OCTOBER 2015

TAKING THE FIGHT TO MALICIOUS CYBER ACTORS:

MOIETY MONEY,

LETTERS OF MARQUE AND REPRISAL,

& THE DE-ANONYMIZATION OF THE INTERNET

BY: MONTGOMERY BLAIR SIBLEY
J.D., Masters, Cybersecurity Policy, CIPP/US
www.PrivacyComplianceConsulting.com
(202) 643-7232
mbsibley@PrivacyComplianceConsulting.com

CONTENTS

OVERVIEW

"*Steve Austin, astronaut. A man barely alive. Gentlemen, we can rebuild him. We have the technology. We have the capability to make the world's first bionic man. Steve Austin will be that man. Better than he was before. Better... stronger... faster."* Oscar Goldman

Just like Steve Austin at the start of the 1970s television show "The Six Million Dollar Man", our Internet is "barely alive." Beset by malicious actors intent on preying on our personal privacy and property rights; the greater harm they do is denying to us the full realization of the potential of the Internet to usher in a new economic prosperity for all of mankind. I herein claim – akin to Oscar Goldman in the Six Million Dollar Man – that we can rebuild the Internet; We have the technology, We have the legal capability. If we are brave enough to do so, the Internet will be: "Better... stronger... faster."

The Technology: A vast array of existing software tools are available to be deployed in offensive cyber attacks against malicious cyber actors to pursue, publicly identify, plunder their assets and punish, virtually – and in the real world – these 21st Century *hostis humani generis* or enemies of mankind.

The Capability: Under the existing international legal framework the United States presently has legal authority through Moiety Money and Letters of Marque and Reprisal to offensively respond to the asymmetric cyber-war declared on the United States by these malicious actors. Additionally, seventy percent (70%) of the world's Internet traffic passes through data centers in Loudoun County, Virginia providing both legal and practical authority to the United States over the Internet to require identification of all users of the Internet thereby unmasking these cyber *hostis humani generis*.

Patently, in this cyber-war, our federal government, which by its very Charter was organized to provide for the "common defense", is failing and failing miserably. If we are brave enough to do so, we can fight back and realize an Internet well policed by the United States resulting in a "better... stronger... faster" Internet. Most importantly, we will be rewarded by this effort with significant economic growth now lost to data stolen by these cyber *hostis humani generis*.

I. THE UNACCEPTABLE STATUS QUO

The Internet is a trans-border domain – best estimates are that roughly 2.5 billion people and more than 1 trillion "Internet of things" are connected to the network. In that domain, We, the People of the United States, are under constant cyber attack. So forget the semantics: These cyber attacks are nothing short of war on our way of life by another name. We are at Cyber War with malicious actors.

Hacking attacks on U.S. companies often originate overseas and transit foreign servers.[1] Looking at just the total number of annual malware events – 170 million across all organizations – the simple math results in the conclusion that five (5) malware events occur every second. The forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000.[2] Recently, the federal government's own database at the Office of Personnel Management ("OPM") was hacked. The result: 19.7 million applicants for security clearances had their Social Security numbers, fingerprints and other personal information stolen. The hackers rummaged through various OPM databases for more than a year – creating a significant threat to national security.[3]

Obviously, our federal government not only cannot – as promulgated in the Constitution – provide for our "common (cyber) defense" in this Cyber War but for its own cyber defense as well.

However, it is not just personal information that is being compromised, but the very foundation of our economy. The Commission on the Theft of American Intellectual Property recently concluded that:

> The scale of international theft of American intellectual property is unprecedented – **hundreds of billions of dollars per year**, on the order of the size of U.S. exports to Asia. The effects of this theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the

incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. . . .**The American response to date of hectoring governments and prosecuting individuals has been utterly inadequate to deal with the problem**.[4]

The conclusions are inescapable:

- The United States and its Citizens are losing much from the unrestrained cyber-attacks that are rapidly proliferating;

- Cyber attacks are asymmetric in the current paradigm, with malicious attackers having the virtual high ground over defenders who solely concentrate on passive fortifications – patching the newest hole in their defenses and creating taller and thicker walls;[5] and

- Current passive cyber security defenses such as intrusion detection, anti-virus, and hardened software are not sufficient to repel cyber attackers.

In conventional kinetic warfare this defensive passivity would be considered entirely nonsensical, given the available active strategies, such as counterattacks and deception.[6] Nevertheless, today's federal policy and legal framework for guiding and regulating the response to these constant cyber-attacks is ill-formed, undeveloped, and highly uncertain. All public policy related to cyber attacks solely focuses on defending domestic computer systems and networks against attack.[7]

Inanely, resort to offensive cyber strategies – "Hack-Back" in cyber parlance – is presently prohibited by federal laws criminalizing any retaliatory self-defense against these virtual assaults. For example, the Computer Fraud and Abuse Act, 18 U.S.C. §1030 *et seq*. and the Fraud and Related Activity in

Connection with Access Devices, 18 U.S.C. §1029 both prohibit and criminalize individuals and corporations from undertaking Hack-Back activities. Starkly, the Justice Department's Manual on Computer Crime, states: "Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as 'hacking back' into the attacker's computer – even if such measures could in theory be characterized as defensive. Doing so may be illegal, regardless of the motive. . . [T]he company's system administrator can contact the system administrator from the attacking computer to request assistance in stopping the attack or in determining its true point of origin."[8]

Good luck asking a Chinese network system administrator for assistance in stopping a cyber attack emanating from his computer network.

In sum, such federal laws require that the Citizens and corporations of the United States leave their virtual doors to their virtual houses unlocked for any malicious cyber actor to walk in during dinner and violate the privacy and steal property all the while preventing the owner from getting up from the dinner table to prevent such violation and theft.

This is simply asinine.

II. WE HAVE THE TECHNOLOGY

The *status quo* of passive response to the constant plundering of our personal privacy, property, and economy must stop. We certainly have the technology to respond and fight this rapacious behavior by malicious actors which threatens our very way of life. That presently prohibited "technology" falls under the category of "Cyber Offense."

Cyber security specialists categorize the main Cyber Offense tactics as the three "A"s: Annoyance, Attribution and Attack. Annoyance involves tracking a hacker and leading him into a fake server, thereby wasting his time. However, wasting a hacker's time is ineffective given the computing power which amplifies the "time" a hacker has at his disposal.

