Journal of Military and Strategic Studies

VOLUME 14, ISSUE 2, 2012

Wild, Unsubstantiated Predictions: The Future of Computer and Network Security

John Aycock

Introduction

To predict the future is to join the ranks of august company indeed: the Oracle of Delphi, John the Baptist, Shakespeare's Witches. It is also to entertain the very real possibility of being grievously, staggeringly wrong, although King Duncan may beg to differ. Undertaking such a task in a rapidly-changing area like computing technology is surely the epitome of foolishness, yet predicting the future in this area is precisely what this paper sets out to do. As this is a matter of sheer -- albeit somewhat informed -- speculation on my part, I will dispense with the traditional "academic we" throughout.

My goal is to predict the future of computer and network security over the short term leading to the medium term, approximately the span of the next five to ten years. For brevity, I will use the overhyped and overused "cyber" prefix (e.g., cybersecurity, cyberwar, cyberterrorism) despite its uncanny ability to send me into paroxysms of eye-rolling.

Predictions about cybersecurity are meaningless to make and to understand without first taking into account the context, the world in which these predictions are going to play out. I begin there, looking at the current technical and social context for cybersecurity. From there, I identify some key trends that I think underlie the next two sections: the future of attack and defense.

ISSN : 1488-559X

Context

I was part of the microcomputer age. My first computers, a Commodore PET and an Apple][e, practically begged to have their internals played with. In the former case, loosening two screws allowed you to lift the hood (quite literally; it even had a rod to hold the case open, just like a car). The Apple was even easier, with a case whose top panel could be ripped off *sans* tools. Once inside, the individual chips and components in the computers were ones that were widely available, and a knowledgeable user could swap parts or repair them. You could run any software you wanted, or develop your own. The entire machine was yours.

During this time, Orwell's year came and went and we all dutifully read *1984*. Constant state surveillance was part of some fictional dystopian future, it seemed, or something that happened in some Communist country far away. It was the Cold War and we knew who the enemy was and more or less where to find them if necessary.

Once I arrived at university, I was introduced to this amazing thing called the "Internet." This was pre-web, pre-Google, pre-general-public. It was a painful thing to use, in retrospect, where to search for information or software really *was* a search, manually sifting through one site after another. Yet still it was amazing: the ability to instantly, freely communicate with places all over the world. Unencrypted protocols like telnet and rlogin were used constantly, even though it was well known that they were insecure. Really, the chances of anyone having the capability and the incentive to eavesdrop or attack seemed remote indeed. This Internet thing had not shown up on governments' radar in any significant way; it was only in the years to come that governments would discover it and begin to puzzle over what it was and what to do with it. It was a different time.

My reminiscing is done for a reason. It is helpful to see where we are at now, technically and socially, and how much things have changed to this point before looking at the future. Clearly, some things are no longer legal or possible, something I expect to continue as we move forward. In the remainder of this section, I review the current technical and social context.

Technical Context

I will start at the computers we use and move outward. It is hard *not* to observe the rise of mobile computing; armies of head-bowed texters serve as a constant reminder. In terms of cybersecurity, I do not see these as terribly revolutionary, however. The threats that are occurring on them are primarily cases of old types of threats being repackaged. Furthermore,

the limitations of computing power that once dogged mobile devices are becoming less relevant with each new generation of more-powerful devices. Mobile devices are evolving into something akin to our desktop and laptop computers, just ones that happen to be easier to tote along.

