Is Cyber Shape-shifting?

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: Technologies have evolved so rapidly that companies and governments seem to be regularly trying to catch up to new capabilities and thereby making quick decisions that have the potential to set precedents and present international challenges.[1] Is cyber capability changing so fast that our sensemaking is lagging? Is cyber shape-shifting?

With the opportunity to a take step away from the technical aspects of cyber and consider the taxonomy, this paper explores the domain of cyber by structuring the conceptual problems and by putting the individual small solutions into their respective places within a conceptual framework.

The paper breaks cyber into seven (7) concepts and discusses each of them:

1. knowledge trajectory – aligning cyber to knowledge economies;
2. discrimination – categorizing various cyber weapons;
3. recombinant and mutable – discussing how cyber weapons can be easily modified when compared to traditional kinetic weapons;
4. model/object dichotomy collapse and free replication – discussing how in cyber, the code is the object, making it easy to duplicate the weapon and how traditional methods of sanctions may no longer be suitable;
5. speed of light – the challenge of detecting cyber weapons and the ease with which they can be shared;
6. dynamic multidimensional space – discussing the change in theatre of operations and how collateral damage is an expected outcome; and
7. scope of impact – discussing the true impact of cyber weapons and their behaviour.

The paper challenges the reader further by proposing the possibility that cyber is not a Domain of Warfare and that the term "cyber attack" may likely benefit from an alternate label such as "cyber espionage" or "cyber sabotage". We discuss how cyber is impaired by:

1. attribution, making it difficult to identify the source;
2. scope of impact resulting in manipulation, interruption/disruption, and bullying; and
3. highly dependent on the target's cyber hygiene and IT business processes.

Because of these challenges, we propose cyber is rather simply a tool or tradecraft for the purpose of espionage or sabotage.

Keywords: *capability and maturity model integration, cyber hygiene, cyber weapons, espionage, knowledge economies, knowledge trajectory, tradecraft, weapons of mass interruption, weapons of mass manipulation*

1. INTRODUCTION

In the Cyber Domain, nearly every criminal act is described as an "attack". Over the past few decades, numerous claimed "cyber attacks" have been carried out by various sources with various degrees of impact and using various vectors of attack.[2] But is it suitable and widely accepted to classify these attacks[3] in cyber as a Domain of Warfare?[4]

The evolution of technology on both the hardware and software sides has been widely embraced around the globe. The prevalence of Internet based services and the desire to be constantly connected to one another is an unstoppable energy. Although a war could

[1] The Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States (January 5, 2017), p5 paragraph 1 states *"…countries do not widely agree on how such principles of international law as proportionality of response or even the application of sovereignty apply in cyberspace."* (Clapper, Lettre and Rogers 2017)

[2] Middleton (Middleton 2017), NATO Review Magazine (NATO Review Magazine 2013), and Vaidya (Vaidya 2015), each describe the history of cyber crime activities.

[3] In Schmitt's paper, he examines the meaning of "*attack*" (Schmitt 2012) as it applies to Cyber Operations and International Law.

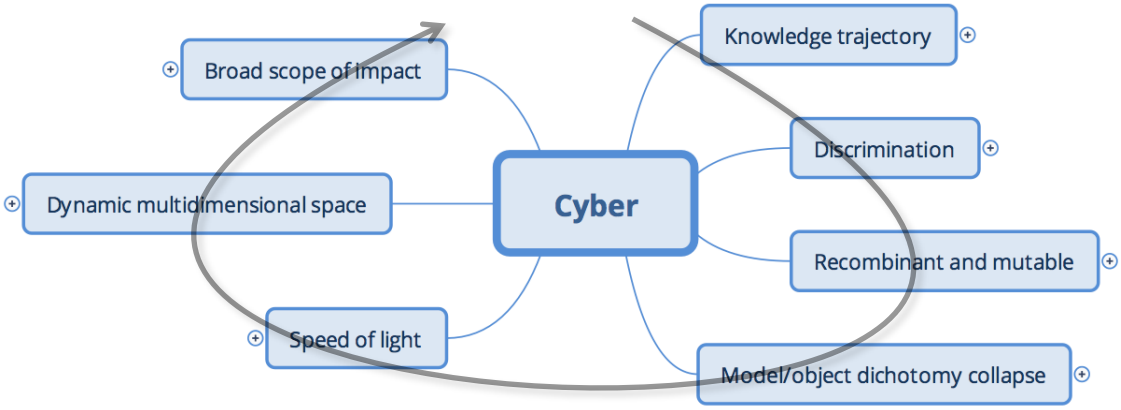
[4] On pp680-681 in chapter "*Cyber Warfare*" of Solis' textbook, he discusses the definition of "*cyber attack*" and related behaviours under the Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL). It states: *"For both international and noninternational armed conflict, an excellent 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)
The following paragraph states: *"…cyber theft, cyber intelligence gathering, and cyber intrusions that involve brief or periodic interruption of nonessential cyber services clearly do not qualify as cyber attacks."* (Solis 2016, 680-681)

take place in this space, the decision to declare this space as a Domain of Warfare must not be taken hastily. One may be able to injure or kill one another with a fork or a spoon, but it most likely does not mean we create a Domain of Warfare for Utensils.

NATO[5] (defensive only) and various nations[6] have already stood up Cyber Operations[7] and/or Cyber Commands[8] in light of the trend, coining cyber or cyberspace as a Domain of Warfare among land, maritime/sea (including surface and subsurface), air, and space. Considering cyber spans all domains, the driving governance behind these organizations or branches must be well defined.

In an effort to give cyber a proper comparison to traditional kinetic warfare, this paper explores the taxonomy of cyber to help provoke thought. Although the paper does not deliver a definitive conclusion or present qualitative test results, it does encourage the reader to study the presented concepts in a different way that may change the way we perceive and consider cyber operations. To tackle this task, the paper discusses seven (7) concepts that encompass the cyber domain. The concepts labelled in the mind map of Figure 1 below are the header for each section of the paper. Each concept of cyber branches further into a hierarchy of ideas that are discussed in detail throughout this paper.

FIGURE 1. MIND MAP OF CYBER OPERATIONS



2. KNOWLEDGE TRAJECTORY

The maturity of any discipline can be described into a trajectory of knowledge. When exploring the cyber domain, we can appreciate that only a few, if any, have mastered it. Table 1 below shows the five stages of knowledge economies as described by the second author (Watson); that work in itself an extension of the discussion in the book "*Software Architecture: Perspectives on an Emerging Discipline*" (Shaw and Garlan 1996, 8).

Art: When painting, each artist has their own representation of the scene, resulting in significantly different paintings. Advanced persistent threats (APT) are a form of an art. It takes a skilled resource that has rare and unique talents to be able to be an advanced persistent threat. Each APT behaves differently from another when applying their unique talents.

Craft: Groups such as CIRCs[9] and CERTs[10] and those that create cyber weapons tend to depend on a model of sharing information. The notion of master and apprentice is normally applied to sharing a craft and can be seen in the cyber world when a student learns from a teacher using online videos thereby creating consistent teaching. These groups of masters and apprentices create towers of knowledge and/or styles.

[5] Paragraphs 5 and 6 describes *"NATO's [cyber] defensive mandate"* and that the allies *"recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea"* (Minárik 2016).
[6] Joint Statement for the Record to the Senate Armed Services Committee (January 5, 2017), p5 paragraph 2, *"As of late 2016, more than 30 nations are developing offensive cyber attack capabilities."* (Clapper, Lettre and Rogers 2017)
[7] Communications Security Establishment Act, subsection Mandate, paragraph 19 *"Defensive cyber operations"* and paragraph 20 *"Active cyber operations"* (House of Commons of Canada 2017)
[8] In paragraph 1 of a memo to the Secretary of Defense, President Trump states: *"…I direct that U.S. Cyber Command be established as a Unified Combatant Command."* (Trump 2017)
[9] Examples of CIRCs: Canada Cyber Incident Response Centre (Public Safety Canada 2016) and NATO Computer Incident Response Capability (NATO Communications and Information Agency 2016)
[10] Examples of CERTs: US (US-CERT), Carnegie Mellon University (Carnegie Mellon University CERT®), and Australia (Australia Computer Emergency Response Team (CERT))

Discipline: Cyber defence systems and the practise of cyber hardening rely on heuristics or "rules of thumb". Hackers can also fall into this group whereby they download tools and follow a set of common practises to achieve their goal. Users of these tools normally do not understand the underlying defensive cyber operations methods or active/combative cyber operations exploits. They simply use the tool as they have been taught.