Attribution uses tools to trace the source of an attack back to a specific location, or even an individual hacker. Once known, the identity of the hacker can be dutifully reported to police authorities. Obviously, with the vast majority of hackers being situated in countries which possess neither the resources nor will to prosecute these malicious actors, such "reporting" is practically useless to stop further attacks. Cybersecurity experts criticized efforts to prosecute cybercriminals as a waste of time and say the people who are arrested are rarely the right people: They're often the middlemen instead of the kingpins.[9]

Thus it is the third "A" – Attack – that remains to secure the Internet from malicious actors. To "Hack Back," a company accesses a hacker's computer to disrupt, deny, degrade, or destroy the information within that computer and/or the hacker's computers/networks themselves.[10] These steps are presently illegal under federal law.[11]

A selection of such cyber offense tools – presently banned from use by Congressional action – would allow significant negative consequences to follow cyber attacks on the interests of the United States, its Citizens and corporate entities. For example:

A. BOOBY TRAPPING SOFTWARE: Booby trapping software can serve as an automatic start to the counter-attack process. As an automated response, booby

traps could quickly engage the attacker before he or she even realizes that the attack has failed. This would allow the counter-attack to catch the attacker unaware and before he or she has a chance to retreat and abandon the source of the attack. With automated attack toolkits such as Metasploit[12], an automated counter-attack may gain access to the offending system thereby allowing an escalation of the Hack-Back to virtually harm the attacker. The result: Restoring equilibrium between attackers and defenders in the digital domain.[13]

B. SNIFFER SOFTWARE: Botnets are one of the biggest threats to computers and networks. The botnet infects a computer then connects the computer to the hacker's command and control server ("C&C server"). The botnet runs in the background and communicates with the C&C server to receive instruction that typically involves being part of malicious activities performed against networks without the knowledge of the owner. The victims of the botnet attacks number in the millions of infected computers. Sniffer software tools are able to identify the C&C server domain names and Internet Protocol address – a numerical label assigned to each computer connected to a computer network that uses the Internet – that have been contacted by the infected host. Once identified, software is available to shut down the C&C server and thus stop the cyber attacks.[14] Indeed, it is possible to remotely physically destroy the C&C server by setting it on fire by: (i) disabling the computer's fan and overheating the computer until it catches on fire[15] or (ii) reading the values from the computer's internal battery, re-programing the battery's firmware, and then overcharging the batteries until they catch on fire.[16]

C. ANTI-WORMS: An Internet worm is type of malicious software that self-replicates and distributes copies of itself to its network. These independent virtual viruses spread through the Internet, break into computers, and replicate without intervention from and unbeknownst to computer users.[17] Among the most notorious malware worms were the CodeRed[18], Blaster[19] and Slammer[20] worms which collectively caused billions of dollars of damage. Yet, rather than just constantly patching the software holes that allow Internet worms to proliferate, there exists a method that transforms a malicious worm into an anti-worm which disinfects its original.[21] Yet, use of such anti-worms is prohibited by federal law.

D. ATTRIBUTION TECHNIQUES: Cyber-attackers launch attacks through numerous computer stepping-stones to hide their identities as they steal

confidential information from victims. By using stepping-stones, it becomes very difficult to trace-back the attack to the originating computer. A Pebbletrace scheme imbeds Zero-day[22] based Pebbleware in the stolen information and thereby enables investigators to trace-back to the attacker's machine which has the stolen information.[23] Likewise, (i) the "honey badger," locates the source of an attack, tracking its latitude and longitude with a satellite picture, and (ii) "beacons", which are placed in documents to detect when and where data is accessed outside the user's system. Upon such information the identify of the attacker and his physical location can be known.[24] Yet, as above, use of these software techniques enter the gray area of the law potentially subjecting the user to federal criminal prosecution for Hacking-Back.

E. **MASTER BOOT RECORD DESTRUCTION** – The Master Boot Record is 512 bytes at the beginning of a computer's hard drive that contains the partition table for the hard drive. The first 440 bytes are blank, therefore it's a great place for counter-cyber attack software to hide itself. Publicly available software – if you know where to look – called Rombertik, once planted on the Master Boot Record, encrypts a computer's files using a random 256-byte encryption key for each file. None of the encryption keys are saved anywhere effectively randomizing all the data on the disk making it virtually impossible to recover that data. It's like putting the hacker's hard-drive through a shredder.[25] Yet again, such action is prosecutable under federal law.

F. **BASIC INPUT OUTPUT SYSTEM (BIOS)**: The most important component of a computer system is the BIOS as it holds the code which is executed at the time of turning on the computer and thus is considered as the trusted computing base. Unfortunately, the BIOS of new computer systems (servers, laptops, desktops, network devices, and other embedded systems) can be easily changed remotely which can cause denial of service, stealing of information or addition of new backdoors which can be exploited by attackers for causing business loss, passive eaves-dropping or total destruction of system without knowledge of the user. The attack on the Iranian Nuclear Power Plant by the Stuxnet virus is an example of such a BIOS attack.[26] Similar BIOS attacks could be launched against malicious cyber actors giving them a taste of their own medicine.

In sum, at present their exists a wide-range of publicly available offensive

cyber attack capabilities – and many more not publicly known and/or yet to be created – to allow those under cyber attack to defend themselves by striking back again malicious cyber actors. Yet, federal law prohibits such basic self-defense by individuals and corporate entities.

Instead, our presently authorized offensive cyber actions are confined to the military which presents two obvious problems. First, there is an ever-diminishing pool of talented recruits from which the military can draw. According to a 2009 report from Mission Readiness: "27 percent of young Americans are too overweight to join the military."[27] Thus, the pool from which the military may draw upon for recruits is nearly 30% smaller due to obesity. This is a huge waste of intellectual talent in a cyber war which does not require physical fitness.

Imagine this: Our present video-game generation turned loose on real-world gaming in which the malicious cyber actors are the prey to be identified, confronted and destroyed. At present, there are currently over 34 million core video gamers in the United States, and they are playing video games for an average of **22 hours every week**.[28] Image further those millions of man-hours put to use developing new offensive cyber software, tracking down malicious actors and engaging them in a manner which benefits society, rather than solely the self-gratifying, synthetically-significant, onanistic behavior of these video gamers.

