticed. In order to move past our current state of occasional flare ups and crises, we need to identify and follow a more proactive approach by finding more common ground and forging more agreements.

Incident Response and Capacity Building Agreements

An easy place for governments to start doing this is within the incident response typology.

H5 - Incident response agreements are common across different governments just as cooperation between CERTs is.

Status: False

Not only are agreements over incident response and capacity building among those less commonly pursued, these typologies lack any significant agreements that move the ball forward. Bilateral incident response agreements are most often pursued between democratic governments, similar to defense agreements, and capacity building agreements are nearly this exclusive as well. Additionally, the majority of these multilateral/multistakeholder agreements that do exist tend to be regional.

There are several possible explanations for the current lack of incident response and capacity building agreements. The lack of incident response agreements might be that cooperation between CERTs already fills this void to an extent, but that argument doesn't hold up very well. CERTs do have a crucial role to play in national and international cybersecurity, but their mandates only go so far. Whereas CERTs can exchange information such as how to recognize different new strains of malware on a machine and coordinate incident responses, they don't have the authority to place bigger requests at an international level. CERT's mandates fall short when a situation goes beyond purely technical topics. If there were ever a ruinous operation against an international impactful target like a major international bank, concerns such as monetary costs of damage as well as digital records disparities (to name a few) would be outside of the mandate of CERTs, but also too burdensome for existing mutual legal assistance agreements to address amply.

Governments are most likely aware of this. Just the fact that incident response agreements beyond CERT cooperation exist is enough to demonstrate that governments clearly see some value in them beyond what CERTs can provide. Plus, agreements and activities usually have to be repeated over and over to create a norm, so multiple efforts would be expected for this typology as well. Another possibility may be that governments are simply approaching their close allies in establishing international agreements over cybersecurity before branching out further. This is more likely, but it still doesn't answer why other typologies have readily reached across polity ranges. Cybercrime should be a more politically contentious topic than incident response and capacity building, yet the cybercrime typology seems to have seen much more progress.

While there's room for multiple interpretations of why the incident response and capacity building typologies have such slim polity statistics, what seems to fit the given results best is that governments simply view cybersecurity in terms of relative advantages instead of absolute advantages. Governments viewing cybersecurity in terms of relative advantages explains why they would be willing to coordinate over judicial matters, but not over more technical leaning cybersecurity topics like cooperating over better protecting critical infrastructure and setting up agreements for assistance in case of an emergency. Governments may feel more comfortable knowing that other governments are generally more vulnerable. This is really unfortunate, but it's also an opportunity for future cooperation. The majority of cybersecurity threats are non-affiliated criminals. Governments would not be sacrificing their place within the competitive realm of cybersecurity by establishing agreements that commit emergency assistance and help coordinate preparedness efforts. Likewise, governments are quick to call cybersecurity a transnational issue. If they truly believe this, they should be eager to establish agreements cooperating over securing critical infrastructure that criminals can easily target and agreements over ensuring a basic level of competency for practitioners..

Probably, governments aren't necessarily opposed to more encompassing incident response and capacity building agreements, but they are preoccupied with other topics they prioritize higher. There are nearly as many bilateral activity limiting agreements as there are incident response agreements, and considering that those should be significantly harder to agree upon, that shouldn't be the case. It implies that governments are acutely worried about other governments, as opposed to more common and likely criminal threats.

At the moment, the incident response clause with the most clout out of any relevant agreement comes from the UN GGE 2015 Report, it reads:

> *"States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty."*

While this is a start, two sentences is nowhere near as comprehensive an agreement as could most likely be attained. Similarly encompassing agreements over capacity building are even less established, with most capacity building happening in forums and conferences that free governments of any official commitments or benchmarks. Compare this to another typology, cybercrime. The Budapest Convention on cybercrime goes on for over twenty pages specifically listing how to facilitate cooperation. There's no good reason why an equivalently prolific capacity building or incident response agreement can't be established. This is even more so important with the incident response typology as its very nature implies a major disruption or emergency has taken place, which is the exact moment when a predefined plan is most valuable.