Science: Understanding the underlying principle is essentially a science. When it comes to cyber, this falls under Computer Sciences. Individuals or groups of individuals who write malicious code or derive methods to perform cyber crimes are examples of the use of science in cyber. Reversing or dissecting of code along with research and testing to cultivate vulnerabilities and exploits are other applications of science.

Engineering: Finally, the knowledge of engineering advances common practises into best practises. The result of successful engineering in cyber is the industrialization of a cyber weapon.

When these five Knowledge Economies are aligned to the Capability and Maturity Model Integration (CMMI Institute) from 1 to 5 (chaotic, repeatable, defined process, managed, optimization and continual improvement), we can assign the cyber maturity of various individuals, companies, and governments in an unconventional qualitative manner.

TABLE 1. KNOWLEDGE ECONOMIES RELATED TO CYBER AND CMMI

Knowledge Economies	Definition	Relation to Cyber	CMMI
Art	• Rare unquantified talent • Wide range of consistency	• Advanced persistent threats	Initial or chaotic
Craft	• Master and apprentice • Consistency from good teaching	• CIRC and CERT • Cyber weapon construction (or the writing of malicious code)	Managed or repeatable
Discipline	• Heuristics	• Hacking and Cyber defence • Practise of cyber hardening	Defined
Science	• Underlying principles are well understood	• Computer science	Qualitatively managed
Engineering	• Best practices applied • Highly reproducible	• Kinetic warfare	Optimizing or continual improvement

Since we choose to be connected over the Internet and suffer from each other's shortcomings and failures, we may collectively be very low on the maturity scale even if we individually measure higher using the knowledge economy model.

3. DISCRIMINATION

In general, cyber weapons can be organised into four high level categories: Weapons of mass interruption, weapons of mass manipulation, surgical or tailored weapons, and weapons of mass destruction. Each of these four categories is described below.

A. Weapons of Mass Interruption (WMI)

Weapons of mass interruption cause a form of chaos in the interconnected cyber space by introducing delays into normal cyber workflow. Well-known examples of weapons of mass interruption are, but not limited to, wide spreading viruses, Trojans, worms, botnets, or email spamming resulting in a variety of outcomes including diminished or denied services to exfiltration of data including passwords. The offending operations often include a relatively small introduction or alteration of information on a system resulting in an increased amount of network traffic from the infected system.

Some historical examples of this type of weapon are listed below.

1. 2000-05-04: ILOVEYOU (worm) (CERT® 2000)
2. 2001-09-18: Nimda (worm) (CERT® 2001)
3. 2003-01-24: SQL Slammer (worm) (CERT® 2003)
4. 2004-01-26: Mydoom (virus) (CERT® 2004)
5. 2007-01-19: Storm (Trojan) (Symantec 2007)
6. 2009-03-29: Confiker (worm) (US-CERT 2013)
7. 2009-05-28: Bredolab (Trojan) (Symantec 2012)

Interestingly, the impact of weapons of mass interruption have not been as prevalent in the recent past[11]. One may say it could be credited to our improved level of maturity such that we are able to detect and defend against such attacks with common tools. One may also argue that it may be a result of countermeasures and that countermeasures trigger more opportunities to counter from all sides, however, this behaviour is unlikely as we still see some of these types of weapons reaching cyber borders.[12]

B. Weapons of Mass Manipulation (WMM)

Weapons of mass manipulation tend to alter or delete information. "Cyber attacks" using weapons of mass manipulation generally have longer lasting effects than those causing interruption, however, a well-managed and mature Information Technology service deliver model can generally recover within a short and/or reasonable amount of time, and with this capability, the weapon behaves akin to a weapon of mass interruption technique versus mass manipulation.

Recovery from mass manipulation may involve the complete destruction or quarantine of the attacked systems followed by a full restoration of data using a safe and un-infected backup set.[13] Hardware impacted by firmware altering attacks can prove to be more time-consuming to recover from, as the ability to restore firmware may not always be possible, thereby resulting in potential hardware procurement and shipment timeline challenges.

Ransomware is a good example of a manipulation weapon. It alters the data on a computer using a method of encryption but does not delete it immediately. (Wikipedia 2017) Although the prevalence of ransomware seems to be rising as of mid-2016 through 2017, in comparison to other types of malware and cyber weapons, it remains a negligible quantity.[14]

An example of a weapon of mass manipulation was the Saudi Aramco deletion of data and overwriting of the Mast Boot Record (MBR) of over 35,000 computers, via the Shamoon virus. In 2012, Shamoon also left behind propaganda showing what was likely supposed to be a burning flag of the USA, however, possibly due to poor coding, the burning flag was only partially visible (Wikipedia 2017).

A second example of mass manipulation was the shutdown of 30 power substations in Ukraine also impacting small parts of other surrounding nations. The impact was short-lived lasting between 1 and 6 hours. The hackers used a poorly situated remote access point to the Supervisory Control and Data Acquisition (SCADA) network that bypassed air-gapped systems and the expected two-factor authentication.[15]

Weapons of mass manipulation are not only those that are inadvertently contracted, they can also be purposefully directed to result in the manipulation of public or political perception or opinion. These types of "cyber attacks" have commonly surfaced as fabricated articles, opinionated articles, and comments in social media circles to name a few.[16]

C. Surgical or Tailored Weapons

Surgical or tailored weapons are not discovered as easily, but when they are uncovered, they do receive a level of government and corporate attention.[17] They can be written and delivered to attack a specific unit of information technology at an organization level

---

[11] Wikipedia, article on "*Timeline of computer viruses and worms*" (Wikipedia 2017), when reviewing the list of malware in the timeline presented, one can see the progression from WMI to WMM. The article lists WMI malware in 2015 through 2017, however, the quantity is far less than those described in the 1990 through 1999 and 2000 through 2009 inclusive.

[12] Benzmüller's review of AV-Test's statistical data of new malware between 2007-2017 revealed that in 2016 there were on average *"780 [new malware specimen] per hour"* and in 2017Q1 alone there were on average *"858 [new malware specimen] per hour"*. (Benzmüller 2017)

[13] Symantec's "*Ransomware: 5 dos and don'ts*" describe (1) the proper cyber hygiene including performing backups and (2) the behaviour of common ransomware. (Symantec 2017)

[14] Benzmüller summarized the ransomware analysis of 2016 through 2017 as *"…the total volume of ransomware was hardly detectable and vanishes in the flood of other malware."* He also noted that *"The share of ransomware is growing substantially. In the general flood of malware it is hardly measurable."* (Benzmüller 2017)

[15] Zetter described the vector of attack in paragraph 8 of the article. (Zetter 2016)

[16] The ODNI describes some of the evidence accumulated by the CIA, FBI, and the NSA regarding Russia's (at a nation state level) campaign to influence the 2016 US Presidential election in the declassified report. (Office of the Director of National Intelligence (ODNI) 2017)
Calabresi, paragraph 9 states *"…a Russian soldier based in Ukraine successfully infiltrated a U.S. social media group by pretending to be a 42-year-old American housewife and weighing in on political debates with specially tailored messages."* (Calabresi 2017) and *"…Russia created a fake Facebook account to spread stories on political issues like refugee resettlement to targeted reporters they believed were susceptible to influence."* (Calabresi 2017)
Shane descried the use of counterfeit online social media profiles, *"genuine accounts that had been hijacked"* (Shane 2017), and the US national and international public that seem to be influenced by the Russian sourced individuals and stories.