Second, deployment of these offensive cyber military resources is limited by the Law of Armed Conflict which presently does not easily allow release of these offensive cyber weapons in the interest of private sector economic concerns.

The take-away from this picture should be self-evident: Unleash – in a controlled fashion – the potential of the crowd upon our cyber attack problem and the result will be spectacular. Better software, better cyber watch-dogs, in short, a better Internet.

III. WE HAVE THE LEGAL CAPABILITY

Along with the Technology to fight the cyber threats to our way of life, we have the present Legal Capability to offensively engage the malicious cyber actors. Admittedly, in 2009, the self-appointed-arbiter-of-all-things-legal, the American Bar Association declared that: "the single greatest difficulty encountered thus far in the development of a legal response [to the national security cyber threat] lies in the trans-national nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace."[29]

I strongly disagree.

The United States does not "need to secure international agreement" for controlling offenses in Cyberspace. Instead, as we have done the last two centuries, we must lead by utilizing the existing legal framework with fearless integrity to make right what we – the United States alone – have wrought: An anonymous internet more damaging every day to the privacy and property of the United States, its Citizens and corporate entities.

By deploying two well-established legal vehicles – Moiety Money and Letters of Marque and Reprisal – and removing the anonymous nature of the Internet, order can be imposed upon the damaging chaos of the Internet we have created.

A. MOIETY MONEY

The first step to re-gaining control of and imposing law and order in cyberspace is employing the well-established role of "Moiety Money" to pay informants for providing information leading to the identification and/or arrest of cyber-criminals. These schemes are variously known as "reward programs", "bounty schemes", "incentive payment programs", and "moiety acts".[30] Presently, the Internal Revenue Service can pay informants up to $2 million for calling in valuable information. In the first thirty years of this program, more than seventeen thousand informants collectively earned over $35 million from the IRS under this program.[31]

The Environmental Protection Agency will pay up to $10,000 for information on illegal dumping of hazardous materials.[32] The Insider Trading and Securities Fraud Enforcement Act of 1988 gives the Securities & Exchange Commission authority to award bounties to: "the person or persons who provide information leading to the imposition" of a monetary penalty for insider trading.[33] Homeland Security, like the IRS, has long been authorized to give rewards to informants providing information relating to the violation of Customs laws. Under these laws, persons who provide information leading to the seizure of a vessel or baggage subject to seizure are eligible for rewards of up to twenty-five percent of the take. Remarkably, under these rules, private citizens not only may provide information regarding Customs violations but also may actually seize the vessels or baggage in question as long as the seizure is reported immediately. The total award cannot exceed $250,000 for any case.[34]

Finally, under the "Rewards for Justice" program, the Secretary of State may authorize rewards for information that leads to the arrest or conviction of anyone who plans, commits, or attempts international terrorist acts against U.S. persons or property, that prevents such acts from occurring in the first place, that leads to the location of a key terrorist leader, or that disrupts terrorism financing.[35]

Remarkably, Congress has not established similar bounty schemes for those malicious cyber actors who cause significant damage to the economy of the United States. Instead, Congress has affirmatively hampered pursuit of these malicious cyber actors by those who have the skill and who could be monetarily motivated to identify these individuals. Patently, a bounty scheme which would release individuals and corporate entities to turn their talents to this problem and handsomely reward them for success could go a long way in cleaning up our virtual Dodge City.[36]

Consider the Trident Breach case: Criminal hackers stole $70 million from 400 American companies in a short time frame. The mode of theft involved infecting hundreds of thousands of Americans computers with the "Trojan" virus called ZeuS. ZeuS located the bank information on the infected computers and then sent that information to the hackers. In 2008, the criminal hackers recruited three thousand (3000) money "Mules" by advertising work-at-home jobs which required the opening of bank accounts. The cyber-criminals then wire-transferred from business payroll accounts to the bank accounts of the Mules. The Mules then

– after deducting a small commission – wired the stolen funds to bank accounts in Eastern Europe.

When banks noticed the losses piling up, they stopped the direct wire-transfers back to Eastern Europe. The cyber-criminals responded by sending dozens of students, mainly from southern Russia, to be a new breed of money mule. The cyber-criminals obtained work/study visas for the Student-Mules who then opened bank accounts to receive the stolen money which they then sent back to Eastern Europe. The FBI was unable to locate eighteen of the Student-Mules who were still in the United States.

Learning of this roadblock, Professor Gary Warner of the University of Alabama at Birmingham unleashed the students in his Computer Forensics and Justice Studies class to find the wanted Student-Mules. "So the students used the techniques we had taught them during investigating online crime [class] and began crawling Facebook pages and VKontakte, which is a Russian version similar to Facebook and were able to quickly identify profile pages of almost all of the at-large mules," Warner said. Warner's students discovered one of the students-turned-mules had brazenly posted pictures of herself with a wad of hundred-dollar bills. Another had posted a picture of himself dressed in an "I ♥ New York" top, arms aloft, celebrating in a bar with his friends – some of whom turned out to be other money mules. And another was pictured standing next to the new car he had presumably just bought. As a result, seventeen of the eighteen mules were arrested by the FBI.[37]

The point should be plain: Motivate and harness the power of the crowd to lend their diverse talents to augment the limited resources of the government by handsomely rewarding efforts that result in successful identification of malicious cyber actors.

B. LETTERS OF MARQUE AND REPRISAL

Yet Moiety money is not enough as it limits crowd-sourced cyber investigators to passive acts of research: an army of cyber Sherlock Holmes sniffing for clues and making connections between disparate bits of evidence yet without the ability to bring the cyber pirates to justice . Much more is needed now, as it was two hundred years ago when our founding fathers faced an

analogous threat to the security and commercial interests of the newly-formed United States by high seas pirates. Their response?

Article I, Section VIII of the U.S. Constitution which states in relevant part: "The Congress shall have Power To . . . grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water." Letters of Marque and Reprisal are: "a license authorizing a private citizen to engage in reprisals against citizens or vessels of another nation."[38] Privateers were authorized by the State not only to protect their own interests, but to aid in the war effort by assisting in the destruction of the commerce of the hostile nation. They paid for themselves, in the end, with profits from the commerce they destroyed.

