Cyber Weaponization: Analysis of Internet Arms Development

Jason Gordon
infectionvectors.com
gordon@infectionvectors.com

ABSTRACT

Internet attacks are a familiar part of cyber residency for every modern institution. While the criminals behind the attacks, their business practices, and the illicit economy that propels most of the acts have been the subjects of many researchers, the refinement of the tools employed has not. We posit the concept of weaponization as an important facet of Internet security research in the context of three specific email-based attacks. The paper draws parallels between the study of cyber weapons and kinetic arms, particularly biological threats. Finally, the paper points to possible benefits and means of studying weaponization as part of a complete cyber security effort.

Keywords

weaponization, cyber attack, dangerousness

1. INTRODUCTION

The term "weapon," regardless of context as cyber or physical is taken to mean, "something…used to injure, defeat, or destroy" [21]. In 2003, while arguing against the commonly held philosophy of information warfare (IW), Thomas wrote that the apparent policy of the United States military was to avoid defining what an "information weapon" is altogether [26]. Indeed, as is noted later in this section, this nebulous category of weapons can include a broad variety of technologies. For this work, the author did not consider the use of kinetic weapons that are often used in the information warfare arena, such as Electro-Magnetic Pulse (EMP), High-energy Radio Frequency (HERF) guns, or even traditional artillery [4] in favor of focusing on strictly malware and policy-based responses.

The use of malicious code on the Internet lends itself to many of the same discussions of traditional munitions [16], (physical) weapon development (outfitting technology in such a way to make a viable weapon, or "weaponization"), and storage as are seen in military and defense communities. A weapon is used to increase the harm someone can inflict; leveraging the strength of its wielder many times over to produce a grander result than could be expected without the tool. In this paper, we document our examination of cyber weapons and compare their development to physical weapons – specifically those being studied by biological warfare experts. The scope of this paper was limited to email-borne weapons. Although overlooked in terms of technical novelty, email-based operations are a good foundation for studying the cyber battle space, both in terms of previous research into the business model of criminals (such as those behind the Bagle worm [15, 22]) and now with respect to weapons improvement processes because of the breadth of attacks they employ. Email is a "universal" medium for any type of payload, not unlike the paper envelope, box, or automobile in the physical world – historically, carriers of both kinetic and microbial weapons.

Computer Security Conference 2008, Myrtle Beach, South Carolina (April 16-18 2008).

Cyber-virus fighters encounter many of the same challenges of their kinetic weapon researching counterparts. Just as traditional weaponry (explosive-based, but primarily biological and chemical weapon parallels are discussed here) is optimized by increasing its destructive power or delivery precision; it is also made less effective by studying those areas and developing countermeasures. Biological threats are studied for the same reasons – to make stronger toxins and better understand the threat. In addition, the use of offensive capabilities is finding its way into the security postures of many organizations, tactics that could be described as "weaponizing the defenses." This paper addresses weaponization of cyber assets and the place of weaponization as a practical study in computer security research.

Previous work in this area has included a broad discussion of cyber arms control as a possibility between nation-states [7] and the detection of weapons ("hacking tools" [8] and malware) as they are used on target systems. This previous work has not dealt with weapons development processes, rather, much of that work focuses on the nature and rules of cyber warfare [4] or the integration of information systems into kinetic weapons [1]. Libicki [19] offered the first complete framework for defining information warfare, including warnings for some of the technological responses covered here. Denning has done more than any other individual to define the components and principles of information warfare, including: distinguishing "offensive" from "defensive" (and "dual-use") weapons while providing a comprehensive review of the challenges in criminalizing weapon ownership [9], the role of nation-state cooperation in restricting cyber arms [8], and related war fighting doctrine [10].

2. OF WEAPONS AND WEAPONIZING

A virus can be a weapon, whether biological or cyber in origin, but it cannot account for a victory alone. A biological virus cannot win a battle, take over a country, or execute any "orders" other than to make people and animals sick. Malware is incapable of destroying buildings, overthrowing governments, or making tactical decisions. In both cases, the pathogen may be capable of destabilizing the targeted environment and allow for a complementary attack to succeed. A biological pathogen may weaken a nation to the point where an invasion is made winnable. Similarly, a broadly-distributed trojan may allow the attacker to

invade a network and complete reconnaissance efforts – or absorb enough resources to allow for a separate attack all together. As such, refining biological elements into increasingly more useful (powerful) weapons and ranking those weapons by threat capacity is the subject of tremendous research [5].

