COMP 116: Computer Security

Nika Korchok Wakulich

Sunday, December 11, 2016

Mentor: Michael Glennon

Interdisciplinary Approaches to International Cybersecurity Policy Making

How Collaboration Between Tech and Diplomacy Can Foster a Safer Cyber Space

Abstract

International law has been, for hundreds of years, based on historical precedence, informed by an acknowledgement of previous transgressions and steadfastly committed to ensuring a collective safety based on an agreed-upon set of regulations. The state of modern international cybersecurity, therefore, fails in all of these realms. While the Internet was established as ARPANET by the U.S. Department of Defense in the 1960s as "a pioneering network for sharing digital resources among geographically separated computers" ("ARPANET and the Origins of the Internet," DARPA), this early medium was also introduced as a backup communication network in the event that a physical war destroyed telephone lines. The internet's origins are derived from a Cold-War-induced state of pre-emptive defense. Now, in an era where cyber attacks themselves could cripple telephone lines, power grids, water supplies or untold systems of national infrastructure, the need for a new means of defense has presented itself. This essay attempts to dismantle preconceived notions of existing international cybersecurity policy by addressing three key areas — the attribution problem, the question of territory in cyberspace, and jurisprudence for alleged cyber crimes.

Introduction

On a domestic front, the United States is seemingly more primed than ever before to fight the onslaught of cyber crime that will evidently spring forth in the years to come. The incoming Trump administration was recently advised to train 100,000 cybersecurity specialists by the year 2020 in order to face growing national cybersecurity problems (Paglieri, "Panel to Trump: Train 100,000 hackers"). President Obama's Executive Order 13636, issued in 2013, created the National Institute of Science and Technology's Cybersecurity Framework to maintain an efficient cyber environment that promotes safety and liberty (Executive Office of the President, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity").

Yet, cyber attacks continue to take place on a daily basis. International cooperation has seen lukewarm, if any, success. Take for example, the treaty that resulted from the Council of Europe's 2001 Budapest Convention on Cybercrime. In "Cybersecurity Treaties: A Skeptical View" by Jack Goldsmith, the efficacy of the treaty is all but dismantled, "The Cybercrime Convention is widely viewed as unsuccessful. It achieved "consensus" on computer crimes only by adopting vague definitions that are subject to different interpretations by different states. Even with vague definitions, many nations conditioned their consent on declarations and reservations (the United States had more than a half dozen) that further diluted the scope of covered crimes, making the treaty's obligations even less uniform and less demanding. While the mutual assistance mechanisms in the treaty improve on what came before, they do not work well" (Goldsmith, 3).There is an unprecedented necessity for clear, unilateral cooperation in the fight against cyber crime on the international scale.

This paper presents a brief examination of three problems that the international community is facing in the creation of effective law and policy on cyber crime and cyber warfare: the attribution of attacks, the definition of territory in cyberspace, and the jurisprudence of cyber crimes. Each section focuses on obstacles that are faced when addressing each issue and presents interdisciplinary approaches to creative problem solving, to better assemble coherence in law.

First, to set forth a precedence to create an effective dialogue between technologists and policymakers so that the attribution problem can be mitigated. The combination of computer

software and algorithms, as well as the social engineering aspects of policy, can combine to create a formidable Swiss Army Knife to properly attribute cyber attacks.

Second, to define cyber space as a new domain — similar to the classifications of air, space and naval combat — would allow for a starting point of reference in future policy. Historical precedence will do little to serve what is so new.

Third, to address issues with current jurisprudence with respect to international treaties defining cyber warfare and weaponry. This concludes by citing examples of effective governing bodies that foster interdisciplinary dialogue between experts in a range of fields, which allow for a cohesive approach to the interdisciplinary issue of cyber security.

The final part of this paper consists of a twofold proposition to combat cyber attacks — personal civilian responsibility based upon an education of current cybersecurity principles, and the suggestion for a new branch of combat to be defined on an international scale. In the same way that laws exist for defining territory in air, sea and land, new treaties must be established to either establish international domain over the internet — an unlikely scenario based upon the sheer size and volume of both the internet and the dark net — or to establish cyberspace as a nationless state with territorial law henceforth to be established.

To the Community

If there was even a question as to the importance of cybersecurity, then the battle may already be lost. This year alone has seen two of the biggest DDOS attacks in recent years — the DDOS attack on Dyn servers for websites such as Github, Spotify and Twitter, among others, (Woolf, “DDoS attack that disrupted internet was largest of its kind in history, experts say”) left many without access to these sites for days, and also revealed vulnerabilities in the system architecture; a recent attack on Deutsche Telekom servers in Germany left roughly 900,000 people without their broadband service while the company combatted an attack on its hardware[8]. But beyond the domestic scope, there are new international threats — reports about Russian hackers manipulating the United States presidential election eventually led to the allegation’s confirmation by the Central Intelligence Agency and other national security organizations. As it is described in an article by David E. Sanger and Scott Shane for the New

York Times, “American intelligence agencies have concluded with “high confidence” that Russia acted covertly in the latter stages of the presidential campaign to harm Hillary Clinton’s chances and promote Donald J. Trump, according to senior administration officials” (Sanger and Shane “Russian Hackers Acted to Aid Trump in Election, U.S. Says”).

Worms like Stuxnet and entire web infrastructures like that which comprised the Silk Road — a malicious program to slow down nuclear centrifuges and an anonymous online illegal drug-trafficking market, respectively — are both familiar and foreign. While avid newsreaders may recognize the buzzwords associated with those two major cases, there are few, if any, citizens in the general population who fully comprehend the intricacies or the magnitude of these two examples of “cyber warfare.”