What I think is important about mobile devices is that they are a clear embodiment of a trend that has been under way for years, just ensconced inside too-large computer cases. The microminiaturization of computer internals means that they soundly earn the label that used to be confined to the dusty backs of television sets: no user-serviceable parts inside. It's not that it's dangerous, though. It's simply becoming increasingly impossible for any human, regardless of training. Computing devices can't be repaired, can't be altered, can't be controlled by the user in the same way that they once could. The Apple iPad, for example, is reputedly very difficult even to take apart.[1]

On the software side, one interesting development has been the idea of a "walled garden," a controlled software and content ecosystem, of which Apple's iTunes is an exemplar. Arguably the vetting of software applications is a good thing from the point of view of cybersecurity, where it prevents malicious software from being installed on computers, but it also enables a large degree of control over what legitimate applications appear. The path for entry into the walled garden of the App Store is tightly controlled, complicated, and can constantly change.[2]

It is useful to remember, as we move from computers to the networks that connect them, that the Internet experience is not universal. Internet access in China, for example, is famously filtered through the so-called "Great Firewall of China"[3] that is able to block sites as well as watch network traffic for prohibited content in real time. Even in Western countries, allegations

---

[1] K. Wiens, (2012, 15 March). New iPad teardown. http://ifixit.org/1843/new-ipad-teardown/.

[2] J. Gruber, (2010, 9 September). A taste of what's new in the updated App Store license agreement and new review guidelines. http://daringfireball.net/2010/09/app_store_guidelines. See also; N. McAllister, (2010, 3 June). How to get rejected from the App Store. *InfoWorld*. http://www.infoworld.com/d/developer-world/how-get-rejected-the-app-store-854?page=0,0; and J. Snell, (2010, 9 September). Apple's App Store guidelines go deeper than Adobe. *Macworld*.

http://www.macworld.com/article/1153993/app_store_guidelines.html.

[3] OpenNet Initiative. (2009, 15 June). Internet filtering in China.

http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf.

of monitoring Internet traffic[4] and of censorship (e.g., the Opennet Initiative, 2010, notes "Australia's Internet censorship regime is strikingly severe") already exist. And this monitoring and censorship makes a nice transition to the social context.

Social Context

Once upon a time, I would have naively thought that monitoring and censorship, especially without oversight, would immediately fall afoul of the law. No longer. Fueled by a war on terror, legislators have been emboldened to pass and attempt to pass some surprising and dismaying laws. For example, hot on the heels of the September 11 attacks, the United States' Patriot Act effectively extended their legal jurisdiction to the entire Internet, redefining their notion of a "protected computer" to be "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States".[5]

The desire for governments to put monitoring legislation into place seems now to vary only by the particular rationale that they use to justify it, and how little oversight will be required. Besides the old justifications involving counterterrorism, anti-piracy, and protecting children, there are relative newcomers like Olympics security.[6] The UK has been particularly active in this legislative area of late, both in monitoring[7] and censorship.[8] Canada is no

[4]Wired. (2006, 17 May). AT&T whistle-blower's evidence. http://www.wired.com/science/discoveries/news/2006/05/70908.

[5] United States. (2001). Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) act of 2001. Public Law 107-56, 107th Congress.

[6] D. Barrett, (2012, 18 February). Phone and email records to be stored in new spy plan. *The Telegraph*. http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html. See also; McCaskill, S. (2012, 20 February). UK government to demand data on every call and email. *TechWeek Europe.* http://www.techweekeurope.co.uk/news/uk-government-to-demand-data-on-every-call-and-email-61583.

[7] BBC News. (2012a, 1 April). Email and web use 'to be monitored' under new laws. http://www.bbc.co.uk/news/uk-politics-17576745. See also; BBC News. (2012b, 2 April). Warning over need for safeguards in email and web monitoring plan. http://www.bbc.co.uk/news/uk-politics-17580906; and A. Faiola, & E. Nakashima, (2012, 2 April). Britain weighs proposal to allow greatly increased Internet 'snooping.' *Washington Post*. http://www.washingtonpost.com/world/europe/britain-weighs-proposal-to-allow-greatly-increased-internet-snooping/2012/04/02/gIQAOerQrS_story.html.

shrinking violet either, with similar monitoring legislation being proposed recently; the Minister of Public Safety, in a masterstroke of hyperbolic rhetoric, painted critics of the bill as siding with child pornographers.[9]

Another legislative trend is the influence of corporate interests on government via lobbying efforts. This is particularly visible in the area of copyright and intellectual property, with bills like SOPA and PIPA (MacKinnon 2011; McCullagh 2012).[10] Digital locks on content, such as those supported in the latest Canadian copyright law reform (Schmidt 2012), are another example. Cynically, one could observe that these seem like attempts by established industries to avoid adapting to new business models, by legislatively trying to slow technical change. I would also link it back to the walled garden from the last section, as an attempt to control what a user can do, see, and run on their computer.