The history of Letters of Marque and Reprisal starts with Henry II who issued such Letters in 1243 to coastal seafarers to "annoy our enemies by sea or by land," even though the individuals had not suffered personal loss.[39] The object of the Letters of Marque and Reprisal were not only hostile nations, but the pirates who roamed the un-policed high seas. To counter the pirate threat, international law quickly develop to declare pirates to be enemies of the human race, *hostis humanis generis.* The noted 16th Century legal scholar Alberico Gentili[40] declared that pirates were the common enemies of all mankind, and that they could be attacked with impunity by all, because pirates are without the pale of the law. As the scorners of the law of nations they can find no protection in that law.[41]

Our nascent Continental Congress issued Letters of Marque and Reprisal to promote raiding against Britain's economic assets in North America during the Revolutionary War. This approach was deemed necessary because the young United States lacked a navy of sufficient size to confront its early enemies. The Letters expeditiously authorized a much-needed military capability to wage war when other tools were not readily available.[42] Thus, it was no surprise that when the Constitution was finally adopted, Congress was given explicit authority under Article I, Section VIII to issue Letters of Marque and Reprisal.

Subsequently, under authority of Article I, Section VIII, Congress enacted legislation permitting the seizure of pirate vessels. In the case of *United States v. The Brig Malek Adhel* (1844)[43], a pirate vessel was seized in Brazil. In approving of the seizure, the United States Supreme Court held that: "a pirate is deemed, and properly deemed, *hostis humani generis* because he commits hostilities upon

subjects and property of any or all nations, without any regard to right or duty, or any pretense of public authority." Thus piracy obtained the status as a *jus cogens*[44] norm and any nation can enforce and punish pirates, wherever the culprits may be found and without regard to where the offense occurred.[45] It is worth a moment's detour to recognize that while the 1856 Paris Declaration Respecting Maritime Law[46] abolished Privateering through Letters of Marque and Reprisal, the United States never ratified this Declaration. As such the Declaration does not *de facto* nor *de jure* prohibit the United States from issuing such Letters of Marque and Reprisal.

Lacking now a similar capability to confront our cyber enemies, it is time Congress dusted off the Letters of Marque and Reprisal authority it possesses and unleash our cyber-privateers to confront the cyber pirates.

1. PIRATES & CYBERSPACE

"Cyberspace" has been defined as: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[47] As such, it is most legally analogous to the high seas, and thus Cyberspace is a *res communis omnium* or the common heritage of all humankind, not subject to the appropriation by or any sovereignty. Regrettably, Cyberspace has evolved to offer anonymity to malicious users thereby allowing such users to plunder and pillage with impunity.

To address the malicious users of the Internet, the United States has made its position clear: The "development of norms for state conduct in cyberspace does not require a re-invention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace."[48] Moreover, the United States has served International notice that: "the following activities may qualify as violations of U.S. territorial sovereignty: attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy."[49]

International law is grounded upon the notion of *Jus Cogens* or peremptory norms which refers to certain fundamental, overriding principles of international

law, from which no derogation is ever permitted.[50] There is universal agreement that "Piracy" enjoys the status as a *Jus Cogens* norm and that all nations can punish pirates, wherever the culprits may be found and without regard to where the offense occurred.[51]

2. CYBER PIRATES & LEGAL NORMS

This, however is not the 17th Century but the 21st Century, and while a few seafaring pirates still remain, *viz,* Somalia, the much larger contingent of these *hostis humani generis* sail the electronic seas armed with virtual raiding vessels that can appear from anywhere at any time and inflict significant damage harmful to the commercial and national security interests of the United States and its Citizens. Fortunately, existing International Law fully equips the United States to engage these cyber-pirates wherever found.

Sovereign Immunity generally prohibits State actors from intruding into the cyber infrastructure of another State as that would be considered an exercise of jurisdiction on foreign territory and therefore a violation of the principle of Territorial Sovereignty. Yet, Territorial Sovereignty is not limitless. One well-recognized principle of International Law is the "Effects Doctrine" which allows a State to exercise jurisdiction over conduct notwithstanding that the conduct does not take place within its own territory. The condition precedent for the exercise of such jurisdiction is that the conduct produces harmful "effects" in the State's territory.[52]

The European Attorney-General has detailed the scope of the "Effects Doctrine":

> The two undisputed bases on which State jurisdiction is founded under international law are territoriality and nationality. The former confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place. The latter confers jurisdiction over nationals of the State concerned. Territoriality itself has given rise to two distinct principles of jurisdiction: (i) subjective territoriality, which permits a State to deal with acts which are originated within its territory, even though completed abroad (ii) objective territoriality, which conversely,

> permits a State to deal with acts which originated abroad but which were completed at least in part within its own territory. **[The Effects Doctrine] confers jurisdiction upon a State even if the conduct which produced [the effects] did not take place within the territory**." (Emphasis added).[53]

Applying the "Effects Doctrine" to Cyberspace thus permits the exercise of jurisdiction by the United States over individuals – and their property – who have conducted cyber operations against the cyber infrastructure of the United States regardless of where those persons or their property are situate.

The "Effects Doctrine" in the jurisprudence of the United States was first formulated by Judge Learned Hand in *United States v. Aluminum Co. of America*[54], and now is enshrined at §402 of the Restatement of Foreign Relations Law of the United States, 3rd: "[A] state has jurisdiction to prescribe law with respect to . . . (c) conduct outside its territory that has or is intended to have substantial effect within its territory."

