Cyber Weapons and the U.S. Constitution

Neal Kushwaha
Founder and CEO, Impendo Inc., Ottawa, Canada
neal@impendo.com

Bruce W. Watson
Chief Scientist, IP Blox, Eindhoven, Netherlands
bruce@ip-blox.com

Abstract: Over the last few decades, several technology specialists have collected computer viruses and other malware. Today, if one desires, they can download current malware collections from Internet- based sources[1]. It could be argued that a large majority of older malware would not be as effective as the day they were written, due to the target systems of their time. But what if a nation state's tailored cyber weapons cache was copied and used against you, your fellow citizen, a corporation, your nation, or another nation?

The public perception of cyber weapons combined with the interpretation of the U.S. Constitution's Second and Fourteenth Amendments may lead the U.S. public to believe they have the right to bear "cyber" arms and use them. Upon establishing that U.S. citizens have these rights, this paper examines the possibility of cyber weapon storage regulations, the challenges of policing, and the potential international impact.

This position paper compares cyber weapons and their use with traditional firearms, allowing the reader to easily digest the contrasts and similarities. The paper further explores the complexities of cyber borders, attribution, harming unintended targets, the black letter rules of the Tallinn Manual, and more. Will these challenges influence U.S. law makers to possibly consider limiting the interpretation of the U.S Constitution's Amendments to explicitly exclude cyber weapons?

Keywords: *cyber weapons, U.S. constitution, second amendment, fourteenth amendment, cyber borders, weapons of mass interruption, weapons of mass manipulation*

1. INTRODUCTION

Nation states, news articles, academics, and the public are using terms to describe areas in the cyber domain such as "cyber attack", "cyberwarfare", and "cyber weapons". As exciting as these words may be, they carry consequence.

Exactly what is a "cyber weapon"? The U.S. Department of Defense does not have an official definition of the term.[2] After his keynote during the Q&A, at the 2018 McAleese Defense Programs Conference, U.S. Air Force Gen. Paul Selva stated:

> "*Cyber weapons do actual damage. …. Yet, we chose to call them non-kinetic. A non-kinetic strike from space that causes no damage on the planet, can cause unspeakable damage in the constellation. … So I'm not trying to be argumentative, but cyber's not a non-kinetic space.*" (Selva 2018)

If cyber weapons are to "cause injury or death to persons, or damage or destruction to objects" (Solis 2016), then they must compromise systems that impact human life, systems that manage critical infrastructure including nuclear or military facilities, government infrastructure, and the like. These types of weapons tend to be tailored or surgical weapons as opposed to those that are common malware.

The Tallinn Manual 2.0 rule 103 commentary 2 states "…cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack[3]." (Schmitt and Vihul 2017, 452)

In this paper, we examine the possibility that cyber weapons can be carried and possibly used by U.S. citizens under their constitutional rights. We break down the following five areas and summarize our thoughts.

1. collecting cyber weapons – similar to firearms, stocking or collecting cyber weapons may be a national right;

[1] Various blogs and online discussions offer access to malware collections (Malware Sample Sources for Researchers 2018).
[2] The terms "cyberspace", "cyberspace operations", and "cyberspace superiority" are the only terms that appear in the dictionary (DOD Dictionary of Military and Associated Terms, February 2018 2018).
[3] The Tallinn Manual 2.0 rule 92 states: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." (Schmitt and Vihul 2017, 415)

2. storage of cyber weapons – as with firearms and ammunition, what kind of logical and physical storage methods would be considered appropriate for cyber weapons?
3. defending boundaries – discussing how cyber borders aren't as clear as physical property lines and if it may be acceptable to use cyber weapons in self-defence?
4. proliferation of cyber weapons – policing challenges of when a cyber weapons cache is "copied"; and
5. international impact – discussing the potential perspectives of other countries.

2. RIGHT TO HAVE

The U.S. Constitution's Second Amendment states:

> "A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed." (Cornell Law School, Legal Information Institute n.d.)

Various rulings on the carrying and use of a stun-gun in the state of Massachusetts U.S., upon appeal, finally resulted the defendant Caetano being found not guilty.[4] The state argued that the stun-gun was not in use at the time the Second Amendment was enacted and therefore, was not a weapon that was covered under the amendment. However, upon appeal, the U.S. Supreme Court ruled that the second amendment extends to all weapons including ones that may not have existed at the time of enactment.

The U.S. Supreme Court also stated that the Second Amendment protects "arms" that were not invented or available when the Second Amendment was written, and that stun-guns could not be banned stating they could not be used in warfare. Oddly, it seems switchblades, knives, and other exotic weapons do not have the same protections and as a result are banned in some states.