Can every network asset be weaponized? The answer to this question is important to researchers and security practitioners alike – if it is possible to weaponize everything in cyber space, then we can define the qualities of all technology that will be exploited. If the answer is no, then it would certainly be worth studying the facets of any particular technology that make weaponization possible and impossible. In a review of current physical defenses [27] against microbial armaments, we find the best overview of what attributes strengthen biological weapons:

- Turning a threat into an easily distributed form
- Constructing a novel delivery system
- Making the form more deadly or more difficult to stop

In the next section, we look at Simple Message Transport Protocol (SMTP) based weapons in the context provided above. Security professionals often define their practice in terms of attacks - by way of the vulnerability or what was exploited. Currently, those definitions would include whether the attacker used system protocols as intended (delivering only a malicious payload, often relying on some form of social engineering and most similar to the attacks presented here), exploited the transport vehicle itself (as seen in injection attacks), or altered the system infrastructure itself (as in the case of stack/heap overflows) [23]. Law enforcement concerns itself with the where, who, and why as important factors. The study of weapons and weaponization is distinct from those areas. As security researchers, we will likely never know enough to predict when or why an attacker will employ a weapon, or where the weapon will be used. We can, however, identify how a weapon is constructed and improved, possibly leading to an understanding of the tool in greater depth than the wielders.

We evaluated the nature of weaponizing SMTP technology in three separate ways: monitoring and categorizing a year's worth of phishing attempts against a single target's customer base, by studying a trojan packaging system, and through a discrete attack.

2.1 Chasing it Down

During the twelve-month period from March 2006 through March 2007, we collected, catalogued, and analyzed fraudulent email messages targeting JP Morgan Chase (Chase) banking customers that arrived at a single email box [20]. Phishing scams routinely weaponize email technology itself, taking advantage of the inherent lack of authentication to deposit a counterfeit plea from "Chase" on the desktops of millions of potential victims. Attacks involving email in this manner have been categorized as "brand hijacking," a reference to well-known terrorist activities which involve arms of some variety.

Each of the scams employed the same goal: an attempt to get the recipient to click the provided link. None of the email collected carried an executable attachment. The front of the scams remained fairly constant, varying only the precise personal information they attempted to harvest from the victim. The attacks varied only the shells in which they traveled, from the victims' perspective, the "motivator" behind the message. This level of change is more than enough to make it difficult for defenders to filter scams based on subject lines, content, or sender addresses. Motivations were divided into five groups: a request to update information, a software update, an awaiting message at the Chase website, a financial incentive, or the use of fear (warning the account holder of a possible compromise to their account). The messages collected over the course of the year broke down as follows:

Table 1: Motivation breakout for JP Morgan Chase hhish (March 2006-March 2007)

Motivation	Percent of Total
Update Information	15.15
Update Software	4.55
Message	3.03
Financial Reward	18.18
Fear/Warning	59.09

Taking a routine confidence scam and adding official (yet publicly accessible) images, dire messages, and carefully-planned web fronts gives the scheme a distributable form, and it is readied for mass delivery via an illicit spam network [6, 14]. The lack of executable and extremely variable content makes distribution easy for the attacker.

2.2 mIRCy Waters

Communicability is an attribute of viral and bacteria-based illnesses, and one that is the goal of many attackers for their wares on the Internet. More importantly, this facet of weapons development is understood by even the least sophisticated coders that take part in illicit cyber crime. Internet Relay Chat (IRC) - based trojans, a large part of the Internet's bot net plague, come in all sizes and compositions. In most cases, the IRC client employed by the trojan author is mIRC. It is not uncommon to find the trojans behind these attacks introduced by innocuous sounding email messages, imploring the recipient to follow the included link to a software update, friendly greeting, or new game. Of course, the file retrieved from the linked location is not what it pretends to be and instead installs any number of applications on the new host.