[17] Roberts discusses the use of SQL injection code to reveal unauthorized information of key organizations to hackers. (Roberts 2017)

down to a specific file or object. Generally, they do not spread too far beyond the intended target and thereby limit collateral damage.

It is entirely possible that a tailored cyber weapon may be re-useable on another target without further customization of the weapon. This is likely due to the type of vulnerability or exploit that may have been used.

Examples of these are the theft of credit card details of SONY PlayStation and Microsoft Xbox clients (among others)[18], the US Office of Personnel Management (OPM) data breach including personal information such as fingerprints of 5.6M federal employees (Wikipedia 2017), Stuxnet on nuclear centrifuges in Iran (Mueller and Yadegari 2012), and the BOTNET attack on Estonia (McGuinness 2017), and the data breach at Equifax (Wikipedia 2017).

D. Weapons of Mass Destruction (WMD)

At the time of writing, we have yet to be made aware of a cyber weapon of mass destruction, in other words one that directly causes mass casualties and/or loss of life, damage to structures, or damage to the biosphere. One could present the case that the shutdown of 30 power substations affecting approximately 230,000 people during the 2015 "cyber attack" in Ukraine may have impacted lives, however, there is little reported evidence of this during the short-lived outage.

One may also consider the sabotage of the Siberian natural gas line explosion of 1982 (disputed as 1989) was the first documented "cyber attack". However, this has been contested as *"not caused by a system shutdown, but by deliberately creating overpressure in the pipeline by [manually] manipulating pressure-control valves in an active control process."* (Rid and McBurney 2012, 9) Poor construction causing a leak followed by a poor decision to manually increase the line pressure may have caused the gas to ignite when two trains collided. (Wikipedia 2017)

Transformers that feed hospitals can fail at any time and the utility does not provide a redundant unit for them. We have seen rodents such as a squirrel take up shelter inside a transformer unit located on or near a facility causing a short resulting in a loss of utility power.[19] Replacing a failed primary transformer provided by the utility often has long lead times, sometimes as high as 3 to 12 months. During this time, the critical service such as a hospital is expected to operate with alternate power, such as uninterruptible power supplies supported by generators, flywheels, and the likes.

For data centres, the Uptime Institute defines utility as an "*economic alternative*"[20]. They also specify that data centres should expect loss of utility power and Tier III and IV facilities should live and operate through such conditions without any loss of critical load. Extending this to cyber, if a hospital or other critical service were to lose utility power due to a "cyber attack", it would be considered highly unlikely that they would not have an alternate source to generate their own power. If they did not have an alternate source, then the service could not be truly considered critical, as it was never prepared to support any type of loss of utility.

Alternatively, one may argue that the impact of a "cyber attack" to a state, organization, or even an individual can be a reflection of their cyber hygiene or negligence to remain current with global cyber security directions.

When it comes to air gapped systems, the awareness to jump air gapped networks and achieve access to command and control systems is likely not resting solely on cyber capability and involves the support of various other vectors of attack including but not limited to those such as HUMINT and SIGINT. This type of behaviour is related to sabotage and espionage. (Wikipedia 2017)

4. RECOMBINANT AND MUTABLE

Imagine the difficulty in conceptualizing and designing a traditional kinetic weapon that performs reasonably well in hand-to-hand combat and is equally capable of delivering a large explosive yield with a radius that could encompass an average European country. Now imagine the same under cyber, where the programmer has merged existing code into a new cyber weapon that will be able to apply all actions of the code. The programmer does not need to design new components of the cyber weapon. They simply need to write a method to merge the capability under one package or payload of code.

The idea of hybridizing conventional kinetic weapons is something that is time consuming and challenging when attempting to achieve good results, however, significantly simpler in cyber. An example of this is the merged SpyEye and ZueS malware. SpyEye

[18] The Daily Mail article describes the acts of hackers known as "*LizardSquad*", releasing 13,000 passwords and credit card details harvested from various companies on Christmas Day. (Boyle 2014)

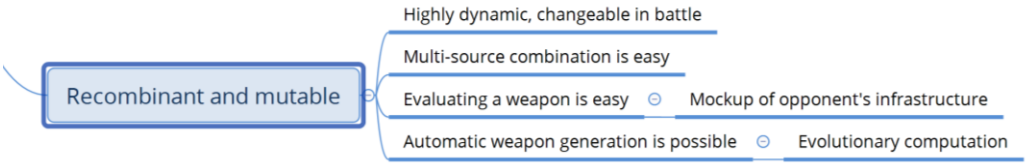
[19] Mooallem, discusses various cases where squirrels are the root cause for the failure of power distribution. (Mooallem 2013)

[20] Uptime Institute under the section "*Utility feeds determine Tier level*" they state: *"…utility power is subject to unscheduled interruption – even in places with reliable power grids…Most Tier Certified data centers use utility power for main operations as an economic alternative, but this decision does not affect the owner's target Tier objective."* (Uptime Institute, LLC 2017)

impacted a variety of browsers while ZueS targeted Microsoft Windows environments. Both SpyEye and ZueS harvested banking user credentials. (Lyden 2011)

From the mutable perspective, cyber weapons can also be written to change in battle, resulting in highly dynamic and agile weapons. Besides the ease of use, conventional weapons may be selected based on their yield among several other attributes, however, a cyber weapon can be equipped with access to a wide variety of dynamic alternatives that can be applied based on programming logic. These changes can be made very rapidly and designed to operate with or without human intervention.

FIGURE 2. MIND MAP OF CYBER OPERATIONS - RECOMBINANT AND MUTABLE



Evaluating cyber weapons can be discreet and also performed expeditiously. For example, testing a missile launch and detonation of payload can not only be time consuming but also very obvious to your adversaries and allies. In cyber, however, one could create a simulated environment of an opponent's infrastructure and document the outcomes of the variants without informing other parties. Then, as needed, one could recreate the simulated environment in short order to perform more tests of the cyber weapon. Automated restoration of these logical virtual test environment(s) can be employed to achieve an even faster set of test results.

Taking a step further, considering cyber weapons can selectively deploy a variety of payloads, then it may also possible to fully auto generate cyber weapons. This level of evolutionary computation can lead to a variety of outcomes including ones that could counter a counter-attack or even completely change the direction of the original "cyber attack" causing confusion at the repair level.

5. MODEL/OBJECT DICHOTOMY COLLAPSE

One of the more fascinating ideas behind the comparison of cyber and kinetic weapons is that the design is now the object. That means, one also no longer needs to use the lengthy process of (1) design to (2) manufacture to (3) shipping to (4) testing and potential (5) alterations of the design all the while disclosing the weapon to a wider body of individuals.

Having the design of a kinetic weapon or the chemical make-up of a weapon does not mean you can make it. In fact, you may be a long way from being able to put any of that information to use. However, having the design of software brings you much closer to having the actual software, and in the hands of an experienced programmer, they are effectively the same.

Companies and agencies have filed classified patents via trusted and cleared patent agents or patent attorneys to protect their inventions.[21] They may then employ contracted trusted and cleared private organizations to manufacture and ship the inventions to the government for use. This involves many external trusted hands on the invention and product while attempting to uphold supply chain integrity.

Cyber weapons, on the other hand, can be treated strictly as trade secrets, similar to Google's search algorithm or Coca-Cola's beverage recipe, and only employ a select group of trusted and cleared individuals within the chain of command. This model limits exposure of the design, which as stated above, is the object.[22]

In order to manage the proliferation of cyber weapons, access to the design of cyber weapons will need to be blocked to keep them out of harmful hands. Once a cyber mercenary gets their hands on a cyber weapon, they can easily deploy it with very little or possibly no training. Because the theft or copy of a cyber weapon is easily achieved, as is the ability to distribute it (thereby arming other cyber mercenaries), a very low barrier to entry exists in cyber operations.[23]

[21] *"Top Secret Patents"* (Collins 2009), *"UK keeps three times as many patents secret as the US"* (Marks 2010), and *"143 New Patents That Won't See the Light of Day"* (Marshall 2011) all reference classified patents.