The goal of this paper is to serve as an educational tool, to heed the 1998 warnings of L0pht and take ownership for those powerful tools which we must use everyday. Cyberspace is frighteningly and magically a very new realm, with great possibility for destruction and community, it is our responsibility to take personal accountability, engage in education and understand the technological tools we use every day. Read closely. Pay attention. Start taking ownership for the safety of your community by taking ownership of your own safety in cyberspace.

Part I: Addressing the Attribution Problem

Attribution remains at the crux of modern international cybersecurity policymaking. Nation-states represent a duality of interests in pursuing attribution: the more that is known about malicious software, systems or procedures, the more a nation’s cybersecurity capabilities are revealed; conversely, knowing nothing about the capabilities of attackers renders everyone powerless and without a clear direction for pursuing legal retribution for cyber crimes.

In “The Road Ahead: Gaps, Leaks and Drips” Tufts Fletcher professor Michael Glennon states, “Attribution permits the target to assign responsibility. It provides the rules’ ultimate enforcement mechanism—the ever-present threat of retaliation and punishment. It therefore establishes compliance incentives… [it] enables legal recourse against transgressors, not only in

the International Criminal Court and other international tribunals, but also in the domestic courts of nations that comply with their international obligation to investigate and prosecute war crimes" (Glennon 380). Without attribution, there can be no legal proceedings for cyber warfare, and without legal proceedings, there can be no establishment of a new precedence for the increasingly militarized world of cyber space. However attribution relies on being able to identify, as Glennon states, the computer, the attacker and the government or organization behind that attacker (Glennon 382).

The problem of attribution is vast, with many subsections of information too expansive to cover in this singular paper. This section will instead set the stage with an example of two major roadblocks to attribution: the multiplicity of identities present in the use of Botnets and Proxies. A comparison model is then established between two studies which present novel methods of attribution — the first using Natural Language Processing to analyse source code, the second using SVM-based classifiers to analyze binary code for stylized author signatures. These two studies present a brief insight into the complexity of attribution of an attack, revealing both possibility and hesitation at relying on software to identify attackers.

Part A: Multiplying Identities with Botnets and Proxies

A botnet is an army of centrally controlled computers that have been hijacked by an attacker in order to perform commands as a small army. The term botnet comes from the words "robot" and "network;" an attacker assembles a botnet by infecting computers with malware via a myriad of hacking and social engineering techniques; these computers then act as unwittingly as zombies for the host node ("What is a botnet attack?" Kaspersky Lab). Once a botnet is assembled, the machines can perform amplified attacks, likely the most infamous of which is a DDoS attack or a distributed denial of service attack. A DDoS attack will flood a server with requests, either leading to a server crashing (as in the October attack on the Dyn servers of Github) or can lead to the botnet's host gaining root access to a specified system to collect data. A botnet's link to the attribution problem lies in its very nature of attack by amplification: due to the high volume of IP addresses that will be linked to a botnet, the difficulty of tracking down a

singular attacker is increased by the number of zombie computers it is using. In some cases, the size of a botnet can be millions of computers or more.

A honeypot is a means of attributing the source of a botnet attack by acting as a decoy system, set up to appear as though it has valuable data, access rights and assets that would be valuable to an attacker; however the honeypot exists in a state of isolation where it can be monitored and generally used as a larger part of an intrusion detection system (IDS) (Rouse, "Honeypot"). According to Margaret Rouse of SearchSecurity, "Data placed in a honeypot with unique identifying properties can also help analysts track stolen data and identify connections between different participants in an attack" (Rouse, "Honeypot"). A honeypot, however, remains useful so long as two things happen: it is used and it is undetected by the botnet controller. In a research paper by Pang Wing et al, Wing describes the fallibility of honeypots, "Attackers could detect honeypots in their botnets by checking whether compromised machines in a botnet can successfully send out unmodified malicious traffic" (Wang, 1) after which a removed honeypot from a botnet would be useless. If a honeypot is never chosen by an attacker, its efficacy would also be rendered void. With this in mind, a botnet could still remain untraceable to a source and the attribution of an attack could be nearly impossible.

With the sheer volume of DDoS attacks in the past year alone, it is clear that botnets will not decrease in popularity with hackers who wish to conduct massive attacks. In the case of attribution of attacks, the amplification allowed by a botnet exponentially increases the difficulty of pinpointing a singular attacker. Honeypots on their own do not always determine a botnet controller. Therefore, a singular system can never be put in place as the standard for attribution for a botnet-conducted attack. Other avenues must be explored.

A proxy system presents a similar challenge. As described by W. Earl Boebert in "A Survey of Challenges in Attribution", a proxy acts as an intermediary in the transmission of packets, allowing a packet's IP address to be transformed from the original sender to that of the proxy(Boebert 45). Furthermore, Boebart explains the difficulty of attribution due to proxies on the international stage, "…forensic examination of hostile packets may reveal a source IP address that indicates only the major institution from which the packet came. More detailed attribution requires cooperation of the institution, which may either be impossible (owing to to

absence of detailed logs) or not forthcoming. The latter is often the case when the packet in question has crossed national boundaries"(Boebert 45). This further begs the question of how one is defining nationhood when in reference to cyberspace. To attribute a packet to an institution or a government requires cooperation, the definition of which currently remains vague on the international stage.