Confidence Building Measure Agreements

Although the quantitative results for the confidence building measures (CBM) typology suffered from a broad definition, this typology is concerning from a qualitative standpoint. Most commonly we see forms of information sharing and establishing points of contact for resolving issues. These agreements should be encouraged, but they are not enough. The debate among policy makers now seems to be how to best make forward progress.

The predominant method right now involves voluntary norms and defining acceptable behavior. This diverges from historical confidence building strategies. Traditional agreements like the Anti-Ballistic Missile Treaty, Prevention of Incidents In and Over High Seas Agreement, and the Limited Nuclear Test Ban all made sure to formally commit parties to specific regulations through a treaty. The closest that cybersecurity CBMs get to extracting official assurances out of any given party are the 2015 UN GGE sections on voluntary norms. These are often ignored. Attempts at laying out additional CBMs, such as the OSCE's 16 Cyber-CBMs (OSCE, 2016), are useful thought exercises, but they lack one key component: assigned responsibilities. Everyone is in favor of supporting norms and CBMs in cyberspace, that is until they're the ones being restricted by them.

H6 - Confidence building measures span widely across polity scores and geographies.

Status: False

The fact that multilateral/multistakeholder CBMs are predominantly established regionally is telling. Considering that this study may be mixing true CBMs with different cooperative activities between already trusting allies suggests that governments are branching out to their closest peers to set up these cooperative activities and that in time they'll expand to do these activities more globally. Despite this study's inconclusive CBM quantitative results, through reading these typologies it's clear that policy makers should be expanding their CBM playbooks. Expanding and pushing for new voluntary norms is useful in that it gets competing governments to agree on certain topics they didn't agree on or consider before. However, policy makers need to focus their efforts on committing governments to participate in ongoing CBM activities that they must sign onto and take some sort of responsibility for. Even if these activities are mirror

images of regional agreements, that still gets governments used to participating in global CBMs, which would be useful. These activities could be as mechanical and simple as sharing information and best practices on a recurring basis through an agreed upon forum. The point is that there is repetition, and that a specific government officially agrees to participate via some sort of treaty or formalized document for which it is responsible.

Standards Setting

Much like setting fuel emission standards for vehicles to be sold in a certain country, governments can agree to force products to be certified as reasonably secure before being eligible to be sold on the market. Or at the very least they can offer a sort of 'cyber security nutrition facts' system to help non-technically inclined consumers understand what generalized security features their product includes (Healey, 2018). These types of agreements were nearly non-existent in ICCD and are not widely adopted at the moment. One reason for this is that agreements pertaining to market and ecommerce standards tend to fall outside of the scope of ICCD because they are more often pursued as privacy and consumer rights topics than the government oriented cybersecurity topics included in ICCD.

The European Commission has already put out a proposal for this type of agreement, although it is yet to be formalized. (European Commission, 2017) No one else has made progress in this area. One possible situation would be for governments to make these product standards agreements open so that others could join. These agreements could also encompass the company selling the product, ensuring they have the proper incident response and product life-cycle processes in place to track a product's security status as it ages and to effectively handle security

breaches. Understandably, agreements like this might brush up against concerns of market competitiveness, although there are a number of ways this could be managed. The agreements could only apply to products and companies that hit certain benchmarks like units sold or revenues. Governments could even establish a process for empowering already existing private companies to audit products and companies and distribute certifications appropriately as to avoid undue costs on their own behalf.

Realistically these agreements seem to be far off. Plus, simply saying it would be helpful to set standards oversimplifies the whole topic of cybersecurity. What constitutes a secure Cisco switch [networking device] is a completely different set of standards than what constitutes a secure banking application.

Defining 'Cyber Terrorism'

Appending the phrase 'cyber' onto old topics is a great way to reinvigorate their importance and shift the discussion to dealing with how the topic changes due to new technologies, but doing this also muddies the term's definition. Unfortunately this has happened a lot. 'Terrorism' in particular has been affected.