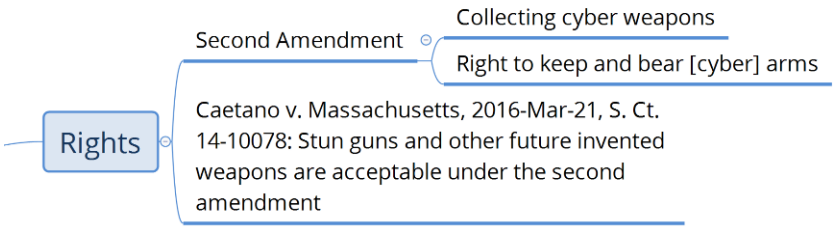


FIGURE 1: MIND MAP OF RIGHTS TO OWN CYBER WEAPONS

"Is Cyber Shape-shifting?" (Kushwaha and Watson 2018) discusses how malicious cyber behaviour is akin to espionage and sabotage, neither of which are considered an attack and therefore not resulting in any destruction. The cyber weapons were described as Weapons of Mass Interruption (WMI), Weapons of Mass Manipulation (WMM), and tailored or surgical weapons.

Extending the U.S. Supreme Court ruling to cyber along with the Law of Armed Conflict's interpretation of cyberwarfare and cyber attack[5], if one were to argue that certain cyber weapons cannot be used in warfare to cause mass destruction, then it may be possible that the citizens of the United States are able to use, "keep and bear [cyber] arms" as part of their constitutional rights.

3. STORAGE REGULATIONS

With the foundation that U.S. citizens maintain constitutional rights to bear cyber arms, would there be laws or possibly restrictions in place for the storage of these modern weapons?

In the U.S., laws regarding the storage of a common firearm varies from state to state.[6] For example, all firearms in the state of Massachusetts must be stored in a locked container with a tamper resistant lock. In other states, it is a crime to leave a loaded and unsecured firearm accessible to a minor. In such cases, leaving the loaded firearm in a drawer or a box in a closet is not an offence,

[4] Jaime Caetano had used a stun-gun in self-defence on her boyfriend who was abusing her (Caetano v. Massachusetts 2016).

[5] On pp680-681 in chapter "*Cyber Warfare*" of Solis' textbook, he discusses the definition of "*cyber attack*" and related behaviours under the Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL). It states: *"For both international and noninternational armed conflict, an excellent definition of a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects."* (Solis 2016, 680-681)

[6] The website of the Gifford's Law Centre to Prevent Gun Violence compares state level laws in the U.S. for the safe storage of firearms (Giffords Law Centre to Prevent Gun Violence n.d.)

but leaving it out on a table would be. A small number of states also require that the firearm be stored in a locked state, or a trigger lock as an example.

When applying this model to cyber weapons, residents of various states may be required to store them on disconnected networks. Generally, air gapped computing environments protect themselves from various forms of intrusion, however, in this case the air gapped device is protecting the connected devices. Such regulations would limit the option to store cyber weapons in the cloud.

Nevertheless, cloud storage could be an option in some states where the restrictions are not as strong. Cloud storage service providers such as Amazon, Microsoft, and Google (as a small few examples) may be unwilling to store cyber weapons in conventional cloud storage spaces due to various reasons including liability concerns. If cloud storage of cyber weapons is an option, restrictions (such as encryption) that are adequate for data at rest, may be imposed.

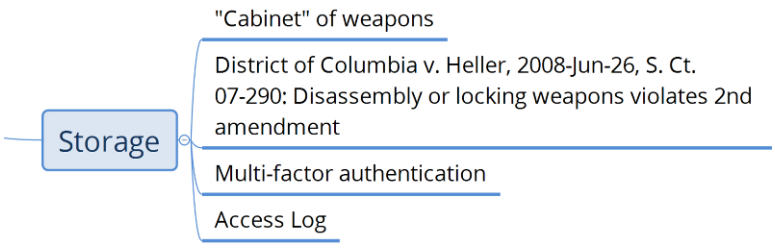


FIGURE 2: MIND MAP FOR THE STORAGE OF CYBER WEAPONS

Other states may also require cyber weapons cache storage to use multi-factor authentication in the form of something you know (example, a password), and something you have (example, a key card or biometrics). This would deter intruders and limit undesired remote access to the cyber weapons cache.

In addition to both air gapped and multi-factor authentication levels of controlled access to stored cyber weapons, various states may also require a regularly maintained access log. Such access logs could be reviewed by third parties or governing bodies to ensure that the cyber weapons cache has been only accessed by the individuals that are authorized to do so, which raises the question – who should have access to the cyber weapons cache?

Just because a family lives together, does that authorize the entire family to access the cyber weapons? Do they know and understand the various implications of their handling and use? These thoughts tend to lead to user training but are also applicable in relation to storage. Similar to keeping firearms out of a child's reach, should these cyber weapons be locked in cabinets or would it be adequate to store them on a computer or USB drive (as an example) and leave these on a table in your home?