Part B: Natural Language Processing in Attribution Software

The abstract of "Identifying Authorship by Byte-Level N-Grams: The Source Code Author Profile (SCAP) Method " states, "Source code author identification deals with identifying the most likely author of a computer program, given a set of predefined author candidates" (Frantzeskou et al, 1).

The SCAP (Source Code Attribution Profile) method proposes a new avenue for attribution through the use of n-grams. An n-gram is a sequence that "can be defined on a byte, character or word level"(Frantzeskou et al, 4). By dividing source code into a series of n-grams, Franszetkou et al were able to analyze for a series of quantifiable metrics that determine the identity of an author, including but not limited to "indentation, placement of comments, placement of braces, character preferences.. the degree to which code and comments match, and whether identifiers used are meaningful" (Frantzeskou et al, 3). The human degree in code is essentially what defines this as a natural language (human language) problem, which explains why natural language processing was used as a framework for the experiment. To capitalize on individuality and human error, attribution can be attained. Frantzeskou et al used the n-gram divisions to create specific profiles for their authors and then applied machine learning algorithms to their data in order for specific authors to be matched to programs in the database. Franztekou et al even ran experiments that accounted for the discrepancies between user-friendly and malicious software, "Since the source code used in malicious cyberattacks typically do not contain comments, the second experiment reported here examines the performance of SCAP on comment-free code and on a different programming language" (Frantzeskou et al, 10).

The results of the experiments were largely successful, often finding success rates of 100% if the size of the author profile and the size of n-grams used were both relatively large — above 2000 for the author profile and above 8 for the size of the n-gram. In layman's terms, this means that a larger amount of data, a more complete profile and more input to match with, allowed for a stronger guarantee at 100% accuracy. Frantzeskou also addressed another problem with the results, the malleability of the n-gram size could introduce a bias into the results of forensics examiners. "…the SCAP method is currently semi-automated and therefore open to subjective manipulations… The SCAP (or any n-gram) method can only be protected from unscrupulous and dishonest examiners by continued validation research and full automation which conceals these choices from examiners. …When this validation work is completed, a fully-automated system which cannot be manipulated will be available for forensic use. Meanwhile, digital forensic investigators who are independent of case advocacy and whose record of integrity supports their independence should certainly consider using the SCAP method given the current state of research."(Frantzeskou et al, 11-12) Frantzeskou et al suggest that the software be used by digital forensic investigators as a secondary support for investigative research. Since the software is not currently a fully-automated system, the risk is still prevalent that the results are malleable and that full accuracy cannot be currently attained.

Part C: Matching Stylistic Tendencies in Program Binaries to Known, Unknown Authors

In "Who Wrote This Code? Identifying the Authors of Program Binaries," Nathan Rosenblum, Xiaojin Zhu, and Barton P. Miller of the University of Wisconsin, Madison, present two SVM-based classifiers that identify authorship by matching binary code to known authors based on two main stylistic markers: idioms and graphlets.

The methodology of their experimentation allowed the researches to match given binary code to those stylistic tendencies of a "known set of programmers of interest" (Rosenblum et al, 178) by creating two types of classifiers. First, Rosenblum et al. focused on first identifying an author based on programmer style in binary code, based on two feature templates that correspond to both low-level instruction level sequences and program details (Rosenblum et al., 175-176).

Second, they created a classifier that identified "clusters" of similar styles of code, which accurately map unknown authors to known authors with a similar style of code-writing.

This methodology allows for an opening of possibilities — not only an identification of an author from a pool of suspect candidates, but the potential to map new and henceforth anonymous authors to those known authors with similar styles. In their conclusion, Rosenblum et al. describe their correctness as being able to "identify the correct author out of a set of 20 candidates with 77% accuracy, and rank the correct author among the top five 94% of the time." (Rosenblum et al, 187).

However, the authors of the study also acknowledge important limitations to their findings, "In author classification, we assume that there exists a known set of programmers of interest, and that training data are available in the form of samples of programs written by each programmer" (Rosenblum et al). While a certain author's programming style may be detected in a program's binary, the key here remains that in order to conduct this identification, the author must already be present in a database system, where their code can be analyzed and matched. If an unknown author is presented, the closest that can be found is a near match in a cluster of similar authors.

Summary

As a note across the board, between the two contrasting systems briefly presented here, there is no guaranteed methodology for 100% accuracy in cyberattack attribution via computational models. As it stands currently, there is no valid means of confirming or denying the author of a malicious program or cyberattack. This issue is compounded when one further examines the data at hand: in the case of an attack, source code is not always readily available, nor is the author of a program present in a database containing known authors of cyberattacks.

For the n-gram method presented by Frantzeskou et al, the success of attribution relies on the retrieval of the source code of an attack. In the case of cyberattacks, if the code for a program is recovered, there is the possibility of encrypted files and also the risk of fragmentation of data.

Identifying the perpetrator in a cyber attack is not as simple as calling in key witnesses, or matching a physical fingerprint. The digital fingerprint is the most elusive of markers as it can

be transformed and morphed at the will of an adept owner.

For classification of an author by stylistic tendencies in binary via the SVM-classifier method, it is imperative that a database of known authors is already present in order to have a comparative model for verification of a contested attribution. If this is a matter of international policy however, this dataset could expand to millions of authors. The accessibility of databases of authors on an international basis then becomes a matter of which nation-states are willing and likely to divulge the information of perhaps their best and brightest hackers. The likelihood of having a complete or reliable dataset diminishes exponentially when presenting known authors of programs becomes a matter of state-secrecy.