In the cybersecurity arena, fledgling high-profile attack efforts have been seen. Because of the difficulty identifying attack sources, actors,[11] intents, and sometimes even targets, it is hard to label some cybersecurity events with any certainty: is an event cyberprotest/hacktivism? cyberterrorism? cyberwar? The only thing that can be safely said is that we have seen what some of these events might look like. From Estonia being denied service[12] to Stuxnet affecting uranium enrichment facilities in Iran[13] to attacks by groups like Anonymous,[14] this may be a glimmer of things to come. This may seem like a subject better suited to be considered as part of

---

[8] T. Brewster, (2012, 18 April). MPs want ISPs to block porn by default. *TechWeek Europe*. http://www.techweekeurope.co.uk/news/mps-isps-block-porn-default-73519.

[9] CBC News. (2012, 13 February). Online surveillance critics accused of supporting child porn. http://www.cbc.ca/news/technology/story/2012/02/13/technology-lawful-access-toews-pornographers.html.

[10] R. MacKinnon, (2011, 15 November). Stop the Great Firewall of America. Op-ed, *The New York Times*. http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html?_r=4. See also; D. McCullagh, (2012, 18 January). How SOPA would affect you: FAQ. *CNET News*. http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/.

[11] I use the term "actors" in a general sense, simply meaning the person or persons responsible for an act. For reasons argued later, I do not think there is a need to make further distinctions into state vs. non-state actors.

[12] The Economist. (2010, 1 July). War in the fifth domain. http://www.economist.com/node/16478792.

[13] M. Clayton, (2010, 30 November). Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program. *Christian Science Monitor*. http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program.

[14] New York Times. (2012, 8 March update). Anonymous (Internet group). http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous_internet_group/index.html.

the technical context, but in fact there is precious little new here from a technical point of view -- even in the case of the mighty Stuxnet.[15] The more interesting part is that these attacks are in response to social, real-world things.

Finally, one easy thing to forget is that the demographics of the Internet are shifting. According to recent estimates,[16] developing countries now possess well over half of the world's Internet users, and approximately one in four Internet users are in China. In terms of the social context, any new users may bring different ideas, social mores, and priorities; in pragmatic terms, there is potential for a large new labor pool for cyberattack and defense.

Key Trends

My cybersecurity predictions can now be seen in their proper technical and social context. The linchpins for these cybersecurity predictions are the trends I predict in this section. These trends can be seen as contextual trends following on from the previous section.

> **Prediction 1.** The big thing in the next 5-10 years is not technology. The big thing that will affect cybersecurity the most is political and social reaction to technology.

We now have plenty of technology. While there will undoubtedly be more and more of it, I do not think that technology will have the biggest impact. Instead, there seems to be a growing awareness of the impact of technology on our lives, how it can dominate our waking hours, how our privacy is being lost either because we give up information or because it is taken from us via surveillance. Not everyone is comfortable with these developments.

At the same time, government seems to be moving a lot faster with respect to technology when it comes to regulation and legislation. There is general acknowledgment of the reliance -- and often overreliance -- of our society and its critical infrastructure upon technology. Making matters worse is the fact that so much of the technology we rely on can be, to be extremely polite, less than resilient. The implications of this technology being disrupted by cyberattacks, either in realistic scenarios or science fiction cyberbogeymen, are worrisome to the people in charge. In some places, the correct functioning of technology itself is an ongoing problem, if the free exchange of ideas is seen as disruptive to the status quo.