3. CYBER PIRATES & THE MODERN LETTERS OF MARQUE AND REPRISAL

Upon these premises, Congress is fully authorized to issue Letters of Marque and Reprisal to: (i) actively participate in shaping national cyber strategy without the interference of the tepid and institutionally-fawning State Department and (ii) make clear that the United States will no longer suffer deprivations upon its Citizens and their property without imposing severe consequence on any who would attempt such folly. Indeed, I would argue that the failure of Congress to issues such Letters is an abdication of each Members' oath to: "support and defend the Constitution of the United States against all enemies, foreign and domestic . . ."[55]

Congress could issue Letters of Marque and Reprisal to private Citizens and/or corporations. Letters of Marque and Reprisal could be used specifically to enable private entities to take action utilizing the offensive software tools described above against malicious cyber actors while immunizing those entities from any domestic or international legal consequences. White-hat computer hackers can engage in monetarily-rewarding cyber-privateering to the benefit of

all Internet users. Congress could readily establish regulations and Internet Prize Courts to govern the orderly deployment and rewarding of cyber-privateering.[56]

Private citizens and/or corporations could augment the Moeity Money set by Congress into a fund where it would be managed and distributed at the discretion of the Internet Prize Court to successful White-Hat Privateers. This, of course, would be nothing new. The use by the United States of private sector security companies to provide police-type services is both legally permitted and widely invoked. Remarkably, more money is spent on private police than public police within the United States.[57] If, in the real-world sphere, we authorize bounty hunters to use kinetic force to apprehend fugitives, why not cyber-force to the same ends in the cyber sphere?[58]

C. RE-WRITING THE RULES OF THE INTERNET ROAD

Last, it is time to invoke the "nuclear" option to control malicious cyber actors. This option involves quarantining the areas of the globe from access to the U.S. Internet until such areas adopt our policies to prevent anonymous use of the Internet. While many arguments can be made to allow anonymous use of the Internet, the simple fact remains that such egalitarian goals must now fall to the reality of the harm anonymous users are causing to the security and economy of the United States. **Accordingly, it is time to require that access to the Internet be conditioned upon identification of each user of the Internet**.

To understand our present ability to de-anonymize the Internet, an understanding of the basic Internet infrastructure is needed. That infrastructure has three relevant major components: (i) Internet Protocol Addresses, (ii) Tier One Internet Service Providers, (iii) Regional Internet Registries.[59]

1. INTERNET PROTOCOL ADDRESSES

First, every device that accesses the Internet is physically connected – by cable or wireless network (Wi-Fi) – to a network of devices which are further connected to other networks of devices to allow global connectivity. Each computer on the network is identified by an Internet Protocol address which is a string of 16 digits used to identify a computer on the network which tells a network your location in the world and your individual identity on the network.[60]

Notably, there are two types of Internet Protocol addresses: "Static" and "Dynamic." Static Internet Protocol addresses always remain unchanged hence the computer is always identifiable. Dynamic Internet Protocol addresses change each time a computer connects to the network. Computer Network System Administrators prefer Dynamic Internet Protocol addresses as they save the time for assigning and maintaining Internet Protocol address information about each computer. Yet by assigning Dynamic Internet Protocol addresses for anonymous Internet interaction users identities are masked. By using Static Internet Protocol addresses, anyone can determine your location and track your identity and monitor your internet activity. Moreover, with the roll-out of Internet Protocol, Version 6 ("IPv6"), the problem of IPv4 IP address exhaustion – a result of the limited number of IPv4 addresses mathematically available – is eliminated given the exponentially higher number of IPv6 address available above the IPv4 limit.

Before the howls of the cosmopolitan elite are screeched in response to this fact and my proposal to make it standard practice to require Static Internet Protocol addresses mandatory to allow such Internet-use tracking, consider this analogy: On the actual highways of the world, do we allow the drivers of vehicles to operate anonymously? The answer, of course is no. The reason is plain: In so much as vehicle operators can cause significant property damage and injuries and/or death to persons, their identities must be know. Accordingly, in order to hold the operators of vehicles accountable for their actions, we require driver's licenses, vehicle registrations, license plates and, significantly, vehicle identification numbers unique to each vehicle on the road worldwide. In that way, if a breach of the law occurs, the perpetrator can be identified and called to account for any damage done. For the same reason, the identification of each Internet user must be required.

2. TIER ONE INTERNET SERVICE PROVIDERS

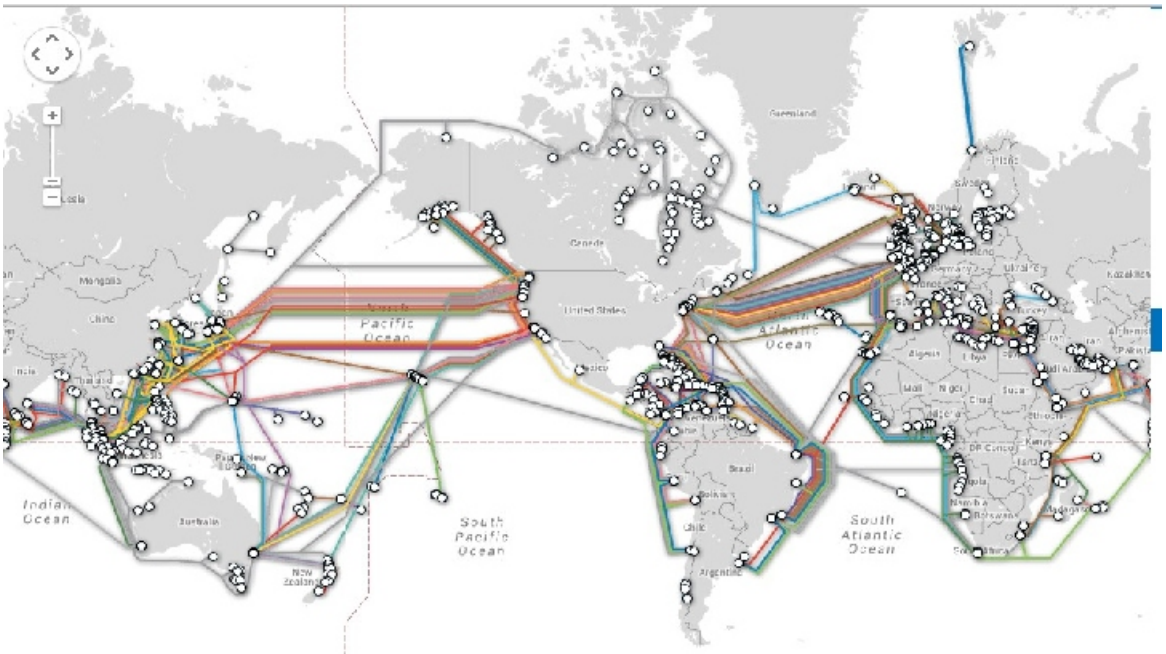
Second, the Internet is divided into Autonomous System Networks which operate independently while cooperating with each other by exchanging routing information for Internet traffic to achieve a global connectivity. The number of unique Autonomous System Networks in the routing system of the Internet exceeded 5,000 in 1999, 30,000 in late 2008, 35,000 in mid-2010, 42,000 in late 2012, and 47,000 in mid-2014 and presently there are 51,677 as of September 2015. The Autonomous System Networks are divided into "Tiers" depending on

their size and scope.