Does vandalizing a website so that it shows pro-Islamic State content as opposed to its intended content qualify as 'cyber terrorism' (Barrett, 2017)? If so, it doesn't seem to be very effective. Yes, it frustrated law enforcement authorities, but no one seemed intimidated nor did anyone's stance on the Islamic State change. Website defacements are commonplace online, so the

Figure 1.5 – Mr. Bean Website Defacement

conclusion here is that just like traditional definitions of terrorism, there's a nuanced point to be made about the intended effect. This is where the real disagreements become more serious.

For example, consider the time someone replaced all of the pictures of the Spanish Prime Minister with photos of Mr. Bean on the EU's website (BBC, 2010). That's clearly not terrorism in Europe, but what about in other countries? The Shanghai Cooperation Organization uses the following definition for 'information terrorism':

> "This threat emanates from terrorism organizations and individuals involved in terrorist activities acting unlawfully though information resources against/regarding them. It 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 information resources" (Shanghai Cooperation Organization, 2009).

Figure 1.6 – Notoriously Banned Picture of Putin

Does fiddling with an important government website count as controlling or blocking a mass media channel? Assuming government officials have a healthy sense of humor, probably not. Does this stunt pose "negative impacts on information resources"? Yes. The point here is that some concepts have been so loosely defined that they essentially become formal ways for governments to claim the right to decide on a case-by-case basis. Also, the threshold here isn't clear at all. Imagine that this same stunt had taken place in Russia, but instead of using pictures of Mr. Bean, the perpetrator used the notoriously banned online picture displaying Putin as a [presumably] homosexual clown. All of the sudden, this comical stunt could very easily be deemed terrorism, at least while Putin or his sympathizers are still in power.

On top of the fact that 'cyber terrorism' online is often fluidly defined by content, there remains additional areas of confusion. Most governments seem to agree that terrorist forums and recruitment online constitute cyber terrorism, but this doesn't translate into the physical world very well. If five violent extremists hang out in their living room discussing their religious ideologies in the physical world, while those individuals are regarded as dangerous, that in itself isn't defined as terrorism; when they do this online it is. Whereas policy-makers seem to want to differentiate regular crime from terrorism based on a question of why someone is doing

something, in most cases online the only thing differentiating cyber crime from terrorism boils down to a question of who is doing it.

Recapping Lacking Areas

- There is a lack of significant incident response agreements. This is most likely due to government's viewing cybersecurity as a relative advantage and not an absolute advantage topic.
- There is a lack of confidence building measures between competing governments that require official commitments, even if those are at the most basic levels.
- Agreements specifying mutually agreed cybersecurity standards for products is a novel area of cooperation and has potential, but is not currently adopted by anyone.
- 'Cyber terrorism' is defined by who is involved, and different countries view these organizations and individuals very differently.

CHAPTER 8: KEY TAKEAWAYS FOR POLICY MAKERS

The last two sections present insightful discoveries about international cooperation concerning cybersecurity. ICCD allows many findings, and many of them remain to be explored. Among this research, the main takeaways are listed below.

Governments view their cybersecurity posture in terms of relative gains, even though it is in their best interest to view this topic in terms of absolute gains.

Incident response and capacity building agreements at the bilateral level are predominantly pursued between democracies and similarly democratic governments. The most compelling reason for this is that governments view cybersecurity as a competitive activity. Evidence suggests that they feel more comfortable knowing their possible competitors are vulnerable. Further, multilateral/multistakeholder incident response and capacity building agreements are dominated by regional organizations, supporting this point further. This insight is contradictory to the language many governments currently use in many of their agreements about how cybersecurity is a transnational issue. Yet, actions speak louder than words, and clearly governments have been very selective in choosing who to pursue such activities with.

Authoritarian governments are involved with agreements over controlling or projecting government authority while democratic governments focus on resilience and defense.

Agreements over terrorism, activity limiting, and cybercrime all have a much stronger representation from authoritarian regimes than other agreements. These categories focus on the

rights and legal powers of governments and reinforce the common viewpoint that authoritarian countries tend to worry about domestic instability and challenges to their authority. In contrast, democracies are more involved with bilateral agreements over incident response, capacity building, and defending themselves. Not only are there often definitional challenges in cybersecurity cooperation, but also differing governments seem to have different foreign policy priorities that they are pursuing. From a practical standpoint this proves very difficult for policy makers. Many liberal democracies are convinced of the efficacy of multistakeholder institutions, but it would appear that not only do opponents of this idea disagree with this assertion, but it actually runs against the grain of their highest foreign policy priorities.