Beyond changing the public face of the scam (the email message), the attacker has to continue the sham by making the downloaded code both easy to transmit and easy to overlook (once the lack of greeting or game is detected). In biological and chemical attacks, one means of improving distribution is making the particle size small enough to become aerosol-borne [12]. On the Internet, this "particle size" equates to the size of a piece of malware – which has been a strong delimiter: a 1MB trojan would be difficult to transfer across dialup circuits – technology overcame this factor and now large kit-produced trojans like Phatbot [6] are easily moved. Care is still required to ensure that a large file does not contain code that will trip generic signature sets, although that is not necessarily paramount to distributing the code to a broad audience.

The same is true for malware "collections" – attacks that require a number of utilities or configuration files to accomplish its mission. This is the case for many IRC-based bots, as they need to include configuration files to ensure the compromised machine

correctly reports back to the author-controlled channel. That handicap has been overcome by rudimentary packaging routines that place the contents into a self-extracting archive, generally a self-extracting archive (SFX) file (as the SFX format allows for scripting both the decompression routine and executing a file from the package). The single SFX file provides a means of taking the concept of a mIRC-based trojan to an improved form, in terms of weaponization. This was part of an "urgent update" collected by the author – there is little doubt as to its real nature:

```
004036D0  BB C0E75500    MOV EBX,explorer.0055E7C0
;  ASCII "agent"
004036D5  BE 7A9F5700    MOV ESI,explorer.00579F7A
;         ASCII     "*     Connect     retry     #5
London.UK.Eu.UnderNet.org (6667)"
004036DA  BD 7C1E5800    MOV EBP,explorer.00581E7C
;  ASCII "C:\WINDOWS\system32\mirc.ini"
```

Figure 1: "Urgent Microsoft Update"/IRC trojan snippet

The above actions are not invisible in the way modern rootkits are, but they are not clearly displayed to the general user either. The weapon is made deadlier by using a number of companion programs to hide the nature of the bot application. These files, such as the mIRC command script file "win.ini" allow the compromised machine to make a connection to the controller's IRC channel and await additional instructions. The routine is not complete, however, as win.ini calls other applications. One of which is a copy of HideWindow 1.43 by Adrian Lopez (circa 1996). The program makes visible windows invisible (and vice versa) to someone viewing the Desktop. It should be clear that the malware coder was somewhat handcuffed by the choice of execution routine, as the mIRC windows is quite visible during startup and is hidden only after a few seconds (as HideWindow/Window Hider is called by an already running copy of mIRC). This is an interesting decision on the coder's part, as the package could very well have had the IRC client begin out of view (minimized), or initiate the entire sequence with a separate file that ensured that Window Hider did its job as soon as mIRC began.

Although not necessarily sophisticated enough to impress most professional malware analysts, the exercise of creating a novel delivery system for even hastily cobbled together criminal schemes is the start of matching a weapon with a release mechanism.

2.3 The iPhony

Taking the incentive-based scam further, we studied the rash of iPhone-related fraud in July of 2007. Coinciding with the launch of the Apple iPhone, criminals distributed a flurry of emails, an attached image file, and a single link with the headline of "You have won an Apple iPhone!." The goal of the scam was to install a piece of malware on the victim's machine. The weapon employed was multi-staged: an email with official-looking graphics (in the same fashion as phishing attacks), and a link. When followed, the link opened a single HTML page ("index.php"), which included an encoded JavaScript routine (edited for space):

```
</script>
<Script Language='JavaScript'>
function    xor_str(plain_str,    xor_key){    var
xored_str  =  "";  for  (var  I  =  0  ;  I  <
plain_str.length;     ++i)     xored_str     +=
String.fromCharCode(xor_key                    ^
plain_str.charCodeAt(i)); return xored_str; }
var plain_str = "\xcc\xe1\xe6\xe1 [clipped here]
```