Moving Forward

Attribution via source code or binary code is possible in a vacuum — when authors and their styles are known, when the entirety of source code or binary code can be taken and analyzed. In the case of cyber warfare, attackers can conduct attacks from remote locations, using different IP and MAC addresses to conceal identity, encrypting or fragmenting data as means of concealment. These studies do not also address the possibility of programs written by multiple authors. How is it possible to attribute an attack if the attacker is in fact a military-commissioned team of special operatives, each with their own code-writing style? In the case of multiple attackers, a clustering method can be more effective at grouping together similar authors — and if a team of special operatives is in fact conducting an attack, it is more likely that their code will be similar simply due to the collaborative nature of building a singular program. However, there is no guarantee in the attribution of said attack.

It is imperative that this field of computer science continue to expand upon the research that currently exists. Investing more money in research and development could be a start to finding faster and more sophisticated algorithms that more accurately map and identify both known and unknown authors.

A key issue with attribution is also the disconnect between current scientific research in finding improved attribution methods and the policymakers who must understand those attribution methods to create new laws. It is imperative that the content and findings of this

research be more widely distributed amongst the necessary parties in international cybersecurity policy making. The more that policymakers are aware of the limitations to attribution of attacks, the better that Security Councils can assess the risks and rewards of plans moving forward. Attribution is not impossible, but as it stands, it is nearly so. In order to ameliorate that in the future, international councils must be advised to invest in new research, to better understand how to use tools currently in place and to search for new means of identifying attacks.

Conversely, a twofold-approach to attribution could be put in place. Using national intelligence, diplomatic expertise of conflicts and a grasp of current economic or political turmoils between nation-states, diplomats could help technologists narrow their scope of verification. Foreign policy could help point the verification algorithms in the right direction. Then attribution will be a matter of simply crunching numbers for a small sample size instead of the entire world. An interdisciplinary approach to cybersecurity is the only route with potential to solve the attribution problem.

Part 2: The territory of cyberspace

In "A Declaration of Cyberspace," John Perry Barlow asserts the domain of cyberspace as a new frontier, "Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions" [5]. Although this hacktivist mindset of cyberspace sovereignty could be viewed as either utopian or anarchist, it highlights the transitory and ephemeral nature of a new non-physical space inhabited by millions of computer-users worldwide.

This section outlines a plan for a cooperative effort between technologists and diplomats to forge a new common sovereignty for cyberspace. Drawings from examples of other international treaties — including the U.N. Convention on the Law of the Sea and the Antarctic Treaty System, this section presents evidence of the necessity of a formal definition of cyber space as a stateless commons. Such a measure was inspired by the work of Scott Shackleford in his essay "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law". Shackleford's proposal of delimiting cyberspace as a commons is outlined as follows, "…

cyberspace is not a customary arena over which states may exercise such control. Some have argued that cyberspace is an international commons akin to other commons territories. These traditional areas of the international commons include the deep seabed under the U.N. Convention on the Law of the Sea ("UNCLOS"), the Antarctic Treaty System ("ATS"), and outer space under the 1967 U.N. Outer Space Treaty… In the international commons, all of humanity is the sovereign under the CHM [Common Heritage of Mankind] principle. To the extent that cyberspace is a commons, it is one facing unique challenges and thus requiring exceptional regulatory solutions."

Part A: Naval Space, Sea Space and Cyber Space

While dictating physical limitations between countries is done through the use of borders, the classification of border limitations in two other domains — air and sea — is created by the United Nations Convention on the Law of the Sea (UNCLOS). Part II, Section II, Article 1 of the UNCLOS dictates,

> "1. The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.
>
> 2. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.
>
> 3. The sovereignty over the territorial sea is exercised subject to this Convention and to other rules of international law." (United Nations Convention on the Law of the Sea).

Article 3 also determines the breadth of the Sea belonging to a state as "up to a limit not exceeding 12 nautical mile" (United Nations Convention on the Law of the Sea). These articles clarify the subdivision of a space that is not as physically separate as, for example, a mountain range to separate two countries. In creating a new provision, this 1982 treaty set a precedent for territory and, in doing so, eased the way for jurisprudence to define what constituted an attack by air or by sea between two nation states when a border was crossed.

The same necessity exists for cyber space, with a major caveat: while the division of territory in sea and airspace is significantly more ambiguous than that of land divisions, it still relies on the entity of a physical body. How then, can cyberspace be classified? In terms of the fiber optic cables that connect data centers to buildings? Are all IP addresses within a country's physical borders part of that countries "territory" and what happens when a computer crosses national borders? And how does one define nationality of data that travels across the world in a matter of seconds?

When considering these questions, the inclusion of technological experts becomes evident. In order to determine naval territorial divisions, one speaks to admirals and captains to better understand the nuances of defining a different space. In order to create boundaries in cyber space, those with the greatest expertise — IT, Cyber Security and other technological experts — are necessary to provide insight and a technical backbone to the foundation of such a treaty.

While looking to past treaties of territorial agreement, it is important to not let historical precedence blind policy-makers to the evolving needs of the present. UNCLOS can serve as a model for a new frontier insofar as the treaty allowed for a new definition of territory. The very interconnectedness of the Internet and the data that is shared between users, prevents a direct transfer in application. A new domain must be established. The establishment of this new domain relies on the communication between tech experts and diplomats.