Authoritarian governments are divided in their efforts based on their economies' technical capabilities.

Authoritarian governments are subdivided among their economies' technical capabilities. Counter-terrorism and activity limiting agreements correlate with countries that have much larger higher tech exports. Inversely, cybercrime agreements trend with authoritarian governments whose countries have low amounts of high tech exports. This could be explained in several ways. It could be that a distinction between 'terrorism' as a separate topic from 'crime' only occurs at a certain point in a country's developmental maturity. It could also be that separately prioritizing terrorism isn't a priority for governments until they feel they have the technical capability to do so effectively.

Discussion and dialogue agreements accompany additional agreements roughly one fifth of the time.

Nearly every type of agreement is coupled with an agreement over discussion and dialogue roughly one fifth of the time. This preliminarily suggests that discussion and dialogue agreements have yielded, or at least contributed to, agreements over different topics about a fifth of the time. Future research should look into a possible causal relationship that may offer policy makers a direct understanding of when their discussions are most fruitful and yield results.

CHAPTER 9: CONCLUSION

Viewing international cybersecurity challenges through a 'cooperative approach', as opposed to a conflict-centric lens may offer valuable insights. ICCD has proved a powerful tool for policy research. It offers researchers a central location for all of the world's publicly available agreements over cybersecurity up until 2018. Using ICCD I was able to identify multiple patterns in the vast quantity of current agreements while also pointing out some areas that are lacking.

Through this method I've documented how authoritarian regimes work to project state power in cyberspace and how democracies maintain a defense and resilience oriented approach in cyberspace. Yet this study has only scratched the surface of the insights ICCD offers. Future work can focus on applying a more nuanced approach to troublesome typologies like confidence building measures and activity limiting. Also, future research can look to find relationships between the additional variables, the agreements within ICCD, and the dates they were established. ICCD will save researchers significant amounts of time and allow them to hone in on their primary research focuses within the topic of international cybersecurity cooperation. Additionally, ICCD has quantified one of the most tangible measures of international cooperation over cybersecurity, this means that it may now be possible to compare conflict and cooperation data as it pertains to cybersecurity specifically.

Hopefully this research, and ICCD in its current form, are a start and not an end. As more governments gain offensive capabilities and the political stakes in cyberspace increase, working towards agreements on these topics is needed now more than ever. The time for policy makers to

prioritize these challenges and improve their cooperation is now, as it will only get harder as time goes on and the foreign policy surrounding cybersecurity becomes even more complicated.

REFERENCES

Agreement among the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security. (2009). Retrieved from https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

Unofficial Translation from Russian

Anderson, C., & Sadjadpour, K. (2018). Carnegie Endowment for International Peace. Retrieved from http://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

Arab Convention on Combating Information Technology Offences. (2010). League of Arab States General Secretariat. Retrieved from http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

Ashbaugh, L. (2018, March 27). Cracking Down on Chinese Investment Might Lead to an Uptick in Cyber Espionage. Retrieved from https://www.cfr.org/blog/cracking-down-chinese-investment-might-lead-uptick-cyber-espionage

Assessing Russian Activities and Intentions in Recent US Elections. (2017). Director of National Intelligence. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Auchard, E. (2018, January 18). Lebanese security agency turns smartphone into selfie spycam:... Retrieved April 12, 2018, from https://www.reuters.com/article/us-lebanon-cyber/lebanon-spy-agency-targets-smartphone-users-worldwide-researchers-say-idUSKBN1F726S

Australia-India Cyber Policy Dialogue (Joint Statement. (2017, July 13). Retrieved from http://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-india-cyber-policy-dialogue.aspx

Axelrod, R. (1979). The Rational Timing of Surprise. World Politics, 31(02), 228-246.