Figure 2: iPhone-based trojan download showing hexadecimal encoding of payload

It should be noted that the distribution system employed for this attack carefully kept track of the addresses that accessed the server and which browser made the request for "index.php." In cases where Microsoft's Internet Explorer or a repeat request was responsible for the request, no malicious content was transmitted back to the user. This intelligence allows the attacker to limit the exposure of their attacks, preventing casual researchers (and spiders) from retrieving the malcode. Once decoded, however, the script reveals the following content, now JavaScript escaped as a second layer of obfuscation (edited for space):

```
var mm = new Array(); var mem_flag = 0; function
h()  {mm=mm;  setTimeout("h()",  2000);}  function
getb(b, bSize) {while (b.length*2<bSize){b += b;}
b = b.substring(0,bSize/2);return b;}
function cf()
{var zc = 0x0c0c0c0c;
var a = unescape("%u4343… [clipped here]
```

Figure 3: iPhone-based trojan download payload without hex encoding

A final decode yields the original (edited for space) text of the script:

```
if (v[0] && v[1] && v[2]) {
var data = XMLHttpDownload(v[0], urlRealExe); if
(data     !=     0)     {     var     name     =
"c:\\sys"+GetRandString(4)+".exe";              if
(AD2BDStreamSave(v[1],  name,  data)  ==  1)  {  if
(ShellExecute(v[2], name, n) == 1) { ret=1; } } }
} return ret; }
function   start()   {   if   (!   MD2C()   )   {
startOverflow(0); } [clipped here]
```

Figure 4: iPhone-based trojan download payload without JavaScript escaping

The overflow installs another weapon, an SMTP engine likely to be used in future attacks. Increasing the deadliness of the attack by adding the installation of persistent malware, however, is only one of countless possibilities for the attacker. The script routines are weaponized by the layers of obfuscation, selected to ensure any browser will execute the code properly while dodging network protection measures. The encoding tools make the effort decidedly more deadly to the recipient as the exploit and associated malware can have any number of rounds and permutations of encoding in order to detonate unique revisions on multiple targets within even the most secure of networks.

3. APPLIED WEAPONIZATION

Understanding the weapons, often times better than the criminal wielders, we can change the battlefield. This has been shown to be effective in ballistics research, where firearm registration has been employed to successfully associate guns used in criminal acts with the perpetrators [28]. Biological virus strains used in crimes can be similarly fingerprinted, and although they are associated to an aggressor with less certainty, research and cataloging in this arena has been successful [11]. This is

analogous to the waning of successful "network-based" attacks (such as Smurf, teardrop, and LAND), we have come to know the weapons as well (or better) than those wielding them.

Focus on the weapons instead of their associated vulnerabilities would help solve a number of issues, such as that experienced with XML and SOA applications (popularly referred to as part of the Web 2.0), where preexisting HTML rendering issues plague the later technology [23]. More troubling, perhaps, is the nebulous nature of cyber weaponry currently, allowing for any Internet resident (whether self-defined as an attacker, defender, or passive participant) to employ technology that may ultimately be dangerous to the health of the entire community. The ease with which attackers combine weaponized components into their tactical efforts is shared with network protectors.

3.1 Weaponized Defenses

One can imagine the host of possibilities for employing offensive tactics to protect their respective organizations. While that approach may at first be rejected by the modern security practitioner, consider the variety of weapons that are part of such a strategy and accepted in varying degrees:

- Altering infrastructure (Routing, Name Resolution, etc.)
- Real-Time Block Lists (RBLs)
- Sending phony data to phishing front ends
- Trojanizing Honey-net documents

The use of artificial alterations to Domain Naming System (DNS) and routing entries has been part of many ISPs' practices for years. In the summer of 2007, Cox Communications took offensive action against bot masters by intentionally redirecting client machines that attempt to reach IRC command and control servers [24]. Once redirected, the clients were fed IRC commands by a Cox-owned device. The commands clearly intended to remove an IRC bot from the client machine. Not only does such action violate the spirit of what many Internet users may consider the "rules of the road," by altering infrastructure services arbitrarily, executing commands on a remote machine without user consent meets numerous definitions of malicious. Indeed, if the debate concerning the intent of the ISP is removed, there is little discerning the use of these IRC-based weapons from those employed by illicit enterprises. Infrastructure alterations of this nature are not limited to network services, indeed, the use of kernel patching techniques to fight malware is not uncommon – employing (and impeding the defense of) the same weapon used to install rootkits on unwitting client machines.