As it pertains to data theft, an argument could be presented that a password protected and data encrypted computer or an encrypted external storage device such as a USB drive, is already equivalent to a locked storage container. This would not be the same for physical security concerns regarding theft of the IT equipment.

Oddly, relying on protecting cyber weapons using encryption, passwords, biometrics, or other means, may be considered ineffective as these safeguards are the targets some cyber weapons are designed to compromise.

It is unlikely that various states will require that cyber weapons be stored in a disabled or dismantled state, which for data at rest could be equivalent to encryption. It will also be unlikely for states to limit the carrying of cyber weapons in either active computers or on storage devices. That's because in June of 2008, a Supreme Court decision regarding the District of Columbia v. Heller described that keeping traditional guns unloaded, trigger locked, or disassembled in their home for the purpose of self-defence is a violation of their Second Amendment rights (District of Columbia et al. v. Heller 2008).[7]

4. RIGHT TO USE

Like any weapon, cyber weapons can be used for a variety of reasons. A common reason that tends to surface when justifying the use of a firearm is self-defence. When reviewing the Second Amendment, "the right of the people to keep and bear arms" to ensure the "security of a free state", the idea of self-defence is likely better supported in conjunction with the U.S. Constitution's Fourteenth Amendment:

[7] The U.S. Supreme Court ruling regarding the District of Columbia et al. v Heller (District of Columbia et al. v. Heller 2008) was a precedent setting case which resulted in various lawsuits against other states (Wikipedia 2018).

> "…No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law." (Cornell Law School, Legal Information Institute n.d.)

With respect to a substantive due process claim[8], or the infringement of a citizen's rights not specified in the U.S. Constitution, there are three key major components that must be met:

1. One must be deprived, as it applies to;
2. life, liberty, or property; and
3. with evidence that the government has no justification for depriving those rights.

One could present that self-defence is required in order to protect human life when they believe it is being deprived. Therefore, owning weapons, or cyber weapons, for merely the purpose of self-defence could be a fundamental right.

What if citizens of the U.S. feel they are unable to defend themselves via kinetic means? Does it mean they are not allowed the right to defend themselves? With the fundamental right to self-defence, one could argue that the use of cyber weapons cannot be limited or excluded. In line with firearm ownership, as long as one does not pose any danger to other people who are not a threat to society, they can essentially own cyber weapons.

Couple the right to defend using non-kinetic means with the difficulty of qualifying cyber borders and we have a very complicated problem. Where do cyber borders begin for nation states? The idea that they align with property borders or traditional geographical borders is not widely agreed upon.[9]

For interconnected devices, it may be claimed that cyber borders are at the point of where the package (or group of packets):

1. leaves the source's IT asset;
2. leaves the last IT asset that belongs to the source (example, a router or switch or firewall);
3. leaves the country's last IT asset;
4. enters the destination country's first IT asset;
5. enters the destination's first IT asset (example, a router or switch or firewall);
6. enters the destination's target device (example, a computer or mobile device or other IoT); or
7. is activated at the destination's target device.

The border examples described above are easily digested for interconnected devices, however, how would borders apply when it comes to electronic emanations?

It is considered common tradecraft to be able to read video signals from one's computer as they emanate from the video card[10]. If one were to intercept these signals as they radiate in a 3-dimentional space around a computer (spatially radiated signals), then one could see exactly what another is viewing on their display. The same can be done for keyboard[11], Wi-Fi, Bluetooth, cellular[12], keypads, and other emanations. When considering the radio frequencies and electro-magnetic signals emanating from a technology device, where do the cyber borders lie?

What if it is a little more complicated whereby signals are being picked up by way of conducted emanations from a copper pipe within a wall, as an example, that carries the original signal beyond the effective distance of spatial emanations? Where do the cyber borders lie when intercepting these signals?

---

[8] In the Touro Law Review, Chemerinksy states "when the government deprives a person of life, liberty, or property, is its actions justified by adequate reason[?] This means that if the Government takes away somebody's liberty in an arbitrary or capricious manner, it is a violation of substantive due process." (Chemerinsky 1999)

[9] See chapter "Borders in Cyberspace: Can Sovereignty adapt to the challenges of Cyber Security" in the book "The Virtual Battlefield: Perspectives on Cyber Warfare" (Hare 2009) and rule 81 commentary 2 of the Tallinn Manual 2.0, a rule notably written to apply during armed conflict, states "Restrictions based on geographical limitations may be particularly difficult to implement in the context of cyber warfare." (Schmitt and Vihul 2017, 378-379)

[10] For his Doctoral dissertation, Markus Kuhn researched compromising emanations from display cards (Kuhn 2003).

[11] At the USENIX Security Symposium in 2009, Martin and Sylvain described their research and method for capturing compromising emanations from wired and wireless keyboards (Vuagnoux and Pasini 2009).