Axelrod, Robert (1984), The Evolution of Cooperation, Basic Books

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. Proceedings of the National Academy of Sciences of the United States of America, 111(4), 1298-1303. Retrieved September 19, 2017, from http://www.jstor.org.prxy4.ursus.maine.edu/stable/pdf/23769039.pdf?refreqid=excelsior:db3617bdcfce58d4ff99a618576bbe80

Barlow, J. P. (1996, February 08). A Deceleration Of The Independence of Cyberspace. Retrieved from https://www.eff.org/cyberspace-independence

Barrett, D. (2017, June 25). Websites of Ohio governor, Maryland county hacked, defaced with pro-ISIS message. Retrieved from https://www.washingtonpost.com/world/national-security/websites-of-ohio-governor-maryland-county-hacked-defaced-with-pro-isis-message/2017/06/25/934035b8-59e7-11e7-a9f6-7c3296387341_story.html?utm_term=.f026228cde35

Mr Bean replaces Spanish PM on EU presidency site. (2010, January 04). Retrieved from http://news.bbc.co.uk/2/hi/8440554.stm

Bilge L, Dumitras T (2012) Before we knew it: An empirical study of zero-day attacks in the real world. Proceedings of the 2012 ACM Conference on Computer and Communications Security (Association for Computing Machinery, New York), pp 833-844.

Borghard, E., & Lonergan, S. (2018, January 16). Why Are There No Cyber Arms Control Agreements? Retrieved from https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements

Chabrow, E. (2014, April 2). NSA-RSA Ties Raise New Concerns. Retrieved from https://www.bankinfosecurity.com/nsa-rsa-ties-raise-end-user-concerns-a-6703

Brantly, A. F. (2016). The decision to attack: military and intelligence cyber decision-making. Athens (Ga.): The University of Georgia Press.

Challenges in Cybersecurity. (2011). Institute for Peace Research and Security Policy at the University of Hamburg. Retrieved from https://d-nb.info/1024526593/34.

Chen, Y., & Yang, D. (2018). The Impact of Media Censorship: Evidence from a Field Experiment in China. Stanford University. Retrieved from https://stanford.edu/~dyang1/pdfs/1984bravenewworld_draft.pdf

Chesney, R. (2017, March 08). Legislative Hackback: Notes on the Active Cyber Defense Certainty Act discussion draft. Retrieved from https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft

Choucri, N., Madnick, S., & Ferwerda, J. (2013, October). Institutional Foundations for Cyber Security: Current Responses and New Challenges. Retrieved from https://ic3.mit.edu/wp-content/uploads/2013-16.pdf

Cyber Norms Index, Carnegie Endowment for International Peace, 2018, http://carnegieendowment.org/publications/interactive/cybernorms

Clarke, R. A. (2011). Cyber War. HarperCollins.

Convention on Cybercrime. (2001). European Treaty Series, 185. European Council, from https:// www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use of Information and Communication Technologies. (2016). Organization for Security and Cooperation in Europe. Retrieved from https://www.osce.org/pc/227281?download=true.

DeNardis, L. (Director). (2014, September 10). The Global War for Internet Governance [Video file]. Retrieved from https://www.youtube.com/watch?v=_NRV-GY1v1Q&t=1878s

Definitions and terminology relating to building confidence and security in the use of information and communication technologies. (2010). International Telecommunications Union. Retrieved from https://ccdcoe.org/sites/default/files/documents/ITU-101022-DefinitionTermsPP-10.pdf.

Dutch intelligence agency spied on Russian hacking group: Media. (2018, January 25). Retrieved from https://www.reuters.com/article/us-netherlands-russia-cybercrime/dutch-intelligence-agency-spied-on-russian-hacking-group-media-idUSKBN1FE34W

Farivar, C. (2018, March 30). Finally extradited from Europe, suspected LinkedIn hacker faces US charges. Retrieved from https://arstechnica.com/tech-policy/2018/03/months-after-being- arrested-in-europe-suspected-linkedin-hacker-faces-us-charges/

Finnemore, M. (2017, November 30). Cybersecurity and the Concept of Norms. Retrieved from http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870

Giles, K. (n.d.). Russia's Public Stance on Cyberspace Issues. 4th International Conference on Cyber Conflict. Retrieved November 6, 2017, from https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformation Warfare.pdf.