The RBL has been a part of many spam fighting security teams for years. Updated by various groups with the addresses of "known" spamming entities, RBLs can cause delivery and routing problems that are extremely difficult to track down when innocent networks are added by unreliable sources. In addition, using blocks as a weapon against domains and networks that did not take offensive action against the RBL-protected group is the foundation for a separate debate about taking online actions against suspected aggressors.

Every victim of phishing attempts (that is, every company whose brand is victimized) has likely considered offensive actions against the perpetrators. As described in the previous section, the plight of JP Morgan Chase serves as the context for engaging the cyber enemy through offensive action. If one is justified in automatically redirecting and removing software, and is free to accept lists from which service should be denied, there is little stretch required to use a weapon against a phishing server. Any organization, being besieged with not only attacks but also the liability of successful attacks, may see a remedy in knowing exactly what accounts have been compromised and blocking accesses to them. One well-intentioned SQL injection is all it may take to achieve this result. One persistent cross site scripting (XSS) "redirection" or simply a flood of fake data may be enough to alter the economic benefits of such a scam in favor of the "good guys."

A final example in this regard is the explicit trojanizing of organization-owned files. Placed in a darknet or honeynet, the files await retrieval by someone who has no business retrieving them. The use of the weapon in this case, a trojan, is possibly justified by the passivity of the attack. One would have had to break into a network that was (by design) off limits in order to find and execute the malware.

The development, storing, and positioning of weapons has a singular, inescapable conclusion: the use of the weapon. If any control is to be achieved over cyber weapons, whether in policy or technical form, the strict definition of how they are (or can be) developed, what they entail, and how and when they can be used must be completed. When otherwise innocuous or helpful technologies are weaponized, whether to initiate or defend against an attack, the result is an instable infrastructure. The risks of a policy based on offensive changes to routing schemes, DNS tables, and naturally generated network traffic may help to evade a singular attack. However, it comes with the cost of making network monitoring increasingly complex (and insecure [2]). Breaking the expected "rules of the road" for internal assets brings with it an eroded sense of trust that one can have in their logs, and especially logs from external networks.

3.2 Cyber Weapons Control

Advantages to cyber weaponization discussions include a much-improved understanding of the weapons, the possible policy choices, and the proper employment of cyber defenses.

Certainly implied by a discussion of cyber weaponization is the possibility of arms control across the Internet. This has been addressed in previous works [7] from a nation-state perspective. Beyond the control policies, there is the question of emergency response and preparedness that is more topical to most organizations today. Knowing, "how bad it could be" during a cyber attack is only fully realized when the capability of the weapon is understood. This is not simply a function of knowing what percentage of the discrete asset is compromised, but knowing the lethality [17] of the employed weapon.

Once again drawing on the bioweapon parallel, the response effort of modern military forces should be considered for application in the cyber world. With the study of advancements in biological weapons, the military community has realized the diminishing returns in detection mechanisms versus prevention and remediation. The same may be true of network-based threats. In the study of biological weapons, detection has been discounted as an expensive and logistically infeasible venture [12]. A gas-agent used against troops may be resident for detection for mere minutes, as opposed to liquid agents that made detection a reasonable course by lingering for hours. Consider that obfuscated code may be drawn into a browser or email client before

triggering any type of alert – meaning it is only considered malignant once assembled on a single machine at a single instance in time – detection must successfully extend to every client all the time.

Vaccination has been the de facto defense to biological agents, as the soldier (the "client" in this case) is known and accessible to the service (the "enterprise") prior to deployment. Of course, this relies on broad-based inoculations that can defend against many known weapons. In the cyber battlefield, this inoculation corresponds not only to generic firewall and malware rules, but also inoculating data against attack through encryption and self-destruct routines. Employing fast-acting antigens in the field has improved our defense against bioweapons – possibly "weaponizing the defense" is the right course in Internet security as well, but it will require a combined effort of nation states and private organizations to construct a policy that promotes nonproliferation.