Part B: Sovereignty of Commons

The Antarctic Treaty provides perhaps the best model for provisional documentation of territory for cyberspace. As states in Article IV, Part 2, "No acts or activities taking place while the present Treaty is in force shall constitute a basis for asserting, supporting or denying a claim to territorial sovereignty in Antarctica or create any rights of sovereignty in Antarctica. No new claim, or enlargement of an existing claim, to territorial sovereignty in Antarctica shall be asserted while the present Treaty is in force" (The Antarctic Treaty). The Antarctic Treaty further prohibits nuclear explosions in the space of the Antarctic, and the establishment of military bases and weapons testing. As a shared space classified under the principle of the Common Heritage of Mankind, the Antarctic Treaty sets up a territorial domain that is shared for peaceful purposes

with the goal of scientific research and advancement of human knowledge as the primary goals of its collective international membership.

While this may be an idealistic, utopian view of cyber space, it can provide the necessary framework of open sharing and collaboration that must take place in order to begin setting precedences for combatting cyber crime. The idea of establishing cyber space as a nationless commons is further outlined in the paper by Shackleford, “Nations have every right to protect their sovereign interests through the effects principle. Yet, given that many regard cyberspace as a commons territory, it would be prudent to regulate the commons as in other CHM areas through an international organization, similar to the United Nations Commission on the Limits of the Continental Shelf ("CLCS") under UNCLOS. This body could regulate cyber security similar to the ATS and outer space, but through greater private sector partnerships. Such a theoretical system is reminiscent of John Herz's notion of "neoterritorality," whereby sovereign states recognize their common interests, that is, cyber security, through extensive cooperation, while also mutually respecting one another's independence and the increasingly important role of non state actors” (Shackleford 215).

Moving Forward

The Antarctic Treaty sets forth a precedence for mutual respect and a shared collective goal of both peace and the pursuit of knowledge. In this vein, the UN could move to classify cyber space as a commons domain with parallel limitations to cyber weapons and support of continued research in the domain of cybersecurity.

While historical precedence of air, land and sea treaties do not entirely translate to the interconnectedness of cyberspace, the idea of a commons set forth in the Antarctic Treaty does allow for both collective safety and progress.

It remains to be seen as to the efficacy of setting up a domain in such a manner. Ensuring that a separate nonpartisan organization within the UN take charge of maintaining the safety and freedom of cyberspace through such a charter would ease that transition and ensure that standards for conduct were met. Measures for creating such a governing body are outlined in Part III.

Part III: Current Jurisprudence in Cyberspace

The current lack of coherent jurisprudence dictating proceedings for cyber crimes and cyber warfare puts at risk both nation states and individual citizens. Without clear policy for the definitions of "cyber weapons," "cyber crimes" or "cyber warfare," individuals are subject to loose interpretations of pre-existing laws that govern the misuse of physical force. Since cyber warfare is not reliant on a traversal through physical space by humans, but rather a transfer of malicious packets via any number of different protocols (IMAP, TCP, HTTP, etc.) on networks, then the simple blanket classification of cyber warfare under the same terms is dangerous.

Take for example, the US' current holding and charging of several alleged "cyber criminals." On August 25, 2016, the U.S. Department of Justice detailed in a press release, the conviction of Roman Valerevich Seleznev, aka Track2, 32, a man from Vladivostok, Russia was convicted by a federal jury of "…38 counts related to his scheme to hack into point-of-sale computers to steal and sell credit card numbers to the criminal underworld," (Department of Justice, "Russian Cyber-Criminal Convicted of 38 Counts Related to Hacking Businesses and Stealing More Than Two Million Credit Card Numbers").

Seleznev was taken into custody in the Maldives, and his personal computer was confiscated; after investigation by federal prosecutors, the device was determined to contain " more than 1.7 million stolen credit card numbers, some of which were stolen from businesses in Western Washington. The laptop also contained additional evidence linking Seleznev to the servers, email accounts and financial transactions involved in the scheme" (Department of Justice, "Russian Cyber-Criminal").

Yet the apprehension and trial of Seleznev raises important questions about international cybercrime jurisprudence: At what point does a computer become evidence and how does one determine the legality of Article 4 of the Constitution relating to Search and Seizure with respect to thousands, or tens of thousands of files? Who is responsible for apprehending a cybercriminal when their crimes cross national boundary lines? How can one determine national boundary lines when discussing cyberspace?

If the International Court of Justice is to remain a functional legal body for the prosecution of cyber crime, then it must adapt to new needs.

Part A: The Fragmentation of Efficacy in Diplomatic Bodies

The fragmentary nature of current international cybersecurity groups and policies is best described by Tim Maurer in "Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security." Maurer identifies the major groups at the UN which comprise different factions of cybersecurity policymaking: ITU (International Telecommunication Union), UNODC (United Nations Office on Drugs and Crime), UNIDIR(United Nations Institute for Disarmament Research), UNICRI(United Nations Interregional Crime and Justice Research Institute) and Unicef. Maurer states,

> Throughout their negotiations, member states have been using UN organizations as organizational platforms for their competing agendas. That is also why the UN's activities regarding cyber-security are highly fragmented…The ITU divides the UN organizations' work on cyber-security as follows:
>
> (1) Combating cybercrime: ITU and UNODC;
>
> (2) Building capacity: ITU, UNIDIR, and UNICRI;
>
> (3) Child Online Protection: ITU, Unicef, UNICRI, UNODC.55

While it is undoubtedly the case that cybersecurity is not an isolated field and that it affects persons across all domains, it remains to be seen as to the efficacy of such a fragmented organizational tool to combat one of the most prescient issues in global security. It therefore rests with multiple bodies to create permanent and lasting change on an international scale, yet the division of that responsibility is unclear. Does the UNIDIR take responsibility for defining "cyber weapons," due to a proliferation of personnel with expertise in physical weaponry, or does that task rather fall to those members of the ITU, whose understanding of cyber space may be more subtle and nuanced? Will one of these bodies be able to redefine types of cyber warfare as "crimes against humanity" in the instance that a DDoS attack wipes out the electrical grid of an entire nation?