Goldstein, J., & Freeman, J. (n.d.). Three-Way Street. Chicago, IL: University of Chicago Press.

Groll, E. (2017, December 21). Cyberattack Targets Safety System at Saudi Aramco. Retrieved from http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). United Nations General Assembly. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Healey, J. (2013). A fierce domain: conflict in cyberspace, 1986 to 2012. Vienna, VA: Cyber Conflict Studies Association.

Healey, J. (2017). The Five Futures of Cyber Conflict and Cooperation. Georgetown Journal of International Affairs. Retrieved October 26, 2017

Healey, J. (2018). Building a Defensible Cyberspace.Columbia School of Policy and International Affairs. Retrieved from https://sipa.columbia.edu/sites/default/files/3668_SIPA Defensible Cyberspace-WEB.PDF.

Helsinki Final Act. (1975). Conference On Security And Co--Operation In Europe. Retrieved from https://www.osce.org/helsinki-final-act.

Hoffman, W., & Levite, A. (2017). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace? Carnegie Endowment For International Peace. Retrieved from http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236

INCYDER. (n.d.). NATO Cooperative Cyber Defence Centre of Excellence, Retrieved from https:// ccdcoe.org/incyder.html

ITU Regional Forum on Cybersecurity in the Era of Emerging Technologies, Cairo – Egypt. (2017, November 29). Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2017/CYB-ET/CYB-ET.aspx

Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. (2018, January 12). Retrieved from https://ccdcoe.org/japan-join-nato-cooperative-cyber-defence-centre-excellence-tallinn.html

Maheux, B. (2014). Assessing the Intentions and Timing of Malware. Technology Innovation Management Review. Retrieved October 2, 2017, from http://timreview.ca/sites/default/files/article_PDF/Maheux_TIMReview_November2014.pdf

Marczak, B., Geoffrey, G., McKune, S., Scott-Railton, J., & Deibert, R. (2018). Champing At The Cyberbit. The Citizens Lab. Retrieved from https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.

Mr Bean replaces Spanish PM on EU presidency site. (2010, January 04). Retrieved from http://news.bbc.co.uk/2/hi/8440554.stm

NATO CCDCOE INCYDER Dataset.

Nellis, S., & Cadell, C. (2018, February 26). Apple moves to store iCloud keys in China, raising human rights fears. Retrieved from https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060

Reno, J. (1997, December 10). Statement By Attorney General Janet Reno On The Meeting Of Justice And Interior Ministers Of The Eight. Retrieved from https://tspace.library.utoronto.ca/bitstream/1807/654/3/518cr.html

Russian firm provides new internet connection to North Korea. (2017, November 2). Retrieved from https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2

Rõigas, H. (2015, February 10). An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New? Retrieved from https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

Schmitt, M. N., & Vihul, L. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press.

Orji, U. J. (2015). Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? 7th International Conference on Cyber Conflict. Retrieved November 6, 2017, from http://ieeexplore.ieee.org.prxy4.ursus.maine.edu/stamp/stamp.jsp? arnumber=7158472

Tenth Meeting Of Ministers Of Justice Or Other Ministers Or Attorneys General Of The Americas REMJA X. (2015). Organization of American States, 8. Retrieved from http://www.oas.org/en/sla/dlc/remja/pdf/remja_x_rec_conc_en.pdf
Footnote Page 8

Romo, V. (2018, March 30). As Atlanta Seeks To Restore Services, Ransomware Attacks Are On The Rise. Retrieved from https://www.npr.org/sections/thetwo-way/2018/03/30/597987182/as-atlanta-seeks-to-restore-services-ransomware-attacks-are-on-the-rise

Russian firm provides new internet connection to North Korea. (2017, November 2). Retrieved from https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. (2010). International Telecommunications Union. Retrieved from https://ccdcoe.org/sites/default/files/documents/ITU-101022-StrenghtConfidencePP-10.pdf.

Suleimanov, S., & Marshall, P. (2018, February 8). Users have become the main target. Retrieved from https://meduza.io/en/feature/2018/02/09/users-have-become-the-main-target

Strickling, L & Hill , J (2017) Multi-stakeholder internet governance: successes and opportunities, Journal of Cyber Policy, 2:3, 296-317, DOI: 10.1080/23738871.2017.1404619

Schmitt, M. N., & Vihul, L. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press.