[15] For the explanation, see; J. Aycock, (2011, September). Stux in a rut: Why Stuxnet is boring. *Virus Bulletin*, pp. 14-17.
[16] International Telecommunication Union (ITU). (2011). The world in 2011: ICT facts and figures. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

With such unprecedented fears, it is perhaps natural that government and many regular users long for simpler times. It is natural to want to close ranks, to retreat back to a comfort zone. What is the comfort zone? Governments are used to thinking and operating in nationalistic terms, are comfortable with national boundaries. Regular users are comfortable with communities which, in a broad sense, may be interpreted to be a variety of groupings: friends and family, a religious affiliation, a physical area, a team, a company, a country.

Prediction 2. Fragmentation in the Internet will become increasingly apparent and established over the next 5-10 years.

With a willingness to be in cocoons of comfort, there is very little impetus overall for free, open exchange of data, content, and ideas. I predict that the Internet will begin to reflect this in more ways than it does now.

Eric Schmidt, from Google, was quoted as saying

> "To some, the openness and interoperability [of the Internet] is one of the greatest achievements of mankind in our lifetime. Do not give that up easily. You will regret it. You will hate it, because all of a sudden all that freedom, all that flexibility, you'll find it shipped away for one good reason after another."[17]

I would argue that Schmidt has missed the point, or more precisely has made the correct point but too late. The fragmentation of the Internet has already occurred.

We do not have an "openness" on the Internet now. To assert otherwise is to delude ourselves. National policy creates forced, and sometimes enforced, divisions through legislation. Governments censor content for one reason or another. Social media emphasizes popularity and sharing amongst like-minded individuals, creating a virtual fragmentation, a barrier to the different and unpopular. Customized search results cut out possibilities somehow deemed to be not as relevant. I will call these fragments "zones" not in reference to an area but in reference to comfort zones.

The different types of zone are as varied as the imagination and not necessarily limited to physical location, although each country having a national zone is perhaps the most obvious

[17] B. Woods, (2012, 29 February). Schmidt: UN treaty a 'disaster' for the internet. *ZDNet UK*. http://www.zdnet.co.uk/news/regulation/2012/02/29/schmidt-un-treaty-a-disaster-for-the-internet-40095155/.

division. Iran is apparently trying to create such a zone, for one.[18] I will focus mostly on national zones here, but religion could also play a role, leading to a Christian zone, an Islam zone, a Judaism zone, and so on. History suggests that we are good at exclusion, and zones may also, if inadvertently, create an overlooked "virtual ghetto" and aggravate the digital divide.

The next step beyond recognizing that zones exist is to enforce them, to prop them up with technology. I envision that computers will start being made that are restricted to communicating within a specific zone, a restriction in the hardware itself similar to DVD region encoding. Recall that hardware is becoming much more difficult to modify, making it increasingly hard to defeat any zone-specific restrictions; I would not be surprised to see a coup de grâce delivered in the form of a glue with good heat dissipation properties, so that computer hardware would literally be glued shut and unmodifiable. These hardware restrictions continue the theme of the user having less control over their computer in favor of the computer manufacturer and content providers, and align nicely with zoning initiatives.

At the network level, zone structure can be mirrored in the network design by creating choke points where one zone connects to another (assuming, of course, that they do at all). This leaves an obvious location for monitoring and filtering traffic. Internet traffic is then very much a national policy. Free-trade treaties could be struck to give preferred countries unfettered access to a national zone. The decision over what to do with transmissions from a computer imported from a foreign zone, and therefore having a foreign zone identifier, can be national policy too: route the traffic out of the zone? drop the packets? let the traffic move freely within the zone? It is tempting to imagine a zone rating service, an Internet equivalent of *Moody's*, that would label the trustworthiness of traffic from zones, but that belies the highly dynamic nature of network traffic (and cyberattacks). For operational reasons, I think that the expression of policy as it applies to packets will need to be done within a national zone without recourse to outside agencies, in order to be resilient and responsive.