It is also inevitable that the issue of cybersecurity will fall between the cracks for several of these organizations. The website for the United Nations Interregional Crime and Justice Research Institute lists "Cyber-Crimes" as its second priority in a list of 12 pressing issues

("About UNICRI,"United Nations Interregional Crime and Justice Research Institute), yet a search for UNICRI's associated "Bibliography on Cyber Threats" reveals that the latest updated version was in 2014 ("Bibliography on Cyber Threats," United Nations Interregional Crime and Justice Research Institute). In the span of two years, the field of cyber security has grown and in that process distributed thousands of new literature on cyber threats. The pace of technology is outpacing the speed of bureaucratic prioritization. Fragmentation of power here leads to a dissolving of responsibility, and with it, a harmful negligence to the public.

Part B: The Definitions of Cyber Warfare in International Proceedings

If an attribution of a cyber attack can be determined — for example if the U.S. were to claim responsibility for the Stuxnet worm — then jurisprudence must be established to properly determine a course of action. Since the materials used in cyber warfare are not physical, how can one determine their magnitude? By bytes? By number of computers hijacked to perform an attack via a botnet? In monetary cost of damage due to weakened, damaged or destroyed infrastructure due to a virus? Will a worm, a virus, malware or a DDOS attack be classified as a weapon in the same way that nuclear missiles are classified in the UN's 1970 Treaty on the Non-Proliferation on Nuclear Weapons?

The definition of weaponry may remain elusive for some time, or until territorial delimitations can be placed on cyber space so that illegal activity — with or without the use of weapons — can be prosecuted. With clear definitions for neither territory nor weapons, jurisprudence remains at a standstill.

Goldsmith maintains the belief that the very nature of cyber weapons, and their ties to espionage, make them difficult to define in international documentation of treaties. Goldsmith states, "Offensive cyber weapons are guarded secrets because knowledge about the weapon enables the building of defenses and because revelation about attack capabilities would reveal a lot about exploitation capabilities. Even if nations revealed their cyber weapons, they take variable and changing forms. A weapons ban is thus hard to articulate" (Goldsmith, 6).

Yet remaining gridlocked will not protect future victimes from cybercrime. While the UN's 1970 Treaty on the Non-Proliferation on Nuclear Weapon is not airtight, it, at the very least, allows for a frame of reference, a ground zero for limitations.

As recently as December 7, 2016, the U.S. Department of Justice referenced their work to "increase the cross-border availability of data, through mechanisms like the 24/7 Network, which facilitates the preservation of digital evidence, as well as mutual legal assistance treaties and the Budapest Convention on Cybercrime, which enhance international cooperation in obtaining that evidence" ("Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies," U.S. Department of Justice). The terrifying part of this statement is that the Budapest Convention on Cybercrime produced a treaty on 2001. In the span of 15 years, computer security has developed so quickly as to nearly be unrecognizable from the laws of another decade. The inefficacy of the treaty has already been evidenced by the citation from Goldsmith above. The lack of jurisprudence is evidenced in organizations' apparent necessity to follow the only treaty on international cybersecurity policy that exists — even if that treaty is outdated by 15 years.

Part C: A Model for Interdisciplinary Cooperation

There are two strong examples of intergovernmental cybersecurity organizations which can serve as models for such a future body of the U.N.: the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) of Tallinn, Estonia and the European Cybercrime Centre (EC3). As described on their website, "EC3 is a key part of Europol's, and the EU's, response. The EC3 takes a three-pronged approach to the fight against cybercrime: forensics, strategy and operations" ("European Cybercrime Centre - EC3," Europol). EC3 consists of two forensics teams, digital and document forensics that perform research and development (European Cybercrime Centre - EC3," Europol).

The two teams of EC3 also work closely with members of the Joint Cybercrime Action Taskforce (J-Cat), which is comprised of members from "committed and closely involved EU Member States (Austria, France, Germany, Italy, the Netherlands, Spain and the United Kingdom); non-EU law enforcement partners (Australia, Canada, Colombia and the United

States, which is represented by two agencies: the Federal Bureau of Investigation and Secret Service)" and works on on high-tech crimes such as malware, botnets and intrusion. ("Joint Cybercrime Action Taskforce (J-Cat)", Europol). The diversity of the makeup of the EC3 serves as an important model. With a strong balance between diplomatic and technological backgrounds, the members of EC3 are able to tackle difficult issues of cybersecurity.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) of Tallinn, Estonia, is comprised of five branches — Law & Policy branch, Strategy branch, Technology branch, Education & Exercise branch and Support branch ("Structure." NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia). The CCDCOE offers Cyber Defence exercises, workshops and conferences and makes education of the public a key tenet of its organizational structure and day-to-day mission.