[22] See World Intellectual Property Office (WIPO), "*Patents or Trade Secrets?*" web page. (World Intellectual Property Office (WIPO) 2017)

[23] Solon describes the case where a group called "*Shadow Brokers*" were offering what seemed to be part of an NSA toolset (or state sponsored cyber weapons) operated by a group known as the "*Equation Group*." (Solon 2016) The starting bid for the package set of tools was 1B Bitcoins or approximately $580M USD.

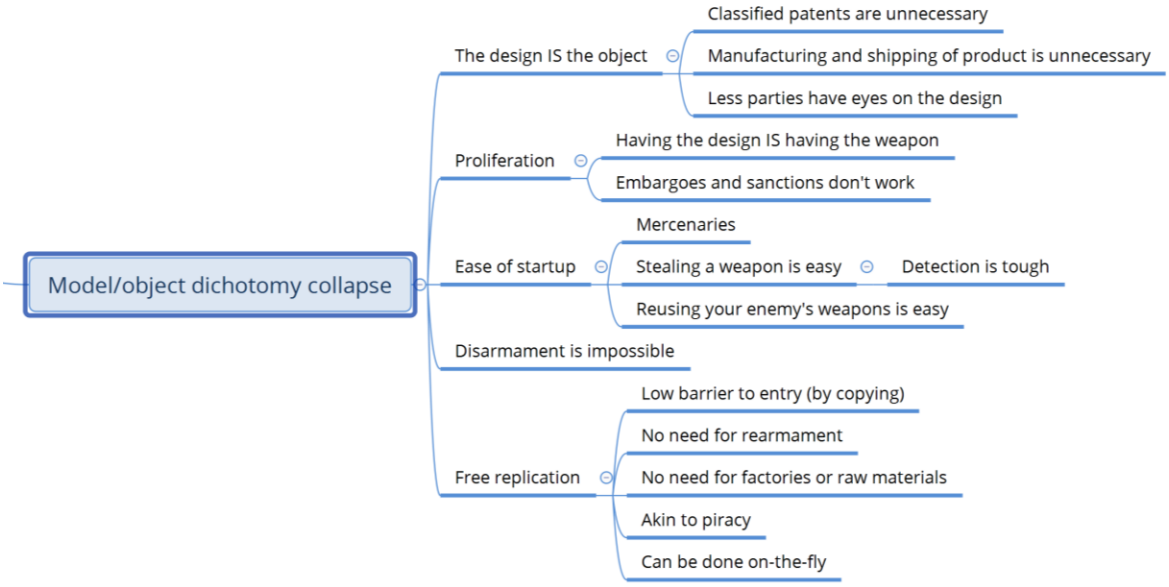
Due to this low barrier, nations who would likely never be able to arm themselves with appropriate kinetic capability to stand up against heavily armed nations or organizations would now be in a position to be considered as a qualified threat in cyber.

Efforts to slow the trade or exchange of cyber weapons may prove to be very difficult to manage via common embargoes and sanctions. New methods of such controls will need to be conceived and put into action. A step further to this problem is the concept of cyber disarmament, which seems near unrealistic. With traditional kinetic weapons, the manufacturing process requires raw materials and factories along with lead times. For cyber weapons, we can effectively avoid this delay and move directly to the object at nearly zero cost, or free replication.

Expanding on free replication, we face new challenges compared to the kinetic world:

1. Piracy: Traditional software or data piracy is managed through lawsuits and other legal frameworks, however, when it comes to cyber weapons, lawsuits are not a viable solution;
2. Replication on the fly: As one fires a cyber weapon, there is a possibility of the weapon replicating itself as it travels towards you; and
3. Rearmament: Cyber no longer requires the rearmament of threat actors. It may simply require new compute capability.

FIGURE 3. MIND MAP OF CYBER OPERATIONS - MODEL/OBJECT DICHOTOMY COLLAPSE



Extremely unique to cyber, when a primary source sends a cyber payload to its primary target, the primary target may be capable of realizing the payload and reusing it on an alternate or secondary target. This concept and capability of one's enemy reusing ammunition or weapons after they have been fired is extremely challenging to manage. If the code is in any way even slightly attributable to the primary source, the alternate or secondary target may consider the primary source as the true attacker. Possibly worse, any target may be in a position to review the payload, learn from it thereby increasing their maturity, and create a more damaging cyber weapon, all the while making it look as though the original attacker created it. These attribution challenges should force nation states to strongly consider the risks of cyber weapons prior to their use.

An example of this behaviour is the Stuxnet attack on Iran's uranium enriching centrifuges. Although not directly mentioned within the leaked classified document, USA's NSA and U.K.'s GCHQ refers to "*Western activities against Iran's nuclear sector*". The document further states that Iran has likely learned from attacks such as Flame, Duqu, Wiper, and Stuxnet and "*has demonstrated a clear ability to learn from the capabilities and actions of others*". (Intercept, The 2013, 1-2)

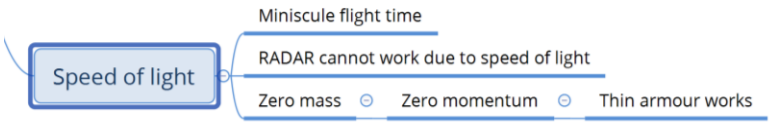
Intelligence supports that Iran replicated the techniques of the attacks in their own attack directed at Saudi Aramco via Shamoon, which is believed to mimic Wiper. Nevertheless, a group called "*Cutting Sword of Justice*" (Wikipedia 2017) took credit for the Saudi Aramco attack. Strangely, a Wiper inspired variant with unknown attribution overwrote the hard drives and MBR of various computers impacting Sony and various banks and other companies in South Korea. Although NSA and GCHQ could not confirm the attribution of the Shamoon attack on Saudi Aramco or any future attack, "*we cannot rule out the possibility of such an attack, especially in the face of increased international pressure on the regime.*" (Intercept, The 2013)

6. SPEED OF LIGHT

Another key difference between kinetic and cyber weapons is that cyber weapons are essentially photons traveling over a fiber network. That means traditional means of early warning systems are no longer effective (example: RADAR) as they must be faster than the speed of light. Detection of malicious activity using various log files is not very effective.[24] Real time methods of malicious detection of activity and data exist, however, in many cases they require a significant amount of effort to develop and maintain current as the payload is hidden among expected good data.[25] This may bring forward the interest to possibly slow the data flow down in order to properly analyse the traffic as it approaches a network. Although possible, this is generally not the intended outcome of high-speed networks and intercommunications.

It is also interesting to note that when a cyber weapon payload arrives, the package may take some time to realize this and may not be ready or triggered to deploy immediately. This delay generally offers defensive systems some time to detect and react accordingly.

FIGURE 4. MIND MAP OF CYBER OPERATIONS - SPEED OF LIGHT



The good news is, since the cyber weapon has zero mass and therefore zero momentum, it does not take much armour to defend. It does take very smart armour or active defence systems. Today's detection techniques and software tend to employ common tools with well-known detection and alert mechanism. Threat hunting tools tend to use historical data to assign a baseline then compare any new activity against the baseline. Although some of this can be automated, the response from the automation software tends to result in several false positives.[26]

To minimize false positives, hands on analysis of the data with computer-assisted threat hunting techniques can be employed. Once again, the result of this effort tends to report its findings much later than one would need to defend against a cyber payload arriving immediately. It should be noted that without proper cyber hygiene and strong IT Security maturity, the ability to apply threat hunting techniques tend to be next to impractical and unachievable.

7. DYNAMIC MULTIDIMENSIONAL SPACE

In traditional kinetic war, the theatre of operation is normally a physical space. Generally, theatre of operations are located in unpopulated areas for many reasons including limiting collateral damage. It can be very obvious when one approaches the theatre of operation using vessels or fleets of vehicles. This approach grants observing nations some time to decide how best to react.