Sukumar, A. M. (2017, July 04). The UN GGE Failed. Is International Law in Cyberspace Doomed As Well? Retrieved from https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well

The EU cybersecurity certification framework. (2017). European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

United Nations, General Assembly resolution 58/32, Developments in the field of information and telecommunications in the context of international security A/RES/58/32 (23 October 2003), available from https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/d39687f7586f53f485256dc1005e12f5?OpenDocument&ExpandSection=5#_Section5

Valeriano, B. (2015). Cyber war versus cyber realities: cyber conflict in the international system. Oxford: Oxford University Press.

Verdelho, P. (2008, March 12). The Effectiveness of international co-operation against cybercrime: examples of good practice [Scholarly project]. In Council of Europe. Retrieved October 28, 2017, from https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF

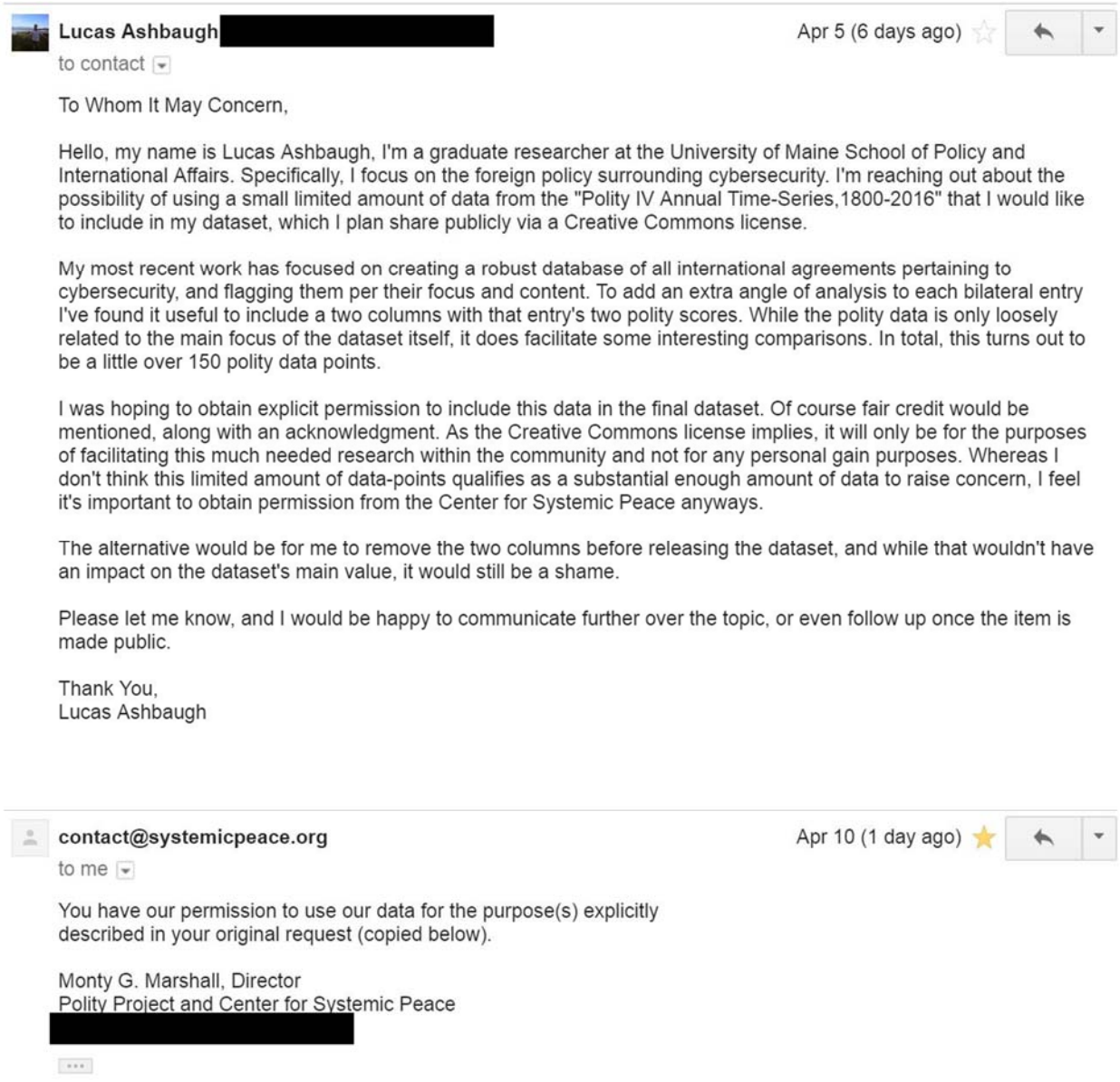
UN Broadband Commission sets global broadband targets to bring online the world's 3.8 billion not connected to the Internet. (2018, January 23). Retrieved from https://www.itu.int/en/mediacentre/Pages/2018-PR01.aspx