[12] At Defcon 18, Chris Paget presented a hands-on case where he used a low cost and low-powered software defined radio and opensource software to intercept cellular traffic and capture a database of mobile device International Mobile Subscriber Identities (IMSI) (Paget 2010).

Consider another scenario where a drone is flying overhead in a public space. Then, with a radio frequency device, one is able to (1) delay or (2) terminate the communications between the remote controller and the drone. Would either action be equivalent to stepping over cyber borders?[13]

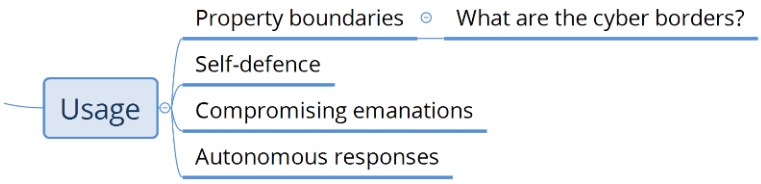


FIGURE 3: MIND MAP OF THE RIGHT TO USE CYBER WEAPONS

The self-defence argument may be difficult to defend. That's because when one claims self-defence with respect to the use of their firearm, it is generally in response to an immediate threat to life. When it comes to manually responding with a cyber weapon, one will likely have adequate time to make better decisions with sound mind and contact police or federal authorities.

Let's consider a cyber hostile has breached one's cyber border and is attempting to cause harm. Could an automated response to such a hostile event be considered self-defence? Let's complicate the example further with the automated response being generated from other known compromised computers in the region or around the globe, such that when some hostile crosses one's border, the response to the hostile is now coming from several unrelated devices. Worse, the attribution could be falsely positioned on others, leaving the owner of the automated cyber weapon response to defend the reason for their cyber hostile behaviour, or possibly exercising self-defence against a proxy.

Autonomous responses are not new in the cyber domain. When one party receives unsolicited commercial email (or email spam), their Unified Threat Management (UTM) and/or Email Security Appliance (ESA) automatically flags the IP address and likely also the originating domain. The UTM/ESA may also be configured to share the hostile's IP address and domain to a private authority, as a collective, to which others subscribe. The subscription service allows others to proactively defend against possible future malicious cyber activity. This autonomous chain of events is very similar to the concept of an autonomous self-defence response.

The Tallinn Manual 2.0 covers self-defence as it relates to a nation state specifically under rules 71 through 75 but not as it relates to an individual defending themselves or their nation state (Schmitt and Vihul 2017, 339-356).

5. POLICING

When it comes to a firearm and bullets, the police are well trained and very skilled in dealing with serial numbers, gunshot residue, unique striations, and more. As for cyber, the federal entities have skilled cyber forensic capability, likely due to the knowledge from the federal law enforcement agencies, but how well does this skill translate down to the state and municipal police levels? In the U.S. some states have developed their own cyber task forces or commands, while all states and others have joined a sharing and cyber analysis initiative.[14]

Notably, the Tallinn Manual's rule 103 distinguishes between a "method" and "means" of cyber warfare (Schmitt and Vihul 2017, 452-453). Consider this example where a hostile would use both:

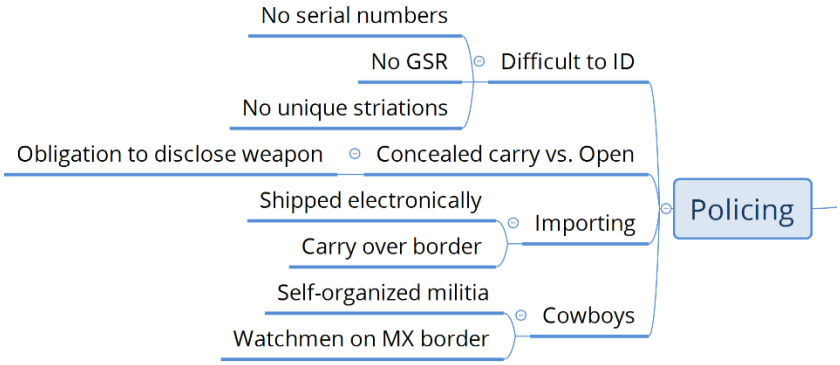
1. A hostile requests multiple free email accounts without any legitimate personal information;
2. Online, the same hostile procures pre-paid credit cards (commercially known as VISA, Mastercard, and AMEX gift cards) from various countries;
3. Using the free email accounts and pre-paid credit cards, the hostile subscribes to virtual hosting through multiple small-entity cloud service providers in these various countries (example: 5 virtual hosts across 5 countries);

[13] See the Popular Science article describing DroneShield's Dronegun which uses radio frequencies to down a drone (Atherton 2016).