Another consideration is how zones impact entities that routinely communicate across boundaries, such as multinational corporations. In that case, I would expect internal communication to be permitted across zone boundaries, from identified corporate network

[18] F. Fassihi, (2012, 6 January). Iran mounts new web crackdown. *Wall Street Journal.* http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html. See also; K. McCaney, (2012, 10 April). Iran building a private, isolated Internet, but can it shut out the world? *Government Computer News*. http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx.; and R. Paul, (2012, April). Iran moving ahead with plans for national intranet. *Ars Technica*. http://arstechnica.com/tech-policy/news/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative.ars.

addresses in one zone to its identified addresses in another. It is only when corporate traffic is sent externally that it would become subject to any zone limitations. What I foresee would be "zone shopping," akin to forum shopping for legal jurisdictions, where a multinational would choose to have all its externally-destined traffic routed internally so that it appears to be sent from the least-restrictive zone.

I should point out that fragmentation into zones is not intrinsically a bad thing. One effect that zones might have, if carefully established, is to increase the signal-to-noise ratio by blocking out irrelevant content. Something else to remember is that, as evidenced recently by the Arab Spring, zones may be(come) areas of greater freedom rather than lesser freedom. The point is simply that different Internet zones have different rules.

Future Attacks

On now to the future. What attacks will we see, and who will be attacking?

From a technical point of view, I think that those expecting wildly new, unanticipated attacks are going to be pleasantly disappointed. I have argued elsewhere[19] that one true test of a watershed, game-changing threat is where our defenses *must* be changed in order to defend against the threat. This does not happen that often; the vast, vast majority of threats are derivative and easily caught with existing technology. Furthermore, when our defenses do need to be changed in any significant way, it is not because of one special case. It is because there are enough instances of a problematic threat that a general defensive solution is necessary, whereas special cases are unique by definition and can be dealt with defensively as one-off events. One nice side effect of this notion is that there will be ample warning before our defenses need any major overhauls.

Having said this, I am not willing to rule out better forms of existing attacks. There are lots of cases where adversaries already have exploitable resources at their fingertips that they are not taking full advantage of. For example, there are many computers, especially mobile ones, that have microphones, and there is potentially monetizable data in their audio stream.[20]

[19] J. Aycock, (2011, September). Stux in a rut: Why Stuxnet is boring. *Virus Bulletin*, pp. 14-17.
[20] J. Aycock, (2010). The Ear of Sauron. *Hackin9, 5* (11), pp. 12-13. See also; R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, & X. Wang, (2011). Soundcomber: A stealthy and context-aware sound Trojan for smartphones. *18th Annual Network and Distributed System Security Symposium*.

Why is this data not being exploited? There are ways to send "better," more convincing spam[21] where a compromised computer is mined for its user's email-sending characteristics, that are then used to automatically custom-tailor a spam message. Why is this not being done? There are different business models, where an adversary can monetize stolen data, without needing to know what data is valuable;[22] by establishing an infrastructure that allows other parties to search compromised computers or bid on interesting stolen data, the adversary becomes data broker. Why is this business model not used?

I think the answer lies, in part, in economics. There is no business case to be made to invest in developing a new attack, new malicious software, or new *modus operandi* when the old ones are working well enough and generating enough revenue. As our defenses improve over time and some old attacks become infeasible or at least less profitable, I expect economic pressure will drive adversaries to create variants on existing attack themes. (Of course, as defenders we would like to pat ourselves on the back for making adversaries' lives more difficult, but it may turn out to be a reaction to the tragedy of the commons, where the population of vulnerable people and systems just gets overexploited. This was explored in relation to phishing by Herley and Florêncio.)[23] While this covers financially motivated adversaries, i.e., most of them, there are some other groups that require additional consideration; I will return to them in a moment.