Although often considered the antivirus software on a computer, an inoculation scheme for cyber assets may be better described as encrypting all sensitive data, separating as much of that data as possible from the public Internet, and employing multi-layer security (MLS) systems.

Efforts to control cyber weapons are hampered by confusion that results from a debate over what a weapon is, when it can be used acceptably, and what liability results. There is evidence that the exceptional ease involved in cobbling together powerful weapons in cyberspace may require a concerted effort similar to that behind the nuclear nonproliferation strategy [3] (no correlation, however, between the impact of nuclear and cyber weapons is intended by the author). In order to dispel myths about the precision and lethality of Internet-based weapons, and thereby efficiently balance both national and organizational security policies, additional work in the area of weapons definition and awareness is needed. As agents of destabilization, the cyber weapon, even those as simple as the SMTP-based exploits noted in the previous section, can have serious consequences for public and private network communications.

3.3 Countering Proliferation

Considering the near infinite permutations of offensive tactics available to attackers (and "defenders") is not the end of a discourse on Internet weaponization. As with potential battle spaces such as space [13] or the seas, simply placing offensive capabilities into the field is a concern to sovereign entities. Beyond the technical wonder of innovative exploits (which may be known as "vertical proliferation" to Internet governors of the future), the bot net explosions ("horizontal proliferation" perhaps) seen in the last few years may need the same approach as arms reduction treaties of decades gone by.

Arms proliferation on the Internet could certainly be met with any one of the following:

- Policy/Legal Export Restrictions (Keeping "dangerous" technology out of the hands of untrusted bodies similar to current cryptographic restrictions [25])
- Orders for Closed Source Software Development (Similar in logic to the above)
- Requiring All Software Packages to be Packed and Encrypted
- Trojanizing Selected Sensitive (Attractive to Attackers) Assets
- Geographic/Nation-based Blocks (DNS, Policy Based Routing, etc.)
- Overt Cyber Attacks

Without a plan for response actions, the defender's actions are likely to be as unpredictable as the attacker's. Successful policies will have the coordination and balance of arms control policies in the kinetic realm – nonproliferation and counterproliferation [3].

Knapp and Boulton explored the role of commercial and private organizations in cyber warfare [18], showing the responsibilities that all Internet residents have in future conflicts. Given this role, it is incumbent upon security practitioners and systems owners at all levels to understand the nature of various cyber weapons and their organization-sponsored response policies. There can be no distinction between a weapon's dangerousness when employed by an "attacker" than when it is wielded by a "defender."

4. FUTURE WORK

The policy implications of defining cyber activities as weaponization form the basis for our continuing work. As the world continues to define the battle space of the Internet, it will be increasingly more important to identify what constitutes weapons development and how both nation states and individual organizations will respond to construction, testing, and deployment of such weapons.

The foundation of meaningful work, however, requires an objective set of criteria for assessing cyber weapons. Currently, this takes the form of an equation, in which we propose the following, influenced by the work of Casadevall & Pirofski in microbial weapon potential [5]:

$$\text{Weapon Strength} = \text{Power} * \text{Communicability}$$

Power, in this case is proposed to be a function of the control ("C") a weapon gives an attacker over its target divided by how symptomatically the weapon is employed. Practically, control means the degree of freedom an attacker has within a system. Symptoms, much like the biological counterparts, are signs that the weapon has been employed successfully. Asymptomatic employment is designated as "A" below:

$$WS = (C/A) * \text{Communicability}$$

Communicability is estimated as the quotient of the susceptibility ("S") of its targets to successful attack from the weapon and the speed (represented as "T," for the time required) of deployment. The speed of a weapon is not necessarily the time it takes to act or to spread, but the time to attack all given targets, independent of the mechanism (self-propagation, mass mailing, etc.). All the values for this calculation are currently qualitative: low, medium, or high (for actually arriving at a value, 1, 2, and 3 can be used, respectively). The higher the result, the more powerful the weapon is, given the context in which the criteria were evaluated. That context is affected by contemporary defenses, Internet architecture, and user awareness. Future efforts are planned to refine the criteria and evaluation system.