Wales Summit Declaration. (2014). North Atlantic Treat Organization. Retrieved from https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

Warsaw Summit Communiqué. (2016). North Atlantic Treaty Organization. Retrieved from https:// www.nato.int/cps/en/natohq/official_texts_133169.htm.

APPENDIX A – COPYRIGHT PERMISSION

Explicit written permission was received from the Center for Systemic Peace to use their polity data, the correspondence is below:



Lucas Ashbaugh [redacted] Apr 5 (6 days ago)

to contact

To Whom It May Concern,

Hello, my name is Lucas Ashbaugh, I'm a graduate researcher at the University of Maine School of Policy and International Affairs. Specifically, I focus on the foreign policy surrounding cybersecurity. I'm reaching out about the possibility of using a small limited amount of data from the "Polity IV Annual Time-Series,1800-2016" that I would like to include in my dataset, which I plan share publicly via a Creative Commons license.

My most recent work has focused on creating a robust database of all international agreements pertaining to cybersecurity, and flagging them per their focus and content. To add an extra angle of analysis to each bilateral entry I've found it useful to include a two columns with that entry's two polity scores. While the polity data is only loosely related to the main focus of the dataset itself, it does facilitate some interesting comparisons. In total, this turns out to be a little over 150 polity data points.

I was hoping to obtain explicit permission to include this data in the final dataset. Of course fair credit would be mentioned, along with an acknowledgment. As the Creative Commons license implies, it will only be for the purposes of facilitating this much needed research within the community and not for any personal gain purposes. Whereas I don't think this limited amount of data-points qualifies as a substantial enough amount of data to raise concern, I feel it's important to obtain permission from the Center for Systemic Peace anyways.

The alternative would be for me to remove the two columns before releasing the dataset, and while that wouldn't have an impact on the dataset's main value, it would still be a shame.

Please let me know, and I would be happy to communicate further over the topic, or even follow up once the item is made public.

Thank You,
Lucas Ashbaugh

contact@systemicpeace.org Apr 10 (1 day ago)

to me

You have our permission to use our data for the purpose(s) explicitly described in your original request (copied below).

Monty G. Marshall, Director
Polity Project and Center for Systemic Peace
[redacted]

BIOGRAPHY OF AUTHOR

Lucas Ashbaugh is, with this thesis, obtaining his Master of Arts degree in Global Policy, with a focus in International Security and Foreign Policy at the University of Maine's School of Policy and International Affairs (SPIA), where he specifically studies cybersecurity and emerging technology challenges in the context of international security. He has both professional technical and policy experience, having worked as: a Digital and Cyberspace Policy Intern with the Council on Foreign Relations, a Policy Analyst Intern for Axiom Technologies (ISP), a Management Information Systems Group Intern doing security audits for BerryDunn CPAs and Consultants, and a Computer Technician for the University of Maine.

He previously graduated from South Portland High School in June, 2011 and the University of Maine Business School in May, 2016 with a B.S. degree in Business Management and a concentration in Management Information Systems.

He is a candidate for the Master of Art degree in Global Policy with a concentration in International Security and U.S. Foreign Policy from The University of Maine in May 2018.