The gradual increase of software in walled gardens, and the gradual increase in controlling computing activities by computer vendors and governments, must be taken in the context that we really have little idea how to build massive, robust, bug-free software systems. Even if the software is controlled, there will still be bugs present in it. The presence of a bug does not automatically mean that the bug is exploitable, but it does point to an general overall weakness that is hard to fix; it would take a massive leap in software engineering technology to solve the problem of bugs, one that has proved elusive for decades. There already exist markets for sales of exploitable software bugs, and as software is increasingly controlled, I predict that the demand for these will increase, along with the price that a good exploit will command.

[21] J. Aycock, & N. Friess, (2006). Spam zombies from outer space. *15th Annual EICAR Conference*, pp. 164-179.

[22] N. Friess, J. Aycock, & R. Vogt, (2008). Black market botnets. *MIT Spam Conference*, 8pp.

[23] C. Herley, & D. Florêncio, (2008). A profitless endeavor: Phishing as tragedy of the commons. *New Security Paradigms Workshop*, pp. 59-70.

Google itself just raised the maximum reward it will pay for finding bugs in its services by over 500%, to $20,000.[24]

My final technical prediction is that adversaries will invest in long-term infrastructure that can benefit their operations and be amortized over many attacks. We see the desire now for adversaries to have robust infrastructure, using (for example) techniques like fast flux and domain flux[25] to make shutting them down difficult. It seems reasonable that an adversary might try to establish their own domain name system, for instance, similar to efforts to keep pirate sites alive.[26] In the distant end of the range of time I'm predicting, perhaps adversaries might even try their hand at physical infrastructure, keeping their critical command-and-control sites alive by keeping them aloft with ever-cheaper and more capable drone aircraft. An unsubstantiated report claimed that the Pirate Bay might be considering something like this already.[27] Adversaries' physical infrastructure may well be used in attempts to subvert the zone structure and its restrictions, giving rise to cross-border data smugglers.

Let me now return to who might be mounting these attacks. I have already discussed financially motivated adversaries, but of course there are other adversaries to consider. These "others" are not the people who engage in cybercrime, but the ones whose goal is cyberwar, cyberterror, and cyberprotest. These are just the ones who have a goal of some kind; for completeness we must also consider random actors too, who just want to see Rome burn and engage in disruptive activity for no apparent reason. The truth is that everyone with a networked computer is potentially a threat.

We need some way to reason about this situation, where everyone is a virtual danger. Traditionally it would be natural to try to determine the affiliation of our adversaries, to both understand their intent and to guide any potential response. But here, I think the situation will change to one where an affiliation will be *assigned* to an adversary. What do I mean by this? I

---

[24] G. Keizer, (2012, 23 April). Google boosts web bug bounties to $20,000. *Computerworld*. http://www.computerworld.com/s/article/9226476/Google_boosts_Web_bug_bounties_to_20_000.

[25] W. Salusky, & R. Danford, (2007, 13 July). Know your enemy: Fast-flux service networks. Honeynet Project. http://www.honeynet.org/papers/ff/. Last modified 16 August 2008. See also; Ollmann, G. (2009). Botnet communication topologies. Damballa white paper. http://www.damballa.com/downloads/r_pubs/WP_Botnet_Communications_Primer.pdf.

[26] Ernesto. (2012, 18 March). The Pirate Bay attacks censorship with low orbit server drones. *TorrentFreak*. http://torrentfreak.com/the-pirate-bays-attacks-censorship-with-server-drones-120318/.

[27] Ibid. See also; R. Miller, (2012, 19 March). Low-orbit servers? Or a Pirate prank? *Data Center Knowledge.* http://www.datacenterknowledge.com/archives/2012/03/19/low-orbit-servers-or-a-pirate-prank/.

think that the follow-on to enforced zones is a push for some level of attribution for network traffic. A mechanism for incorporating this has been being developed and rolled out slowly for over a decade: IPv6, whose larger address space would allow some bits to be co-opted for this purpose. In the simplest case, a computer's hardwired zone identifier could be used as a label, providing a coarse-grained affiliation for traffic, adversarial and otherwise. At the more extreme end of the scale, network traffic could have a verified source address that identifies the originating device and/or the originating user (slightly different, as one device may be used by multiple users, and one user may use multiple devices). This becomes a tradeoff with anonymity, where a person can be anonymous within a zone or not anonymous at all, and is another policy decision.