$$WS = (C/A) * (S/T)$$

Under this scheme, it is possible to estimate roughly the strength of the weapons presented in section 2. At its heart, however, the calculation measures the danger in the respective components, the technology employed by each weapon. For the phishing efforts targeting Chase customers:

$$WS = (High/Low) * (Low/Low) = (3/1) * (1/1) = 3$$

For the "postcard" mIRC-bots:

$$WS = (High/High) * (Medium/Medium) = (3/3) * (2/2) = 1$$

And the iPhone customer-targeted Trojan:

$$WS = (Medium/Low) * (Medium/Low) = (2/1) * (2/1) = 4$$

For historical context, technology such as that employed in the Slammer/Sapphire worm would have been calculated as:

$$WS = (High/Medium) * (High/Low) = (3/2) * (3/1) = 4.5$$

The equation's worth as a definitive measure of how strong a cyber weapon truly is given a specific network environment is not meant to overshadow its value in pointing out how a weapon can be made more effective. The list of qualities that strengthen a biological weapon: deadliness, novel delivery, and distribution potential are reflected in the equation. Power, as represented above as control and stealth, is directly attributable to the "increase deadliness" improvements (as control) over the "novel delivery system" (as the weapons asymptomatic quality). Communicability, as susceptibility and speed, is echoed in the weapon's "distribution ease," and possibly its delivery system as well. Moreover, using an equation such as this to evaluate technology, rather than those things conceived of as traditional weapons, helps point to all technology as having worth as a weapon (also referred to as dangerousness to an enterprise). Using an objective framework for evaluating danger in Internet applications can help organizations address and prioritize threat capabilities of their adversaries.

The plethora of existing attack research has led to inroads in law enforcement. As a community, security researchers have been responsible for aiding in arrests and damaging the economic landscape of cyber crime [22]. However, the development and release of the cyber weapons themselves continues without detailed scrutiny. Our future research will extend the study of weaponization into a similar report focusing exclusively on web application attacks and development of the equation presented above. Additional work with regards to nonproliferation versus counterproliferation is planned.

5. REFERENCES

[1] Adams, J.: Virtual Defense. Foreign Affairs 80(3). May/June 2001. pp 98-112.

[2] Bernstein, D.: Some Thoughts on Security After Ten Years of qmail 1.0. Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, Chicago IL. CSAW'07. November 2, 2007, Fairfax, VA. Available at: http://cr.yp.to/qmail/qmailsec-20071101.pdf. Last retrieved 17 November 2007.

[3] Bredehoft, LtCol B.: Military Strategy for Combating Nuclear Proliferation. United States Army War College, Carlisle Barracks, Pennsylvania. March 2005.

[4] Cahill, T. P., Rozinov, K., Mulé, C.: Cyber Warfare Peacekeeping. Proceedings of the 2003 IEEE Workshop on Information Assurance pp 100-107. United States Military Academy, West Point, NY June 2003.

[5] Casadevall, A., Pirofski, L. The weapon potential of a microbe. TRENDS in Microbiology Vol 12 No 6 pp 259-263 June 2004.

[6] Dailey Paulsen, L. P2P Hacker Tool Poses Escalating Threat. Computer, IEEE Computer Society Vol 37 No 5 pp 2-3. May 2004.

[7] Davis, L.: Arms Control, Export Regimes, and Multilateral Cooperation. Chapter 12 in: Strategic Appraisal: The Changing Role of Information in Warfare. RAND Monograph Reports. 0-8330-2663-1. 1999.

[8] Denning, D.: Obstacles and Options for Cyber Arms Controls. Presented at Arms Control in Cyberspace, Heinrich Boll Foundation, Berlin, Germany. June 29-30, 2001. http://www.nps.navy.mil/da/faculty/DorothyDenning/publications/Berlin.pdf Last retrieved 16 November 2007.