Distance based artillery weapons take time to approach the theatre of operation while in flight. From a defensive approach, the reaction time available to counter these while in mid-flight can be considered beneficial. Methods to track launched artillery, realize the trajectory, calculate the intended location of impact, and even estimate the blast yield based on recognition of the type of artillery are tools that are used by nation states who may not even be directly implicated by the activities or directly involved in the theatre of operation.

In cyber, the theatre of operations does not mean much. Traditional notions of trajectory, location of impact, and blast yield estimation are completely changed if not gone. It is challenging to detect a launched cyber weapon and even more challenging to track it mid-flight. These challenges may seem similar to those described in the section "Speed of Light", but they pose another difficulty when it comes to the theatre of operation. Cyber allows for a completely dynamic theatre of operation, one where collateral damage is very easy.

---

[24] Mandiant states *"…attackers still had a free rein in breached environments [for] far too long before being detected—a median of 205 days in 2014 vs 229 days in 2013."* (Mandiant, A FireEye Company 2015, 1)

[25] Filkins, page 5 paragraph 4, section "*Teaching Machines to Identify Threats*" states: *"Specific domain knowledge related to security…A data scientist must apply security domain knowledge to identify primary and secondary sources of data, determine how to clean and transform acquired data and select the best ML analytical method or algorithm for the problem at hand."* (Filkins 2015, 5)

[26] Lee et al. discuss the increased false positives when applying Security Operations Centre (SOC) based hunting. (Lee and Lee 2017, 8-9)

In cyber space, determining "what is connected to what" is complex therefore determination of the damage impact and collateral damage of a cyber weapon is unpredictable. To leverage the unpredictability, the attacker may decide to utilize multiple sources within the cyber space to launch their "cyber attack" making it difficult to determine the true source. The adversary could also vary the frequency of the attacks along with the sources causing further confusion at the defensive end. Adversaries using virtual hosts to launch their attacks could easily change additional variables of the situation by destroying the virtual images of the various sources.

When looking at the challenge from a corporate or individual perspective, the idea of investigation is essentially akin to self-policing. When a civilian is faced with a break-and-enter at an office or home, normally the primary action is to call the police. The authorities manage the incident by writing a report, performing an investigation, and much more to hopefully solve the criminal case and under legal governance, bring justice for the injured party.

With cyber, civilians tend to take on the investigative effort themselves. This behaviour is similar to tampering with evidence. IT staff spend time combing through log files and looking up DNS records to identify domain owners and in some cases directly contact them. With the absence of police capability to support cyber crimes, civilians are essentially left on their own to police themselves. In areas where police are involved, a lack of uniformity between municipal, provincial/state, and federal levels constructs a "craft" knowledge economy way of cyber policing.

8. SCOPE OF IMPACT

Cyber weapons have a wide range of initial impact with various subordinate and sometimes unpredictable impacts. When considering the purely digital impacts, one can easily notice the similarity of behaviour with traditional espionage. Many news reports describe the negative cyber events as attacks, however, if data has not been lost permanently and is simply duplicated elsewhere (for example), is this behaviour an attack or a type of espionage?

At the World Wide Cyber Threats Hearing on September 10, 2015, now former US NSA Director Admiral Michael Rogers stated that:

> *"terminology and lexicon is very important…and attack and act of war…it's not necessarily in every case how I would characterize the activity that I see."* (Permanent Select Committee on Intelligence 2015, 51m20s-52m02s)

Immediately thereafter, now former US Director of National Intelligence James Clapper reinforced the comment by stating:

> *"…just using the OPM breach is a case and point. That really, although it's been characterized by some loosely as an attack, it really wasn't, since it was an[sic] entirely passive and it didn't result in destruction or any of those kinds of effects, so that the distinction you pointed out, and thank you for doing that, is quite important."* (Permanent Select Committee on Intelligence 2015, 51m20s-52m02s)

In the traditional world of espionage, capturing information or even altering information or public perception is expected criminal behaviour, even during times of peace[27]. The similar behaviour in cyber could be called "cyber espionage" instead of "cyber attack", and result in a criminal case versus a nation state's cyber or kinetic response.

If one were to take such a position, then the alteration of data, such as the WannaCrypt (Wikipedia 2017) or Petya (Wikipedia 2017) ransomware, or deletion of data, such as the Shamoon (Wikipedia 2017) virus, may also fall into the category of espionage and sabotage. The loss of data should be expected, as it could happen due to hardware or software failures at any time. Therefore, other means of data backup and restore capabilities should exist. When other means of data protection do not exist, one could interpret this as negligence. Hence, if data is destroyed via cyber behaviour, then one should be able to restore the data using well-defined and mature Information Technology management processes.

Taking this theory further, leaving misinformation behind and/or highlighting specific information are also methods of espionage. If one were to leave a package in a data store or deposit a package via any means into a computer network resource, could this behaviour be considered espionage? In his paper, Singer compares land mines and IEDs to autonomous cyber weapons as it applies to the direct participation of hostiles, describing the challenges faced with respect to the Law of Armed Conflict (LOAC).[28]

[27] Libicki describes *"…espionage by countries has been treated as acceptable state behaviour…This understanding has been carried over into cyberspace."* (Libicki 2017, 2)

[28] Singer describes *"Often the situation is compared to a civilian placing a mine or an IED, who is regarded as not directly participating after its return, completing the action (the revolving door problem)…"* (Singer 2017, 9)

Tit for tat and Game Theory: Typically, a kinetic attack generally expects a kinetic response. So, would then a "cyber attack" expect a cyber response?[29] When it is difficult to prove attribution, where should a nation state direct its cyber or kinetic response? When the source of cyber behaviour can be misrepresented as almost anyone's computer such as a specific civilian's, how is a nation state able to identify the true source? Would it then attack a civilian? If a precedence is set to attack civilians based on cyber behaviours, then nation states setting this precedence should expect reciprocal actions when the roles are reversed. The challenge of attribution plagues the entire scope of cyber.

Levels of attribution are also a measure of traditional espionage. A nation state may choose to directly engage with another nation's individual(s) to perform a criminal act such as extract information, affect change regarding a specific policy, or infiltration. Equally, the same nation state may decide to perform the same task using a level of attribution that distances them from the actual criminal act, making it difficult to definitively identify state level involvement in court or even at an international community level.

Even if a nation state follows laws and does not target civilians or civilian services when performing cyber activities, their adversaries may not choose to behave the same with their response. On September 28, 2017 at the ICF CyberSci Symposium in Fairfax, Virginia, USA, the now former US Director of National Intelligence James Clapper delivered a keynote and stated:

> *"The big take away for me, is that unless you are very confident in your cyber defenses, it's almost pointless to talk about cyber attacks. The very essence of offense is, you have to have a good defense, … And what complicates it further is, we in the U.S., we have an inclination to be very precise, very limited, very surgical, legalistic. You cannot be assured that the adversary is going to be similarly precise and surgical and legalistic. So if you attack them, you have [to] anticipate a probably much … greater retaliation as a result."*[30]

With respect to the scope of impact, his thoughts shed light on another challenge with cyber activities. Countermeasures may not always be the answer as they may simply result in an escalation of countermeasures.

Thus far, the following examples fall into the purely digital form of attack, which may likely be better described as espionage and their impact to the data's confidentiality, integrity, and availability (CIA):

1. Consumption of computational resources, impacting data availability;
2. Blocking of services, impacting data availability;
3. Copy (or theft) of information, impacting data confidentiality;
4. Alteration of data, impacting data integrity;
5. Deletion (or destruction) of data, impacting availability; and
6. Leaving data behind, impacting data integrity.

Each of these cyber espionage behaviours are most likely criminal behaviour, and similar to traditional espionage.