With this mechanism, there would now be an affiliation imposed on adversaries, regardless of their real affiliation. Any attack-related traffic would bear the mark of its originating zone. Zone boundaries would act as firewalls, where any traffic from without claiming to be from within would be discarded, along with traffic with invalid or absent origin information. It could be argued that an adversary would still just lie or use compromised computers, but with attribution to a zone, especially a national zone, there is an excellent incentive for self-policing of traffic and dropping mislabeled or malicious outbound traffic. The incentive is that there would then be a zone to blame, and appropriate action can be taken to respond in the virtual or physical world.

This leaves us with a binary classification of cyberattacks: originating inside the victim's zone, or outside the victim's zone. Attacks from inside a national zone would fall under national legal jurisdiction and could be traced, a task made more or less difficult depending on the level of anonymity within the zone; attacks from outside a national zone could be throttled, blocked, and responded to. We would be extending our physical borders into cyberspace. (One interesting side effect is that it extends the idea of neutral countries into cyberspace. A neutral zone, with apologies to Star Trek, could act as a trusted network traffic broker between two other zones, possibly throttling or filtering traffic en route.)

My classification may seem incomplete, because I have not separately addressed whether an attack is an act of war, terror, or protest. That is because it doesn't matter. In computer terms, they can be responded to in the same way. True, an act of cyberwar or cyberterror may be accompanied by a coordinated physical attack, but again the "cyber" aspect of the response is the same. We do not need to build special computer defenses for any of them, since they all may employ the same techniques and target the same things.

While a homogeneity of response may make sense from a technical standpoint, it does present some difficulties from a legal standpoint, in particular for military action. Who, for example, is a combatant and thus eligible to be targeted under the Law of Armed Conflict?[28] However, it is misleading to assume that this body of law is static and must be applied as is to future cyberattacks. I suggest that new protocols and amendments to the law will be needed to properly address cyberattacks, rather than trying to fit square pegs in round holes.

Future Defenses

I mentioned Shakespeare in the introduction, and there's something to be said for a good play; the theater is compelling. Malware like Stuxnet may not have been game-changing from a security point of view,[29] but it did serve to help bring the issue of cyberattacks into the popular consciousness. One dangerous result is that the desire to react in some visible way may lead to cybersecurity theater, the virtual analogue to the security theater that we buy tickets to see enacted by the *dramatis personæ* in airports. Imposing overzealous cyberdefense measures with negligible or no impact is a danger that we must always be mindful of,[30] especially if our computers and networks are to be more regulated.

And regulation is the operative word. It would be inconceivable that our roads or the vehicles on them would not be regulated, yet we allow our computers and our networks to operate with almost no regulation whatsoever. This situation will change rather dramatically once zones are firmly established. The price of admission, for a computer's traffic to flow in the zone's network, is that security software must be allowed to run on it. This security software may be one of two types. First, the software may permit a malware infection to be cleaned up remotely, hence allowing easier threat mitigation. Second, the software may be part of an active defense, that would allow defensive, or "good" malware that would attempt to spread, locate, and eradicate other malware. This is an idea which comes up periodically (the Japanese are one

[28] Judge Advocate General, National Defence Canada, (2012). Combatant Status. Chapter 3 in *Law of Armed Conflict at the Operational and Tactical Level*. http://www.forces.gc.ca/jag/publications/oplaw-loiop/loac-ddca-2004/chap03-eng.asp. Last modified 2 February 2012; retrieved 22 June 2012.

[29] J. Aycock, (2011, September). Stux in a rut: Why Stuxnet is boring. *Virus Bulletin*, pp. 14-17.