A Tier One Autonomous System Network Internet Service Provider ("ISP") represents the highest level of Internet Service Provider in its region and all lower tier level ISPs must channel their traffic through a Tier One ISP in order to be connected to the rest of the Internet. Presently the Tier One ISPs in the United States are: AT&T, Verizon, Sprint (Softbank Broadband), Century Link (Qwest), Level 3, NTT/Verio and Cogent.[57]

Given this structure, Congressional/Executive action to control the traffic on the Internet into United States based computers can be accomplished by imposing "Rules of the Internet Road" on these Tier One ISPs. Presently, the Office of Foreign Asset Control[58] orders financial institutions to block the assets of narcotic smugglers and terrorists from transfer from or to them. Likewise, Congress can create an Office of Internet Protocol Address Control agency which would order the Tier One ISPs to block all Internet communications to or from identified malicious cyber-actor computers and the Autonomous System Networks from which they are operating.

Additionally, if the Tier One ISPs are obdurate, a few tactical kinetic snips of the submarine cables[59] which physically connect the World's computers will free the United States from Nigerian Princes seeking to expatriate their vast wealth, Chinese hackers and other malicious cyber actors from troubling our economy and privacy any more.

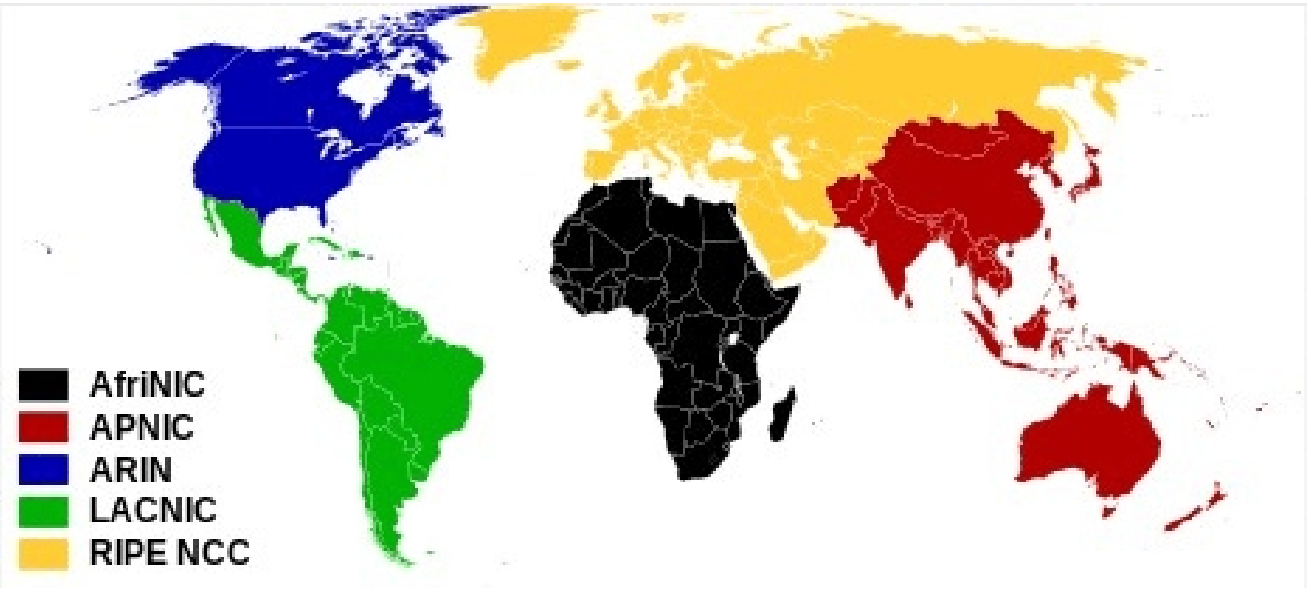


Submarine Cable Map

3. REGIONAL INTERNET REGISTRY

Last, the Internet's operation is controlled by Regional Internet Registries which are organizations that manage the allocation and registration of Internet number resources within a particular geographic region of the world. The Regional Internet Registry system evolved over time, eventually dividing the world into five Regional Internet Registries which allocate Internet Protocol addresses[60]:

1. American Registry for Internet Numbers (ARIN) for North America
2. Réseaux IP Européens - Network Coordination Centre (RIPE NCC) for Europe, the Middle East, and Central Asia
3. Asia-Pacific Network Information Centre (APNIC) for Asia and the Pacific region
4. Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and the Caribbean region
5. African Network Information Center (AfriNIC) was created in 2004 to manage allocations for Africa



The Internet number resources allocated by the Regional Internet Registries include: (i) Internet Protocol addresses and (ii) Autonomous System Network numbers. As such, ARIN could require as a condition of continued assignment of an Autonomous System Network number to a Tier One ISP that they require identification of each person who utilizes a computer network which traverses their Autonomous System Network. As with state-issued driver's licenses, each lower tier ISP would be obligated to obtain satisfactory identification of the owner/user of each Static Internet Protocol address which is assigned. A unique Internet User's License similar to the Driver's License would be required of each person each time they log-on to the Internet.

Moreover, until the other four Regional Internet Registries agree to comply with this identification requirement, all their traffic would be blocked by the Tier One ISP from entering or leaving North America. Simply put, if you want to access the markets and peoples of North America, then you have to play by our Rules of the Internet Road. If they refuse, God Speed, we can do <u>without</u> them.

Plainly, there are significant technical and phase-in issues to be addressed to implement such a scheme. However, the question I pose in response to the expected virulent objections is this: What is the alternative? More of the *status quo* where the economy of the United States loses billions of dollars annually? Our national security compromised by frequent credit card, health and financial information breaches? I am open to alternative suggestions but believe there are none based on the last decade of cyber attacks upon the United States.

IV. ARE WE BRAVE ENOUGH?

We have the Technology. We have the Legal Capability. But are we brave enough to come from behind our ever thicker and ever taller cyber Maginot Line[61] and take the fight to the malicious actors who attack us?