When it comes to assessing the emergence of cyber behaviour into the non-digital space, the impact is not as clear. To remove some of the obvious items from this area, let us ignore systems that are air-gapped by one or more levels. Breaches of air-gapped systems tend to use more than just cyber and thereby likely fall under traditional espionage behaviour. That tends to leave non-critical systems behind. Systems in the cloud, fog (example: Wi-Fi space), or mist (example: Bluetooth space) would once again each be challenged by attribution.[31]

An example of cloud implications affecting a large audience could be a government provided nationwide social service program. In this example, users log into a secure platform online and enter or retrieve their own personal data regarding their social program. Destroying this platform via criminal cyber behaviour (impacting data availability) would likely result in a data restore and repair plus the closing of the vector of attack. Altering of large amounts of data (impacting data integrity) would likely be noticed with proper IT management and not allowed. Altering of data specific to one or few individuals (impacting data integrity) may go unnoticed for a while but the impact may be small and easily repaired with proper IT management and good cyber hygiene. Harvesting of all data (impacting confidentiality) should not be possible when common practises and proper system architecture are applied, and if it were to be possible, only portions of the data would be exposed resulting in a less or unusable incomplete data set. Either way, the entire cyber behaviour is criminal and likely challenging to definitively decide to start a war over.

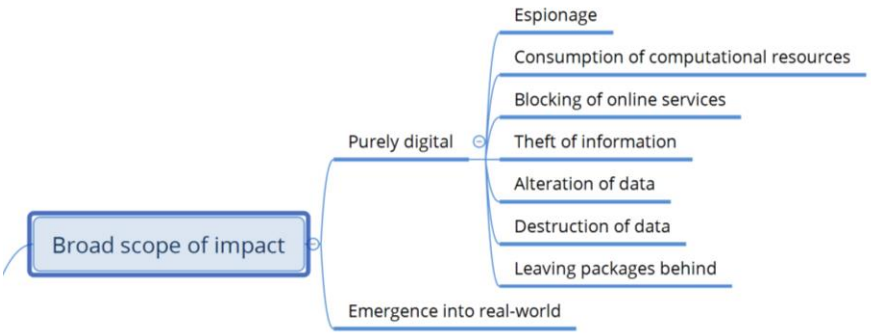
---

[29] On the future of cyber, on August 14, 2017, advance to 49m 46s to 50m 03s of Lt. Gen. Stewart's full speech at DoDIIS 2017: *"I want to be able to hunt for and isolate that malicious strange behaviour. Once we've identified and isolated that malware, I want to analyze it, re-engineer it, and prepare to deploy it against the very same adversary who sought to use it against us."* (Stewart 2017)

[30] Waterman summarizes the keynote delivered by now former US Director of National Intelligence James Clapper including the quote. (Waterman 2017)

[31] Preden's whitepaper describes the concepts of cloud, fog, and mist computing. While a lecturing at the Tallin University in January 2015, Dr. Preden created the term "*mist computing*". (Preden 2016)

FIGURE 5. MIND MAP OF CYBER OPERATIONS – SCOPE OF IMPACT



An example of fog implications affecting a large audience could be a deployment of (1) public Wi-Fi access points susceptible to malicious code or (2) illegitimate cellular radio towers, whereby the impact can be quite large affecting public and private sector users. Normally, if one is communicating at a classified level, these types of public devices cannot be used. Corporate users or unclassified security-conscious users would likely consider the use of VPNs for remote access and employ cyber security common practise controls to limit their risk of exposure. Notably, use of public voice networks to convey tactical responses that will be carried out immediately is allowed in many countries. Hence, the interception of such a call is not much of a concern at a nation state level. Finding the illegitimate cellular radio towers may prove to be challenging but are generally easy to detect by those who are well trained in the art.

Public Wi-Fi access points that are susceptible to malicious code should be updated and maintained with proper IT practises. Any device that is suspect due to potentially compromised code/design or supply chain integrity should be removed from service and replaced with one that does not carry these risks.[32] Once again, the behaviour described is most likely criminal and not one that is causing physical harm or death.

Finally, applying an example to the mist where a large audience is impacted could be a mass exploit of the Bluetooth protocol. Compromised devices could be openly sharing personal information such as contacts stored in cellular phones to credit card information stored within personal mobile devices. Once again, classified devices generally have wireless protocols and wireless capability physically disabled, so there is no impact to these types of devices. Personal and corporate devices impacted by this type of infection would likely be cross-sharing information with each other (impacting data confidentiality). This type of information exchange would result in the rapid use of one's mobile device data storage.

The infection could be easily stopped at an individual level by disabling the Bluetooth antennae or even completely disconnecting from all networks (also known as airplane-mode on some devices). When considering the case of involuntary sharing of credit cards and if an unauthorized user could misuse that credit card information, the risk is mitigated by the credit card companies who allow only low value transactions via mobile devices. All transactions remain monitored by the credit card company and they hold the right to mark the transaction as potentially or certainly fraudulent thereby disallowing the transaction and likely assigning the card as compromised (impacting availability). In any case, this would result in a criminal case and most likely cause mass interruption, but certainly no direct physical harm or death with any expectation of a nation's kinetic response.

Building on the concept of zero mass and zero momentum from the section on "Speed of Light", is the measure of energy. Kinetic weapons have a quantity of joules or kinetic energy applied and delivered. The energy calculation can be streamlined by using the mass and velocity of the object. A 10mm bullet (with a mass of 0.015 kg)[33] leaving the muzzle of an MP5/10 submachine gun (with a velocity of 425 m/s)[34] results in approximately 1,355 joules of kinetic energy per bullet (using the formulas $E_k = \frac{1}{2}mv^2$). Applying the same logic, with 0 g of mass and velocity equivalent to the speed of light, cyber weapons deliver 0 joules of kinetic energy. Therefore, the impact in the physical space is effectively not possible.

[32] Palmer describes the use of hotel WiFi access points to deliver malware (Palmer 2017)
[33] Wikipedia article on "*10mm auto*" where the largest mass described is 15 grams (Wikipedia 2017)
[34] Wikipedia article on "*Heckler and Koch MP5*" where the MP5/10 muzzle velocity is 425 m/s using 10mm calibre rounds (Wikipedia 2017)

9. FROM DOMAIN OF WAR TO TRADECRAFT

When we sit back and look at the history of events of any situation, we tend to see things differently as hindsight is 20/20. When looking back at cyber, many are simply astonished with how far we have come. When reviewing the historical and future behaviour of cyber and comparing it to non-cyber activity, the relationship with espionage surfaces.

During the Q&A after his speech on August 8, 2017 at the annual Space and Missile Defense Symposium in Huntsville, Alabama, General John Hyten, commander of US Strategic Command (USSTRATCOM), stated:

> *"There's no such thing as war in cyberspace. There's just war. We have to figure out how to defeat our adversaries, not to defeat the domains where they operate."* (Hyten 2017)

Hyten's point was to state that the US will defend and deter an adversary with any means necessary. Nevertheless, a nation state may still decide to declare cyber as a Domain of Warfare bringing with it, its own set of challenges. From the difficulty to definitively apply attribution, to the direct participation of hostiles with autonomous cyber weapons (Singer 2017), to the inability to truly cause physical harm similar to a kinetic weapon, the cyber domain is more consistent with espionage and sabotage.

A key difference between traditional and cyber espionage or sabotage is the deterrence with risk of legal punishment. When one performs traditional espionage or sabotage in a foreign country, they are considered a hero in their own country and a criminal in the opposing. If they commit acts of treason against their own country, it is generally the opposite result.[35] Either way, aside from the legal consequences, there may be a risk to one's self, family, and possibly even friends' safety. Because traditional espionage involves the actor to physically enter another country or leave their own, there is a higher risk of being arrested, commonly attracting little to no media attention.

Under cyber, the behaviour may be compared to a dog with a loud bark, but almost no bite. Attribution aside, international political and civilian pressures drive sympathies for the crimes, commonly due to higher media attention.[36] Furthermore, you need to wait for the criminal to enter your country[37] or request extradition, only to be challenged by sentencing guidelines.[38]

What may be plausible is that the idea of full kinetic war is not the goal. This is likely because engaging in full kinetic war with capable adversaries tends to result in a level of mutually assured destruction. This level of deterrence is obvious with nations capable of executing nuclear options.