[14] Idaho (Executive Order No. 2015-07: Establishing the Idaho Cybersecurity Cabinet Taskforce 2015), Michigan (Cyber Section, Michigan State Police n.d.), New York (Governor Cuomo Announces Cyber Security Advisory Board 2013), and Rhode Island (Executive Order 15-10: Rhode Island Cyber Security Commission 2017), Virginia (Commonwealth of Virginia Cyber Security Commission n.d.) are examples of some states that have setup their own cyber advisory board, cyber commission, or cyber task force. All U.S. states, all U.S. territories, and many municipal governments, and tribal nations participate in the Multi-State Information Sharing & Analysis Centre (MS-ISAC) (Multi-State Information Sharing & Analysis Centre n.d.). The U.S. National Fusion Centre Association (NFCA) is another federal and state level intelligence and information sharing example (National Fusion Centre Association n.d.).

   a. As required, the hostile instantiates a virtual host from a pool of memory, CPU, disk, and IP addresses from the cloud provider;
   b. At the hostile's request, the operating system instances are destroyed, and all resources are returned to the cloud provider pool for other clients to use;
4. The hostile installs their own operating systems on each of the 5 virtual hosts (example, a Linux variant using scripts);
5. The hostile jumps from their first instantiated virtual host to the second, third, fourth, and fifth host all located in different countries;
6. The hostile performs their malicious activity from the final virtual host and promptly disconnects from all hosts, thereby triggering a deletion of all virtual hosts and returning all resources into the provider's resource pool.

7.



8. **FIGURE 4: MIND MAP OF CYBER WEAPONS POLICING CHALLENGES**

Using small-entity hosting providers allows the hostile to leverage the likely poor logging policies or possibly overwriting of log files, lowering their risk of being traced. How is a municipal police service able to trace the true attribution? The last virtual host could be located in the same country as the target or a completely unique country that may be a commonly named cyber attribution source in the world. Depending on federal level authorities to deal with all cyber cases is not reasonable. If the example of virtual host hopping becomes normal behaviour, investigation alone could overwhelm federal authorities.[15]

Various states have laws defining the concealed carry versus open carry rights for firearms. In relation to cyber, would individuals be required to disclose that their computer or mobile phone, as examples, have cyber weapons prior to connecting to a public Wi-Fi hotspot?

Knowing that planes are susceptible to certain cyber hacks[16], would there be any requirement to disclose to authorities that your computer or mobile device has cyber weapons while traveling on a plane? What about when driving across geographical borders, would individuals need to disclose to authorities that they carry cyber weapons with them?

Similarly, imagine a future where autonomous (or semi-autonomous) vehicles are widely used. It may be possible that a cyber weapon could be used to disable sensor readings on a nearby autonomous vehicle resulting in a collision. Although one may argue that the vehicle's software should have had better cyber hygiene, the result is still a collision.

Would the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) take on the responsibility of protecting the US from the risk to public safety caused by illegal trafficking of cyber weapons as they do for traditional firearms?[17] Considering individuals can import cyber weapons using electronic means, how could such protections be put in place? For more complex off-line cyber weapons, one could travel to the other party and import cyber weapons by carrying them over the border in a portable disk drive, as an example.

If the U.S. Customs and Border Protection were to search for cyber weapons in all technology devices as they enter or depart the U.S. geographical borders, the effort would become unmanageable. Equally, importers or exporters of cyber weapons would most likely not notify authorities of their transactions. Having rules without consequences or the ability to police them is not an effective way to manage the law.

[15] Reports of U.K. police face delays of up to 12 months to analyze cyber crimes (Peachey 2015).
[16] Keynote speaker of the 2017 CyberSat Summit in Virginia, Dr. Robert Hickey, described how the Department of Homeland Security (DHS) successfully "accomplished a remote, non-cooperative, penetration" (Biesecker 2017) of a commercial Boeing 757 on September 21, 2016.
[17] The mission of the ATF is described on their "Who We Are" webpage (Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) n.d.).

The idea of policing may also extend beyond authorized agencies and services. In Arizona, the Arizona Border Recon, a volunteer militia group founded by Tim Foley, patrol the U.S. and Mexico border dressed in camouflage and armed with firearms (Carranza 2017). They do not have federal authority to behave in a policing manner, at the same time they are not listed on any U.S. anti-government militia list. They were featured on Netflix in a 2015 documentary called "Cartel Land".

> "*I'm down here to defend my country from whoever is coming across that border.*" – Mike LaMarte (Carranza 2017)

If vigilantes defending a geographical border is socially accepted, where could this lead when vigilantes or militias defend cyber borders?

6. INTERNATIONAL IMPACT

It is well known in the intelligence community that certain countries have successfully accomplished international disruption using HUMINT. Countries that didn't have the funding and capability to perform espionage and sabotage, likely suffered. Today, cyber allows all countries to perform on a near equal playing field. Adversary countries can do a variety of things to confuse the impacted party in believing the source of the cyber behaviour is from a completely different country, thus complicating any potential kinetic response.