In the 18th Century, that founding generation did not hesitate to declare their freedom from the yoke of Britain with offensive action. In the 19th Century, when faced with conflicts which threatened to tear this nation apart, our predecessors sprung to offensive action to preserve a Union by refusing to permit slavery to tarnish the organic law premise of these United States that "all men are created equal". In the 20th Century, the "greatest generation"[62] took up arms to defeat the chaos and terror of global fascism.

What will be the future judgment upon those of us of the 21st Century who, by our passive response to this Century's cyber-fascism, cyber-terror and cyber-threats, imperiled the precious rights and way of life our predecessors sacrificed their blood and tears to bless us with?

My answer is plain and to explicate it I quote Abraham Lincoln: "America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves." We are destroying our freedoms and thus our country by allowing attacks upon our way of life without offensive response. This must stop if we are to hold our heads high if and when we meet our forebearers on judgement day.

Accordingly, Congress must not only remove the handcuffs which are preventing us from protecting our "lives, liberty and the pursuit of happiness", but lead the fight by: (i) rewarding through Moiety Money the crowd for policing the Internet, (ii) unleashing the crowd by Letters of Marque and Reprisal to Hack-Back against malicious cyber-actors and (iii) embarking on a "Manhattan Project"[63] to sanitize the Internet through denying access to U.S. physically based Computers by Autonomous System Networks that fail to comply with the new Rules of the Internet Road written by We the People of the United States of America. If done, the Internet will be "Better . . . stronger . . . faster."

END NOTES

1. 50 Stan. J Int'l L. 103; *International Law and Private Actor Active Cyber Defensive Measures*; Paul Rosenzweig

2. *Verizon 2015 Data Breach Investigations Report*, p. 21, 29. Retrieved from: http://www.verizonenterprise.com/DBIR/2015/

3. *22 Million Affected by OPM Hack, Officials Say*, retrieved from: http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

4. *The Commission on the Theft of American Intellectual Property*, retrieved from: http://www.ipcommission.org/

5. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, retrieved from: http://www3.nd.edu/~cpence/eewt/Owens2009.pdf

6. *Booby Trapping Software*, retrieved from: http://dl.acm.org/citation.cfm?id=2535824&dl=ACM&coll=DL&CFID=717474644&CFTOKEN=69961214

7. *Lifting the Veil on Cyber Offense*, retrieved from: http://www.computer.org/web/computingnow/0611/theme/securityandprivacy1

8. *Prosecuting Computer Crimes*, p. 180; retrieved from: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

9. *Is chasing cybercrooks worth it?* Retrieved from: http://www.cnn.com/2010/TECH/03/05/cyberattack.prosecute/index.html

10. *Autonomous Intelligent Agents in Cyber Offence*, Retrieved from: https://ccdcoe.org/cycon/2013/proceedings/d1r1s9_guarino.pdf

11. *Cyber Insecurity – Hacking Back*; Retrieved from: http://www.ft.com/cms/s/2/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.html

12. "Like comparable commercial products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities." Retrieved from: https://en.wikipedia.org/wiki/Metasploit_Project

13. *Booby Trapping Software*, Retrieved from: http://dl.acm.org/citation.cfm?id=2535824&dl=ACM&coll=DL&CFID=546712446&CFTOKEN=71045850

14. S Almutairi. *A new architecture for detecting DDoS/brute forcing attack and destroying the botnet behind*; retrieved from: http://aut.researchgateway.ac.nz/bitstream/handle/10292/7975/AlmutairiS.pdf?sequence=3

15. "We can actually set the machine on fire," said Dmitri Alperovitch, chief technology officer at CrowdStrike, who showed exactly how this kind of attack can be carried out on an Apple OS X computer. At this year's RSA Conference that company demonstrated a way to disable cooling fans while spiking the CPU of a Mac running OS X thus setting the computer on fire. Retrieved from: http://www.networkworld.com/article/2174737/security/rsa-security-attack-demo-deep-fries-apple-mac-components.html

16. *Battery Firmware Hacking*, retrieved from: https://media.blackhat.com/bh-us-11/Miller/BH_US_11_Miller_Battery_Firmware_Public_WP.pdf

17. Retrieved from: https://www.techopedia.com/definition/7786/internet-worm

18. Code Red, 2001 – Code Red infected computers running the Microsoft IIS Web server, exploiting a buffer overflow and defacing Web sites with the text, "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!" A fix had been available for this vulnerability for about a month, limiting its damage — kind of — to just **$2.6 billion**, but Code Red still managed to cause a "major disruption in connectivity," according to the Internet Storm Center. Retrieved from: http://www.itsecurity.com/features/10-worst-virus-attacks-111207/

19. MS Blaster, 2003 – Blaster spread via various Windows operating systems and targeted Microsoft's windowsupdate.com site with DoS (denial-of-service) attacks. It caused widespread trouble and multiple restarts in machines running Windows NT, Windows XP (64-bit) and Windows 2003. Victims included the Federal Reserve Bank of Atlanta, BMW AG, Philadelphia's City Hall, and thousands of home and corporate users. Although its ultimate origin was thought to be Chinese, the Blaster.B variant was created by then-18-year-old Jeffrey Lee Parson, who was caught because he programmed it to contact a domain registered to his father. Retrieved from: http://www.itsecurity.com/features/10-worst-virus-attacks-111207/

20. SQL Slammer, 2003 – This worm began using a buffer-overflow bug in Microsoft SQL Server and MSDE (Microsoft Desktop Engine) database products. It rapidly distributed copies of itself around the world, causing major denials of service and **slowing down the entire Internet**. An estimated 150,000 to 200,000 systems were affected. Retrieved from: http://www.itsecurity.com/features/10-worst-virus-attacks-111207/

21. *WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism*. Retrieved from: http://www.icir.org/vern/worm04/castaneda.pdf

22. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Retrieved from: http://www.pctools.com/security-news/zero-day-vulnerability/

23. *Internet attack traceback: cross-validation and pebble-trace*, retrieved from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4534481

24. *Cyber Insecurity – Hacking Back*; Retreived from: http://www.ft.com/cms/s/2/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.html

25. Retrieved from: https://nakedsecurity.sophos.com/2015/05/06/can-the-rombertik-malware-really-destroy-computers-no-no-three-times-no/

26. Retrieved from: http://www.webroot.com/blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/

27. Retrieved from: http://www.military.com/join-armed-forces/2014/05/14/80-of-military-recruitments-turned-down.html

28. Retrieved from: http://bgr.com/2014/05/14/time-spent-playing-video-games/

29. *National Security Threats in Cyberspace*, retrieved from: http://www.americanbar.org/content/dam/aba/migrated/natsecurity/threats_in_cyberspace.authcheckdam.pdf

30. *Snitching for Dollars: the Economics and Public Policy of Federal Civil Bounty Programs*; Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=221489

31. IRS, Pub. No. 733, *Rewards for Information Provided by Individuals to the Internal Revenue Service* (1997).

32. 42 USC §9609(d), 40 CFR §303.10 (1989).