These two bodies represent small systems in an otherwise complex machinery of the international stage. Yet it is their efficacy of combining multiple disciplines that allows them to create cohesive and effective change. Since its establishment in 2013, the EC3 "has been involved in tens of high-profile operations and over 200 on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed over 800,000 files, the vast majority of which have proven to be malicious,"("European Cybercrime Centre - EC3," Europol).

Moving Forward

The efficacy of the UN in determining international cyber security policy lies in its ability to centralize and diversify the individuals who comprise that group. A marriage between diplomats and technologists is essential in ensuring that a team of cybersecurity policymakers can be informed from both the technical and political aspects of such decision-making. There is one fact that helps to clarify the reasoning for the division of cyber security into so many different factions of the UN: cyber security is not an isolated issue. Cyber security affects every domain, whether it be economic, social, political or humanitarian. Placing cyber security in a silo is not an effective solution moving forward. However, dismantling cybersecurity into parts only decreases any one group's ability to create cohesive policy measures for all.

It is necessary that a new group form: a specialized organization within the UN comprised of leaders in economics, business, foreign policy and technology must be assembled to begin creating a well-informed, resounding dialogue centered around positive impact and serious consideration of the gravity of cyber security concerns of the current era. Without interdisciplinary communication, foreign policy will be ill-equipped to face new and emerging threats from a rapidly evolving technological world; without strong policy, technologists worldwide will be left without a just legal system to protect them in cyber space.

Action Items

Education

In a conference paper from 1998, the hacker think tank L0pht professed the importance of education to an audience at the EMA Summit, “Educating individual users who may just use a personal computer at home on the internet is important. Any computer connected to the internet can be used by to attack any other computer. This means that attackers can use other people's computers as 'stepping stones' to reach their final target. This gives the attacker more anonymity and power to direct an attack from several places at once. So not only can an individuals file's be stolen or destroyed but their computer could be used unwittingly in an attack of another system.”(Wysopal, 12). For any person with a computer, the use of a powerful device comes with the responsibility of owning and operating that equipment safely. In the same way that drivers must pass a competency exam to be licensed to drive on the open road, similar measures must be taken with computer security. While it would be impossible, and perhaps infringing on personal privacy, to force all computer users to undergo a training before being able to access the Internet, measures can be put in place to ensure that computer security is not an afterthought.

Adding computer security as a mandatory class in public schools could be an option. In the same way that children must attend physical education classes to better understand their bodies and adopt healthy exercise habits early on, computer security tools would allow children to understand the internet and be conscious of protecting themselves online.

For anyone who works in the public sector, computer security training must be made mandatory. The United Nations (UNICRI) offers a course for journalists and chief information

officers for the development of cybersecurity knowledge and awareness, the goals of the course are described as "… increasing knowledge, accuracy and accountability with regards to reporting on new threats as well as fostering constructive connections, dialogue and exchange of experiences between different sectors in this area" ("Understanding and Reporting on Cyber Threats," UNICRI). If such a program were implemented for all government jobs, the decreased risk of exposure to threats could also mitigate the likelihood of attacks. The more we know about computer security, the less vulnerable we are.

Finally, education must extend to the international policy stage. In order for policymakers to better craft laws to defend against cyber attacks, they must actually understand those attacks. Education at this level comes from a collaborate, interdisciplinary movement. Experts in technology must have a seat at the table to share information and better guide policy.

Conclusion

International cybersecurity policy and law remain in flux. While the constantly evolving nature of technology itself should be taken into account when defining policy and drafting international agreements on the subject, concrete steps are necessary to ensure the collective safety of the world population. International cybersecurity laws are complex because the weapons and the tools are new: packets have replaced bullets, IP addresses have replaced dog tags. The physicality of cyber space is only seen in its effects on populations and at its very source of cables and data centers. Yet the alien nature of cyber space cannot deter policy makers from creating effective change.

Education is critical. Until effective change can be made, it is the individual responsibility of computer owners everywhere to arm themselves with the knowledge of safety and security in technological engagement.

The future of cybersecurity hinges upon an interdisciplinary approach to tackle the issues of attribution, foundational jurisprudence and decisive territorial treaties for cyber space. Without the input of experts in varied domains, cybersecurity will continue to cripple the international community. Education is one of the greatest tools in this arsenal of interdisciplinary combat against cybercrime, for only by arming individual citizens with the tools to protect themselves,

and by creating a stronger dialogue between decision makers of all domains, can we ensure that are creating a safer cyberspace and a safer world for all.

Resources

"About UNICRI." *United Nations Interregional Crime and Justice Research Institute*. United Nations. Web. 01 December 2016. http://www.unicri.it/institute/

"ARPANET and the Origins of the Internet." *Defense Advanced Research Projects Agency.* U.S. Department of Defense. 2016. Web. 01 December 2016. http://www.darpa.mil/about-us/timeline/arpanet

Barlow, John Perry. "A Declaration of the Independence of Cyberspace" Davos, Switzerland: February 8, 1996. Web. 01 December 2016. https://www.eff.org/cyberspace-independence

"Bibliography on Cyber Threats." *United Nations Interregional Crime and Justice Research Institute*. United Nations. Web. 01 December 2016. http://www.unicri.it/services/library_documentation/bibliographies/cyber_threats/cyber_threats_database.php

Boebert, W. Earl. "A Survey of Challenges in Attribution." National Research Council. 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press. doi: 10.17226/12997. https://www.nap.edu/read/12997/chapter/5

"Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?," Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School. Web. 01 December 2016. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

Department of Justice. "Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies."