So, then what if the meaning of war is no longer only kinetic? Today's wars seem to occur for ideological, political, and economic factors. These wars tend to be fought less with kinetic options and more with sanctions, embargoes, political pressures, policies, and most certainly various methods of espionage. This essentially means nation states are at some level of war all the time. If constant war is today's new model of living, then it is very likely that the tradecraft of the cyber domain is something that may be useful as espionage and sabotage tools to assist in warfare.

The idea that cyber is shape-shifting may come from the wide interpretations and expectations of cyber. It is our opinion that cyber effectiveness is highly dependent on the target's cyber hygiene and the adversary's ability to exploit or infiltrate it. It is similar to the idea that one's ability to avoid HUMINT exploitation and infiltration is highly dependent on how they protect and live their lives. Poor life decisions can likely lead you to be considered a better and/or easier target.

To reiterate, the purpose of this paper is not to apply a definitive outcome or decision. It is written to apply taxonomy and motivate the reader to consider the concepts differently, which may change the way we perceive and consider cyber operations. What may be the impact of calling every cyber event a "cyber attack"? The continued misuse of the term "cyber attacks" can easily lead many to incorrectly identify the situation(s) as a legally defined "attack", thereby applying public and political pressure for a nation state to respond with possibly poor decisions of great consequence.

---

[35] As retired CIA counterintelligence analysts, Sandra and Jeanne describe CIA counterintelligence officer Aldrich Ames as a mole and traitor to the US. Ames provided US intelligence information to the Soviet Union that resulted in the deaths of more than ten Soviet intelligence officers who spied for the US. Sandra described her sympathy for the Soviets and their family members and attributed their deaths to Ames. (Grimes and Vertfeuille 2012)

[36] BBC News describes sympathy offered by American Civil Liberties Union (ACLU) and Amnesty International as they campaigned to have Snowden pardoned. The article also highlights the 2016 "Snowden" film's director's comments (Oliver Stone) describing the US government's activities as *"illegal"*, thereby indicating sympathetic support for Snowden. (BBC News 2016)

[37] Perez reported that a Chinese national was arrested in relation to the 2015 US OPM breach when he entered the US attempting to attend a conference. The charges are related to the creation of the Sakura malware, leaving the reader to assess if other arrests could be made regarding the use of the malware regarding the 2015 US OPM breach. (Perez 2017)

[38] Williams describes how judges are struggling with the sentencing of cyber crimes. (Williams 2016)

REFERENCES

Australia Computer Emergency Response Team (CERT). n.d. Accessed November 6, 2017. https://www.cert.gov.au/.

BBC News. 2016. *Edward Snowden: ACLU and Amnesty seek presidential pardon.* BBC News, US & Canada. 12 September. Accessed November 6, 2017. http://www.bbc.com/news/world-us-canada-37341804.

Benzmüller, Ralf. 2017. *Malware trends 2017.* G DATA Software. 10 April. Accessed November 6, 2017. https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017.

Boyle, Darren. 2014. *Hackers release cache of 13,000 passwords and credit cards of PlayStation, Xbox and Amazon users.* Daily Mail, MailOnline. 27 December. Accessed November 6, 2017. http://www.dailymail.co.uk/news/article-2888339/Hackers-release-cache-13-000-passwords-credit-cards-Playstation-Xbox-Amazon-users.html.

Calabresi, Massimo. 2017. *Inside Russia's Social Media War on America.* Time Magazine. 18 May. Accessed November 6, 2017. http://time.com/4783932/inside-russia-social-media-war-america/.

Carnegie Mellon University CERT®. n.d. *The CERT® Division.* Software Engineering Institute, Carnegie Mellon University. Accessed November 6, 2017. http://www.cert.org/.

CERT®. 2000. *Advisory CA-2000-04, Love Letter Worm.* Software Engineering Institute, Carnegie Mellon University. 9 May. Accessed November 6, 2017. https://www.cert.org/historical/advisories/CA-2000-04.cfm.

—. 2001. *Advisory CA-2001-26, Nimda Worm.* Software Engineering Institute, Carnegie Mellon University. 25 September. Accessed November 6, 2017. https://www.cert.org/historical/advisories/CA-2001-26.cfm.

—. 2003. *Advisory CA-2003-04, MS-SQL Server Worm (SQLSlammer).* Software Engineering Institute, Carnegie Mellon University. 27 January. Accessed November 6, 2017. https://www.cert.org/historical/advisories/CA-2003-04.cfm.

—. 2004. *Incident IN-2004-01, W32/Novarg.A Virus (Mydoom).* Software Engineering Institute, Carnegie Mellon University. 30 January. Accessed November 6, 2017. http://www.cert.org/historical/incident_notes/IN-2004-01.cfm.

Clapper, James, Marcel Lettre, and Michael Rogers. 2017. *Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States.* United States Senate Committee on Armed Services. Accessed November 6, 2017. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

CMMI Institute. n.d. *What is Capability Maturity Model Integration (CMMI)?* CMMI Institute. Accessed November 6, 2016. http://cmmiinstitute.com/capability-maturity-model-integration/.

Collins, B. 2009. *Top Secret Patents.* Inventors Digest Magazine. 10 July. Accessed November 6, 2017. https://www.inventorsdigest.com/articles/top-secret-patents.

Filkins, Barbara. 2015. *The Expanding Role of Data Analytics in Threat Detection.* SANS Institute. Accessed November 6, 2017. https://www.sans.org/reading-room/whitepapers/analyst/expanding-role-data-analytics-threat-detection-36362 .

Grimes, Sandra, and Jeanne Vertfeuille. 2012. *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed.* Annapolis, MD: Naval Institute Press.

House of Commons of Canada. 2017. *Bill C-59: An Act respecting national security matters.* Parliament of Canada. 20 June. Accessed November 6, 2017. http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading#enH2829.

Hyten, John. 2017. "Transcript of Gen. John Hyten's speech from the Space and Missile Defense Symposium." *US Strategic Command.* 8 August. Accessed November 6, 2017. http://www.stratcom.mil/Media/Speeches/Article/1274339/space-and-missile-defense-symposium/.

Intercept, The. 2013. *Iran – Current Topics, Interaction with GCHQ.* 12 April. Accessed November 6, 2017. https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/.

Lee, Rob, and Robert M. Lee. 2017. *The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey.* SANS Institute. https://www.sans.org/reading-room/whitepapers/analyst/hunter-strikes-back-2017-threat-hunting-survey-37760.

Libicki, Martin. 2017. “The Coming of Cyber Espionage Norms.” *2017 9th International Conference on Cyber Conflict: Defending the Core*. Tallinn, Estonia: NATO CCD COE Publications, Tallinn. https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espionage%20Norms.pdf.

Lyden, John. 2011. *Bastard child of SpyEye/ZeuS merger appears online: Malware lovechild monst(e)r/demon.* The Register. 25 January. Accessed November 6, 2017. https://www.theregister.co.uk/2011/01/25/spyeye_zeus_merger/.

Mandiant, A FireEye Company. 2015. *M-Trends 2015: A view from the front lines.* Mandiant. http://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

Marks, Paul. 2010. *UK keeps three times as many patents secret as the US.* New Scientist. 23 March. Accessed November 6, 2017. https://www.newscientist.com/article/dn18691-uk-keeps-three-times-as-many-patents-secret-as-the-us.

Marshall, Eliot. 2011. *143 New Patents That Won’t See the Light of Day.* Science Magazine. 21 October. Accessed November 6, 2017. http://www.sciencemag.org/news/2011/10/143-new-patents-wont-see-light-day.

McGuinness, Damien. 2017. *How a cyber attack transformed Estonia.* BBC News. 27 April. Accessed November 6, 2017. http://www.bbc.com/news/39655415.

Middleton, Bruce. 2017. *A History of Cyber Security Attacks: 1980 to Present.* New York: Auerbach Publications.