[9] Denning, D.: Reflections on Cyber Weapons Control. Computer Security Journal Vol. XVI No. 4, Fall 2000 pp43-53. Also available (last retrieved 17 November 2007) at: http://www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc.

[10] Denning, D.: The Ethics of Cyber Conflict. Draft last retrieved 17 November 2007. http://www.nps.navy.mil/da/faculty/DorothyDenning/publications/Ethics%20of%20Cyber%20Conflict.pdf.

[11] Enserink, Martin. Anthrax: Taking Anthrax's Genetic Fingerprints. Science. November 30, 2001. Vol. 294 No. 5548 pp 1810 – 1812. http://www.sciencemag.org.

[12] Franz, D.: Defense Against Toxin Weapons. U.S. Army Medical Research and Material Command, U.S Army Medical Research Institute of Infectious Disease, Fort Detrick, MD. 1997. Available for review at: http://www.usamriid.army.mil/education/defensetox/toxdefbook.doc.

[13] Garthoff, R. Banning the Bomb in Outer Space. International Security. Vol. 5 No. 3 Winter 1980-1981, pp 25-40.

[14] Gordon, J. Agobot & The Kit-chen Sink. http://www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf. July 2004.

[15] Gordon, J., Linzey, J.: Years of the Beagle. January 2006. http://www.infectionvectors.com/library/years_of_the_beagle.pdf. Last retrieved November 2007.

[16] Grant, R.: Victory in Cyberspace: An Air Force Association Special Report. October 2007.

[17] Henry, R., Peartree, C. E.: Military Theory and Information Warfare. Center for Strategic & International Studies. Parameters Autumn 1998 pp 121 – 135.

[18] Knapp, K., Boulton, W.: Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. ISM Journal, Spring 2006 pp 76-87. Retrieved from http://www.infosectoday.com/Articles/cyberwarfare.pdf 16 November 2007.

[19] Libicki, M.: What is Information Warfare? National Defense University, Institute for National Strategic Studies, The Center for Advanced Concepts and Technology. August 1995. Available as PDF at: http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662&Location=U2&doc=GetTRDoc.pdf, last retrieved 16 November 2007.

[20] Linzey, J.: Chaser: A Year of JP Morgan Phish. March 2007. http://www.infectionvectors.com/library/chaser_iv.pdf. Last retrieved 14 November 2007.

[21] Merriam-Webster's Online Dictionary, weapon, http://www.m-w.com/dictionary/weapon.

[22] Moore, T., Clayton, R.: Examining the Impact of Website Take-down on Phishing. Anti Phishing Working Group (APWG) eCrime Researchers Summit. Pittsburgh, PA, USA. October 4-5, 2007.

[23] Orrin, S.: XML & Web 2.0 Threats You Never Knew About. Computer Security Institute 2007 Conference. Washington, DC. 2007.

[24] Singel, R.: ISP Seen Breaking Internet Protocol to Fight Zombie Computers – Updated. Wired, 23 July 2007. http://blog.wired.com/27bstroke6/2007/07/isp-seen-breaki.html.

[25] Stowsky, J.: Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age. Goldman School of Public Policy, University of California. Research Policy Vol. 33 Iss. 2 March 2004 pp 257-269.

[26] Thomas, T.: Is The IW Paradigm Outdated? A Discussion of U.S. IW Theory. Foreign Military Studies Office, Fort Leavenworth, KS. Journal of Information Warfare. 2003. Vol. 2 No. 3 pp 109 – 116. Also available for review from: http://leav-www.army.mil/fmso/documents/InfoWar.pdf (last retrieved 16 November 2007)

[27] Warrick, J.: The Secretive Fight Against Bioterror. The Washington Post, 30 July, 2006. Available via: http://www.washingtonpost.com/wp-dyn/content/article/2006/07/29/AR2006072900592_pf.html.

[28] Webster, D. Comprehensive Ballistic Fingerprinting of New Guns: A Toll for Solving and Preventing Violent Crime. Johns Hopkins Bloomberg School of Public Health, Center for Gun Policy and Research. Updated November 2002. http://www.jhsph.edu/gunpolicy/ballistic_fingerprinting.pdf.