Without the need to share any attribution data, targeted countries can easily declare the source of the disruptive cyber event as the country of their choice.

The laws around firearms and cyber arms across the various countries complicate travel and arms trades. The position that some U.S. citizens may take with respect to cyber weapons in relation to the Second and Fourteenth Amendments to the U.S. Constitution are certainly unique compared to other countries around the globe. When a U.S. citizen travels to another country where the laws surrounding cyber weapons are far stricter, could they be charged for carrying cyber weapons on their computers and mobile devices? Would countries with stricter laws limit access to cloud repositories with cyber arms? How would that be enforced?

Someday, one may be able to download cyber weapons from Internet sources[18]. Could downloading cyber weapons become the new method to perform arms trade? Leaning on the idea that cyber weapons are designed to take apart the security applied to safeguard data, how safe are cyber weapons stores and could they be stolen and even mass-distributed?

The idea that one could write targeted cyber weapons, or learn to write them, and share it globally thereby resulting in causing harm to many is not far from reality. So even if a country does have stricter laws regarding the importing, ownership, and use of cyber weapons, developers within their borders could write their own cyber weapons.

Conventional weapons (or arms), such as those covered under the UN Convention on Certain Conventional Weapons (CCW), the Arms Trade Treaty (ATT), or the Wassenaar Arrangement do not explicitly cover cyber weapons, however, they are not excluded either. In 1980, when the UN Convention on CCW[19] was adopted, or in 1996, when the Wassenaar Arrangement was approved by 33 founding countries, cyber weapons were not part of our vocabulary.

The Tallinn Manual 2.0 rule 151 commentary 5 through 7 covers a specific condition of the transfer of cyber weapons through neutral territory during armed conflict, and notably there is no mention or reference to the Wassenaar Arrangement (Schmitt and Vihul 2017, 557).

In the last few decades, cybercrimes have most certainly displayed indiscriminate direct and indirect effects. From Stuxnet[20], Shamoon, KillDisk, BlackEnergy[21], and advanced persistent threat actors impacting the energy sector and power grids, other cyber weapons and hostiles may target healthcare sector, the financial sector, or the defence.

---

[18] Shadow Brokers released 300 MB of NSA tools for download (Goodin 2017), however Microsoft was able to manage those exploits within short order (Microsoft Security Response Centre 2017). The NSA's Tailored Access Operations (TAO) group alleged that 75% of their library of hacking tools (equivalent to about 50 TB) was copied and taken off-site somewhere between 2012 and 2015 (Nakashima 2017). It is unknown if and how many other individuals or parties may have copies.

[19] The full name of the CCW is "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects" (The Convention on Certain Conventional Weapons, n.d.).

[20] Lagner dissects Stuxnet in his paper "Stuxnet: Dissecting a Cyber weapon" (Langner 2011).

[21] Zetter describes the vector of attack and its impact on Ukraine and Russia's power substations (Zetter 2016) while the SysAdmin, Audit, Network and Security Industrial Control Systems (SANS ICS) and Electricity Information Sharing and Analysis Center (E-ISAC) analyse the attack and techniques (Case Defense Use 2016)

One could indirectly cause injury or possibly death using cyber by simply performing the following act: Post an anonymous notice on a local Kijiji board with a photo, address, vehicle, and description of a target living in the local area and claim they are a paedophile. The indirect impact of such a malicious cyber activity could include the target being investigated by police services to loss of the target's reputation, job, their children, or spouse. In addition to that, the target may be beaten or killed by citizens who feel the need to take matters in their own hands.

Imagine if this were to occur at a large scale, to many targets in the same city, at the same time, such that the effort to investigate fabricated claims consumes police services resources. Could it be possible to cripple the budgets of public safety related services using such methods? As an impact to the targets, even if the evidence is proven to be false by the police services, the target's reputation may not survive in the long term.

FIGURE 5: MIND MAP OF INTERNATIONAL IMPACT

Malicious cyber weapons targeted at an international community may possibly spread to a much wider audience with little ability to control it. Cyber weapons of mass manipulation such as NotPetya and other ransomware may have been directed at a particular country such as Ukraine, however, it spread to countries in Europe and North America. [22]

International relations will become very tense if a U.S. citizen feels they are within their constitutional rights to defend their country against international cyber threats and decide to use their cyber weapon(s) to disrupt another country's device(s).

7. CLOSING

This position paper explores cyber weapons and the challenges we may face when trying to manage them like traditional firearms. The paper opens with the discussion of the Second Amendment of the U.S. Constitution, stating it could be argued that owning cyber weapons is a U.S. constitutional right.