U.S. Department of Justice: Office of Public Affairs. 07 December 2016. Web. 08 December 2016. https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime

Department of Justice. "Russian Cyber-Criminal Convicted of 38 Counts Related to Hacking Businesses and Stealing More Than Two Million Credit Card Numbers." *U.S. Department of Justice*: Office of Public Affairs. Press Release. 25 August 2016. Web. 01 December 2016. https://www.justice.gov/opa/pr/russian-cyber-criminal-convicted-38-counts-related-hacking-businesses-and-stealing-more-two

"Deutsche Telekom fault affects 900,000 customers." BBC News: BBC News Services. 28 November 2016. Web. 01 December 2016. http://www.bbc.com/news/technology-38130352

"European Cybercrime Centre - EC3." Europol. The European Union. 2016. Web. 01 December 2016. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Executive Office of the President ("Executive Order 13636: Improving Critical Infrastructure Cybersecurity"). Federal Register: National Archives and Records Administration. The White House. 12 February 2013. Web. 01 December 2016. https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

Frantzeskou, Georgia et al. "Source Code Author Identification Based on N-gram Author Profiles." Ed. Maglogiannis, Ilias and Karpouzis, Kostas and Bramer, Max. *Artificial Intelligence Applications and Innovations: 3rd IFIP Conference on Artificial Intelligence Applications and Innovations (AIAI)* 2006, June 7–9, 2006, Athens, Greece. Page 508-515. Web. 01 December 2016. http://dx.doi.org/10.1007/0-387-34224-9_59 Updated/

complete version at: https://www.utica.edu/academic/institutes/ecii/publications/articles/B41158D1-C829-0387-009D214D2170C321.pdf

Glennon, Michael J. "The Dark Future of International Cybersecurity Regulation." *Journal of National Security Law & Policy*: Volume 6:563. 11 April 2013. Web. 01 December 2016. http://insct.syr.edu/wp-content/uploads/2015/11/The-Dark-Future-of-International-Cybersecurity-Regulation.pdf

Glennon, Michael J., "The Road Ahead: Gaps, Leaks, and Drips" (April 4, 2013). 89 International Law Studies 362 (2013). Web. 01 December 2016. Available at SSRN: https://ssrn.com/abstract=2245776

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View (February 2011)," in *Future Challenges in National Security and Law*, edited by Peter Berkowitz, Web. 01 December 2016. http://www.futurechallengesessays.com.

"Joint Cybercrime Action Taskforce (J-Cat)." Europol. The European Union. 2016. Web. 01 December 2016. https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

Paglieri, Jose. "Panel to Trump: Train 100,000 hackers." CNN Tech: Cable News Network. 02 December 2016. Web. 04 December 2016. http://money.cnn.com/2016/12/02/technology/commission-on-enhancing-national-cybersecurity/index.html

Rosenblum, Nathan, et al. "Who Wrote This Code? Identifying the Authors of Program Binaries." University of Wisconsin, Madison, Wisconsin. Ed. Atluri, Vijay and Diaz, Claudia. *Computer Security –ESORICS 2011: 16th European Symposium on Research in Computer Security,* Leuven, Belgium, September 12-14, 2011. Proceedings. Springer, Berlin, Heidelberg. Page 172-189. Web. 01 December 2016.

http://dx.doi.org/10.1007/978-3-642-23822-2_10 or http://pages.cs.wisc.edu/~jerryzhu/pub/Rosenblum11Authorship.pdf

Rouse, Margaret. "Definition: Honeypot (honey pot)." 2016. TechTarget: SearchSecurity. Web. 01 December 2016. http://searchsecurity.techtarget.com/definition/honey-pot

Shackelford, Scott, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" (April 28, 2009). Berkley Journal of International Law (BJIL), Vol. 25, No. 3, 2009. Web. 01 December 2016. Available at SSRN: https://ssrn.com/abstract=1396375

"Structure." NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. 2016. Web. 01 December 2016. https://ccdcoe.org/structure-0.html

"Understanding and Reporting on Cyber Threats: UNICRI specialized course on cyber security for journalists and public information professionals" United Nations Interregional Crime and Justice Research Institute. 2015. Web. 01 December 2016. http://www.unicri.it/news/article/understanding_reporting_cyber_threats

United Nations Convention on the Law of the Sea. "United Nations Convention on the Law of the Sea." United Nations. 10 December 1982. Web. 01 December 2016. http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations." NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, Estonia. 2016. Web. 01 December 2016. https://ccdcoe.org/un.html

Wang, Ping, et al."Honeypot detection in advanced botnet attacks." School of Electrical Engineering and Computer Science, University of Central Florida. International Journal of Information and Computer Security 4, 1. (February 2010), 30-51. Web. 01 December 2016. http://dx.doi.org/10.1504/IJICS.2010.031858 or

http://www.cs.ucf.edu/~czou/research/honeypotDetect-IJICS.pdf

"What is a Botnet Attack? - Definition" Kaspersky Lab: Kaspersky Lab. 2016. Web. 01 December 2016. https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.WFDkJ6IrKog

Woolf, Nick. "DDoS attack that disrupted internet was largest of its kind in history, experts say." *The Guardian*: The Guardian. 26 October 2016. Web. 01 December 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Wysopal, Chris. "The State of Computer Security: Where is it at? How it got that way? What can be done about it?" L0pht Heavy Industries at the EMA Solutions Summit. Thursday October 29, 1998. Web. 01 December 2016.