Minárik, Tomáš. 2016. *NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit.* INCYDER News, NATO CCDCOE. 21 July. Accessed November 6, 2017. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

Mooallem, Jon. 2013. *Squirrel Power!* Sunday Review, The New York Times. 31 August. Accessed November 6, 2017. http://www.nytimes.com/2013/09/01/opinion/sunday/squirrel-power.html.

Mueller, Paul, and Babak Yadegari. 2012. *The Stuxnet Worm.* Tucson, AZ, USA: Department of Computer Science, University of Arizona. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

NATO Communications and Information Agency. 2016. *NATO expands cyber defence coverage.* 1 July. Accessed November 6, 2017. https://www.ncia.nato.int/NewsRoom/Pages/160701_NATO-expands-cyber-defence-coverage.aspx.

NATO Review Magazine. 2013. *Cyber - the good, the bad and the bug-free: The history of cyber attacks - a timeline.* NATO Review Magazine. 17 June. Accessed November 6, 2017. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/.

Office of the Director of National Intelligence (ODNI). 2017. *ICA 2017-01D - Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution.* National Intelligence Council, Intelligence Community Assessment. Accessed November 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Palmer, Danny. 2017. *Hackers are using hotel Wi-Fi to spy on gusts, steal data.* ZDNet, Cyberwar and the Future of Cybersecurity. 20 July. Accessed November 6, 2017. http://www.zdnet.com/article/hackers-are-using-hotel-wi-fi-to-spy-on-guests-steal-data/.

Perez, Even. 2017. *FBI arrests Chinese national connected to malware used in OPM data breach.* CNN Politics. 24 August. Accessed November 6, 2017. http://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.

Permanent Select Committee on Intelligence. 2015. “World Wide Cyber Threats Hearing.” *YouTube.* Archived Hearing Webcast. 10 September. Accessed November 6, 2017. https://www.youtube.com/watch?v=Q3aG0CtZbU4.

Preden, Jürgo-Sören. 2016. “Evolution of Mist Computing from Fog and Cloud Computing.” *Thinnect Inc.* 22 June. Accessed November 6, 2017. http://www.thinnect.com/static/2016/08/cloud-fog-mist-computing-062216.pdf.

Public Safety Canada. 2016. *Canada Cyber Incident Response Centre (CCIRC).* 04 May. Accessed November 6, 2017. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx.

Rid, Thomas, and Peter McBurney. 2012. “Cyber-Weapons.” *The RUSI Journal* 157 (1): 6-13.

Roberts, Jeff John. 2017. *Hackers Breach Dozens of Universities and Government Agencies, Report Says.* Fortune Magazine, Cyber Security. 15 February. Accessed November 6, 2017. http://fortune.com/2017/02/15/data-breach-recorded-future/.

Schmitt, Michael N. 2012. "'Attack' as a Term of Art in International Law: The Cyber Operations Context." *2012 4th International Conference on Cyber Conflict.* Tallinn, Estonia: NATO CCD COE Publications, Tallinn. https://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf.

Shane, Scott. 2017. *The Fake Americans Russia Created to Influence the Election.* The New York Times, Politics. 7 September. Accessed November 6, 2017. https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

Shaw, Mary, and David Garlan. 1996. *Software Architecture: Perspectives on an Emerging Discipline.* Upper Saddle River, NJ: Prentice-Hall.

Singer, Tassilo. 2017. "Update to Revolving Door 2.0: The Extension of the Period for Direct Participation in Hostilities Due to Autonomous Cyber Weapons." *2017 9th International Conference on Cyber Conflict: Defending the Core.* Tallinn, Estonia: NATO CCD COE Publications, Tallinn. https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2008%20The%20Extension%20of%20the%20Period%20for%20Direct%20Participation%20in%20Hostilities%20Due%20to%20Autonomous%20Cyber%20Weapons.pdf.

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

Solon, Olivia. 2016. *Hacking group auctions 'cyber weapons' stolen from NSA.* The Guardian. 16 August. Accessed November 6, 2017. https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group.

Stewart, Vincent. 2017. "Lt. Gen. Stewart's remarks at DoDIIS." *YouTube.* Defense Intelligence Agency. 14 August. Accessed November 6, 2017. https://www.youtube.com/watch?v=Nm-lVjRjLD4.

Symantec. 2017. *Ransomware: 5 dos and don'ts.* Malware, Internet Security Centre, Norton. Accessed November 6, 2017. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html.

—. 2012. *Trojan.Bredolab.* Security Center. 8 August. Accessed November 6, 2017. https://www.symantec.com/security_response/writeup.jsp?docid=2009-052907-2436-99.

—. 2007. *Trojan.Peacomm (Storm).* Security Center. 19 January. Accessed November 6, 2017. https://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99.

Trump, Donald John. 2017. "Presidential Memorandum for the Secretary of Defense, Subject: Elevation of U.S. Cyber Command to a Unified Combatant Command." *The White House.* 18 August. Accessed November 6, 2017. https://www.whitehouse.gov/the-press-office/2017/08/18/presidential-memorandum-secretary-defense.

Uptime Institute, LLC. 2017. *Myths and Misconceptions Regarding the Uptime Institute's Tier Certification System.* 20 July. Accessed November 6, 2017. https://journal.uptimeinstitute.com/myths-and-misconceptions-regarding-the-uptime-institutes-tier-certification-system/.

US-CERT. 2013. *Alert (TA09-088A): Conficker Worm Targets Microsoft Windows Systems.* 24 January. Accessed November 6, 2017. https://www.us-cert.gov/ncas/alerts/TA09-088A.

—. n.d. *US Computer Emergency Readiness Team (CERT).* Accessed November 6, 2017. https://www.us-cert.gov.

Vaidya, Tavish. 2015. "2001-2013: Survey and Analysis of Major Cyberattacks." *arXiv, Cornell University.* Georgetown University. 1 September. Accessed November 6, 2017. http://arxiv.org/pdf/1507.06673.

Waterman, Shaun. 2017. *Clapper: U.S. shelved 'hack backs' due to counterattack fears.* Cyberscoop, Scoop News Group. 2 October. Accessed November 6, 2017. https://www.cyberscoop.com/hack-back-james-clapper-iran-north-korea/.

Watson, Bruce. n.d. "Knowledge Economies and Cyber." *Postgraduate Diploma in Knowledge and Information Systems Management.* Centre for Knowledge Dynamics and Decision Making, Stellenbosch University.

Wikipedia. 2017. *10mm auto.* Vers. 23:53. 29 July. Accessed November 6, 2017. https://en.wikipedia.org/wiki/10mm_Auto.

—. 2017. *Equifax.* Vers. 11:43. 29 September. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Equifax.

—. 2017. *Espionage.* Vers. 16:35. 20 August. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Espionage.

—. 2017. *Heckler and Koch MP5.* Vers. 07:14. 22 August. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Heckler_%26_Koch_MP5.

—. 2017. *Office of Personnel Management data breach.* Vers. 16:32. 8 September. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach.

—. 2017. *Petya (malware).* Vers. 16:37. 14 August. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Petya_(malware).

—. 2017. *Shamoon.* Vers. 17:17. 3 July. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Shamoon.

—. 2017. *Timeline of computer viruses and worms.* Vers. 07:39. 10 August. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms.

—. 2017. *Ufa train wreck.* Vers. 01:31. 21 June. Accessed November 6, 2017. https://en.wikipedia.org/wiki/Ufa_train_wreck.

—. 2017. *WannaCry ransomware attack.* Vers. 20:29. 18 August. Accessed November 6, 2017. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

Williams, Katie Bo. 2016. *Judges struggle with cyber crime punishment.* The Hill. 9 January. Accessed November 6, 2017. http://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment.

World Intellectual Property Office (WIPO). 2017. *Patents or Trade Secrets?* World Intellectual Property Office (WIPO). 10 August. Accessed November 6, 2017. http://www.wipo.int/sme/en/ip_business/trade_secrets/patent_trade.htm.

Zetter, Kim. 2016. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *Wired.* 6 March. Accessed November 6, 2017. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