Upon establishing that citizens have the right to own cyber weapons, we explored the possibility of regulating their storage in an encrypted state or air-gapped networks, however, U.S. case law may be used to argue that any storage regulation is unlawful as per the U.S. Constitution.

Without any storage requirements, we discussed cases where there may be a right to use cyber weapons. The Fourteenth Amendment of the U.S. Constitution may be used to support an argument of self-defence. We then discussed how cyber borders are very vague and not as clear as geographical borders. We then explained how the cyber domain is already equipped with autonomous responses and that autonomous cyber responses to malicious cyber events could be argued as acceptable.

We went on to present the challenges with policing and managing cyber weapons. We discussed the application of these cyber weapons by possible vigilante or militia groups that may defend their cyber borders using cyber weapons similar to how certain groups defend the U.S. border with Mexico.

Finally, we explored the possible international impact. We discussed how cyber weapons are not explicitly described in the Arms Trade Treaty, the UN Convention on Certain Conventional Weapons, or the Wassenaar Arrangement, but their language may

[22] Wikipedia page that describes the behaviour and impact of Petya, NotPetya, and other variants of the ransomware (Wikipedia 2018).

include them. We discussed how the collateral impact of slightly targeted cyber weapons have resulted in a wider than intended scope of impact.

When cyber weapons become an active part of the larger defence industry, we may see companies develop cyber weapons solely for financial gain. We may see their inclusion in the International Traffic in Arms Regulation[23] (ITAR). ITAR already has the history of classifying cryptography as arms and has applied export regulation to software that includes such capability.

U.S. companies that design and manufacture complicated and surgical/tailored cyber weapons could be subject to the regulations of ITAR. Autonomous cyber weapons could be coupled with hardware and be offered as an appliance to existing networks. Users of these appliances could opt-in to support vigilante style counter attacks when one of the appliances in the network makes such a request. The sale of these autonomous cyber weapons could become an entire industry similar to that of firearms. Unfortunately, with the simplicity to alter the source of the malicious activity to make it seem as though it is originating from other sources, including government sources, the joint autonomous response from such a network of appliances could end up harming innocent targets.

What will our future look like with cyber weapons if rapid self-defence becomes common place? Will we as citizens be forced to defend ourselves, similar to what was called the *Wild West* or, will governments and international communities respond with better legislations and laws?

8. ACKNOWLEDGEMENTS

Special thanks to Tomáš Minárik and Raik Jakschis for their valuable input.

9. REFERENCES

Atherton, Kelsey. 2016. *This drone gun knocks drones out of the sky gently, with radio waves*. 28 November. Accessed February 19, 2018. https://www.popsci.com/drone-gun-downs-drones-with-radio-waves.

Biesecker, Calvin. 2017. *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*. 8 November. Accessed February 19, 2018. http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/.

Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). n.d. *Who We Are*. Accessed February 19, 2018.

Caetano v. Massachusetts. 2016. 14-10078 (Supreme Court of the United States, Ashland, Massachusetts, USA 21 March). Accessed February 19, 2018.

Carranza, Rafael. 2017. *Border vigilantes, and the wall they might be watching*. 22 September. Accessed February 19, 2018. https://www.usatoday.com/border-wall/story/vigilante-militia-patrol-us-mexico-border/559753001/.

Case Defense Use. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center (E-ISAC). Accessed February 19, 2018. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Chemerinsky, Erwin. 1999. "Substantive Due Process." *Touro Law Review* 1501-1534. Accessed February 19, 2018. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1638&context=faculty_scholarship.

n.d. *Commonwealth of Virginia Cyber Security Commission*. Accessed February 19, 2018. https://cyberva.virginia.gov/.

Cornell Law School, Legal Information Institute. n.d. *Fourteenth Amendment | Constitution | US Law | Legal Information Institute*. Accessed February 19, 2018. https://www.law.cornell.edu/constitution/amendmentxiv.

—. n.d. *Second Amendment | Constitution | US Law | Legal Information Institute*. Accessed February 19, 2018. https://www.law.cornell.edu/constitution/second_amendment.

n.d. *Cyber Section, Michigan State Police*. Accessed February 19, 2018. www.michigan.gov/msp/0,4643,7-123-72297_72370_72379---,00.html.

[23] ITAR is part of the U.S. Arms Export Control Act (AECA) (The International Traffic in Arms Regulations (ITAR) n.d.)

District of Columbia et al. v. Heller. 2008. 07-290 (Supreme Court of the United States, 26 June). Accessed February 19, 2018.

2018. "DOD Dictionary of Military and Associated Terms, February 2018." *U.S. Joint Chiefs of Staff.* 21 February. Accessed February 21, 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-02-21-153603-643.

2017. "Executive Order 15-10: Rhode Island Cyber Security Commission." *State of Rhode Island.* 7 May. Accessed February 19, 2018. www.governor.ri.gov/documents/orders/ExecOrder_15-10_05072015.pdf.