33. 15 U.S.C. §78.

34. Tariff Act of 1930, 19 U.S.C. §1619 (1994).

35. Retrieved from: https://www.rewardsforjustice.net/english/index.html

36. *Dodge City* (1939), A Texas cattle agent witnesses first hand, the brutal lawlessness of Dodge City and takes the job of sheriff to clean the town up. Retrieved from: http://www.imdb.com/title/tt0031235/

37. NBC News, *University professor helps FBI crack $70 million cybercrime ring*, Wed Mar 21, 2012. retrieved from: http://rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring?lite

38. Black's Law Dictionary p. 989 (9th Ed. 2009).

39. Francis R. Stark, *The Abolition of Privateering and the Declaration of Paris*, 8 Studies in History, Economics and Public Law 227, 271 (1897).

40. Alberico Gentili, (January 14, 1552 – June 19, 1608) was an Italian lawyer, jurist, who served as the Regius professor of civil law at the University of Oxford for 21 years

41. Alberico Gentilli, *De Iure Belli Libri Tres* 423 (1612) (John C. Rolfe trans., William S Hein & Co. Inc. ed. 1995).

42. *Bring Back the Privateers*, retrieved from: http://iissonline.net/bring-back-the-privateers/

43. 43 U.S. (2 How.) 210, 232

44. *Accountability for International Crime and Serious Violations of Fundamental Human Rights: International Crimes: Jus Cogens and Obligation Erga Omnes,* 59 Law & Contemp. Prob. 63; "The term *jus cogens* means the compelling law and, as such, a *jus cogens* norm holds the highest hierarchical position among all other norms and principles. As a consequence of that standing, *jus cogens* norms are deemed to be peremptory and non-derogable. The international legal literature considers the following international crimes as *jus cogens*: aggression, genocide, crimes against humanity, war crimes, piracy, slavery and slave-related practices, and torture."

45. *Restatement (Third) of Foreign Relations of the United States* § 404 (1986). M. Cherif Bassiouni. (Autumn 1996) "*International Crimes: 'Jus Cogens' and 'Obligatio Erga Omnes'*." Law and Contemporary Problems. Vol. 59, No. 4, Pg. 68.

46. *Declaration Respecting Maritime Law*, Apr. 16, 1856, reprinted in 1 Am. J. Int'l L. 89 (Supp. 1907), retrieved from: http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=473FCB0F41DCC63BC12563CD0051492D. The relevant text of the declaration reads in pertinent part: "The above-mentioned Plenipotentiaries, being duly authorized, resolved to concert among themselves as to the means of attaining this object; and, having come to an agreement, have adopted the following solemn Declaration: 1. Privateering

is, and remains, abolished . . . ".

47. Joint Chiefs of Staff, Joint Pub. 1-02, *Dept. of Defense Dictionary of Military and Associated Terms,* at 41 (12 April 2001), retrieved from: http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(00).pdf

48. U.S. President Obama, *International Strategy for Cyberspace*, p. 9, 12; ("We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation . . .")

49. *Id.*

50. Ian Brownlie, *Principles of Public International Law* (5th ed., Oxford, 1998)

51. *Restatement (Third) of Foreign Relations of the United States* §404 (1986). Retrieved from: http://www.kentlaw.edu/faculty/bbrown/classes/IntlLawFall2007/CourseDocs/RestatementSources.doc.

52. Bernard H. Oxman, *Jurisdiction of States*, ¶22 *et seq*., retrieved from: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1436

53. *Ahlström and others v. Commission (In re Wood Pulp Cartel)*, joint cases 89/85, 104/85, 114/85, 116-17/85 and 125-9/85, 96 ILR 148 et seq. (1994).

54. 48 F.2d 416 (2d Cir. 1945)

55. http://www.senate.gov/artandhistory/history/common/briefing/Oath_Office.htm

56. *Let Privateers Marque Terrorism*, retrieved from: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1320&context=ilj

57. Elizabeth E. Joh, *The Paradox of Private Policing*, 95 J. Crim. L. & Criminology 50, 64 (2004).

58. Andrew DeForest Patrick, Note, *Running from the Law: Should Bounty Hunters Be Considered State Actors and thus Subject to Constitutional Restraints?*, 52 Vand. L. Rev. 171, 172 (1999).

59. *History, structure, and function of the Internet*, retrieved from: http://www.ncbi.nlm.nih.gov/pubmed/9579415

60. Retrieved from: http://secureknow.com/cybersecurity/how-to-change-your-ip-address/

57. Retrieved from: http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php

58. "The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction." Retrieved from: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

59. Retrieved from: http://www.submarinecablemap.com/

60. Retrieved from: https://www.arin.net/knowledge/rirs.html

61. "This French line of defense was constructed along the country's border with Germany during the 1930s and named after Minister of War André Maginot. . . The main fortifications on the northeast frontier included 22 large underground fortresses and 36 smaller fortresses, as well as blockhouses, bunkers and rail lines. Despite its strength and elaborate design, the line was unable to prevent an invasion by German troops who entered France via Belgium in May 1940." Retrieved from: http://www.history.com/topics/world-war-ii/maginot-line

62. The term “The Greatest Generation” is from Tom Brokaw's 1998 book: “[I]t is, I believe, the greatest generation any society has ever produced.” who fought not for fame and recognition, but because it was the “right thing to do.”

63. The Manhattan Project was a research and development project that produced the first nuclear weapons during World War II. Retreived from: https://en.wikipedia.org/wiki/Manhattan_Project.