2015. "Executive Order No. 2015-07: Establishing the Idaho Cybersecurity Cabinet Taskforce." *State of Idaho.* 15 July. Accessed February 19, 2018. https://gov.idaho.gov/mediacenter/execorders/eo15/7.15.15%20Cybersecurity%20Taskforce.pdf.

Giffords Law Centre to Prevent Gun Violence. n.d. *Safe Storage.* Accessed February 19, 2018. http://lawcenter.giffords.org/gun-laws/policy-areas/child-consumer-safety/safe-storage/.

Goodin, Dan. 2017. *NSA-leaking Shadow Brokers just dumped its most damaging release yet.* 4 April. Accessed February 19, 2018. https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

2013. *Governor Cuomo Announces Cyber Security Advisory Board.* 10 May. Accessed February 19, 2018. https://www.governor.ny.gov/news/governor-cuomo-announces-cyber-security-advisory-board.

Hare, Forrest. 2009. "Borders in Cyberspace: Can Sovereignty adapt to the challenges of Cyber Security?" In *The Virtual Battlefield: Perspectives on Cyber Warfare*, by Christian Czosseck and Kenneth Geers, edited by Christian Czosseck and Kenneth Geers, 88-105. Amsterdam: IOS Press. Accessed February 19, 2018.

Kuhn, Markus. 2003. "Compromising emanations: eavesdropping risks of computer displays." *University of Cambridge.* Accessed February 19, 2018. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf.

Kushwaha, Neal, and Bruce Watson. 2018. "Is Cyber Shape-shifting?" *Civil-Military Symposium 2017.* Dahlonega, GA: University of North Georgia. Accessed February 19, 2018.

Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security & Privacy* 9 (3): 49-52. Accessed February 19, 2018.

2018. *Malware Sample Sources for Researchers.* 10 January. Accessed March 30, 2018. https://zeltser.com/malware-sample-sources/.

Microsoft Security Response Centre. 2017. *Protecting customers and evaluating risk.* 14 April. Accessed February 19, 2018. https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/.

n.d. *Multi-State Information Sharing & Analysis Centre.* Accessed February 19, 2018. https://www.cisecurity.org/ms-isac/.

Nakashima, Ellen. 2017. *Prosecutors to seek indictment against former NSA contractor as early as this week.* 6 February. Accessed February 19, 2018. https://www.washingtonpost.com/world/national-security/prosecutors-to-seek-indictment-against-former-nsa-contractor-as-early-as-this-week/2017/02/06/362a22ca-ec83-11e6-9662-6eedf1627882_story.html.

n.d. *National Fusion Centre Association.* Accessed February 19, 2018. https://nfcausa.org/.

Paget, Chris. 2010. "Defcon 18: Practical Cellphone Spying." *YouTube.* 31 July. Accessed February 19, 2018. https://www.youtube.com/watch?v=DU8hg4FTm0g.

Peachey, Paul. 2015. *Cyber crime victims refuse to hand over computers for police analysis as backlog creates year-long delays.* 22 December. Accessed February 19, 2018. http://www.independent.co.uk/news/uk/crime/cyber-crime-victims-refuse-to-hand-over-computers-for-police-analysis-as-backlog-creates-year-long-a6783671.html.

Schmitt, Michael N., and Liis Vihul, . 2017. *Tallinn Manual 2.0 on the Internation Law Applicable to Cyber Operations.* Cambridge University Press. Accessed March 30, 2018.

Selva, Paul J. 2018. *Gen. Selva's Remarks and Q&A at the McAleese Defense Programs Conference.* 6 March. Accessed March 30, 2018. http://www.jcs.mil/Media/Speeches/Article/707467/gen-selvas-remarks-and-qa-at-the-mcaleese-defense-programs-conference/.

Solis, Gary. 2016. *The Law of Armed Conflict: International Humanitarian Law in War*. 2nd. Cambridge: Cambridge University Press. Accessed February 19, 2018.

n.d. *The International Traffic in Arms Regulations (ITAR).* Accessed February 19, 2018. https://www.pmddtc.state.gov/regulations_laws/itar.html.

Vuagnoux, Martin, and Sylvain Pasini. 2009. "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards." *USENIX Security Symposium.* Montreal. Accessed February 19, 2018. https://www.usenix.org/legacy/events/sec09/tech/full_papers/vuagnoux.pdf.

Wikipedia. 2018. *District of Columbia v. Heller.* 5 February. Accessed February 18, 2018. https://en.wikipedia.org/wiki/District_of_Columbia_v._Heller.

—. 2018. *Petya (malware).* 18 February. Accessed February 19, 2018. https://en.wikipedia.org/wiki/Petya_(malware).

Zetter, Kim. 2016. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired.* 6 March. Accessed February 19, 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