[30] In fact, a recent study (Anderson et al. 2012) suggests that, at least for cybercrime, investment in defense is wildly out of proportion to the effect the attacks have. See; R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, & S. Savage, (2012). Measuring the cost of cybercrime. *11th Workshop on the Economics of Information Security*, to appear.

of the latest to look at it, as mentioned in *The Daily Yomiuri*),[31] but one of the sticking points is its legality;[32] legislative changes within a zone could allow defensive malware, however.

All this will still not rid us of security problems. As I mentioned in the last section, increasing pressure will cause adversaries to gradually evolve along with defenses. We could take the counterintuitive approach of letting adversaries win once in a while, to try and slow down their need to evolve,[33] but even if we could give this perverse social assistance to cybercriminals, it would offer little comfort for cyberwarriors who have a target in mind. In any case, we see adversaries winning quite enough already, and in the long term we need to move away from the idea that we want all computers to be safe all the time, because it's not possible. We need to accept this fact and shift our focus to managing the reality that some computers will be infected.

Finally, let us not forget the changing demographics. One viewpoint is that this yields armies of Mechanical Turks for cyberattacks, but I prefer to think that vast amounts of human power may also be leveraged in ways yet unimagined for cyberdefense. This may be an opportunity, and newcomers to the Internet may be its salvation.

Conclusion

It is hard to draw conclusions about anything when predicting the future. In fact, one could argue that this entire paper has been a series of conclusions arrived at by looking at the current technical and social context.

I have prophesized a fundamental change in how we perceive and use the Internet and our own computers, one requiring legal, policy, social, and technical changes. It is natural to want to apply judgment to this scenario, and label it as good or bad, when in fact it may simply be different than that to which we are now accustomed. At the very least it is a familiar future, as the boundaries we know in the physical world are extended into cyberspace.

As for computer and network security, the attacks that concern us won't go away. They will, however, be made manageable and understandable in a traditional legal and policy context.

---

[31] The Daily Yomiuri. (2012, 3 January). Govt working on defensive cyberweapon / Virus can trace, disable sources of cyber-attacks. http://www.yomiuri.co.jp/dy/national/T120102002799.htm.

[32] V. Bontchev, (1994). Are "good" computer viruses still a bad idea? *3rd Annual EICAR Conference*, pp. 25-47.

[33] J. Aycock, (2011, September). Stux in a rut: Why Stuxnet is boring. *Virus Bulletin*, pp. 14-17.

Even for skeptics, who may not subscribe to the full-blown vision of the future I've laid out, I hope that this has provided some food for thought. In particular, it serves as a framework for thinking about the Internet as a fragmented entity -- an *already* fragmented entity -- where the pieces can be regulated and policies applied at a national level.

Acknowledgments

Thanks to Jörg Denzinger and Anil Somayaji for helpful discussions and suggestions, as well as the panel members at the workshop where this paper was presented: John Adams, Ron Deibert, Harvey Rishikof, and John Sheldon.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. *11th Workshop on the Economics of Information Security*, to appear.

Aycock, J. (2011, September). Stux in a rut: Why Stuxnet is boring. *Virus Bulletin*, pp. 14-17.

Aycock, J. (2010). The Ear of Sauron. *Hackin9, 5* (11), pp. 12-13.

Aycock, J. & Friess, N. (2006). Spam zombies from outer space. *15th Annual EICAR Conference*, pp. 164-179.

Barrett, D. (2012, 18 February). Phone and email records to be stored in new spy plan. *The Telegraph*. http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.

BBC News. (2012a, 1 April). Email and web use 'to be monitored' under new laws. http://www.bbc.co.uk/news/uk-politics-17576745.

BBC News. (2012b, 2 April). Warning over need for safeguards in email and web monitoring plan. http://www.bbc.co.uk/news/uk-politics-17580906.

Bontchev, V. (1994). Are "good" computer viruses still a bad idea? *3rd Annual EICAR Conference*, pp. 25-47.

Brewster, T. (2012, 18 April). MPs want ISPs to block porn by default. *TechWeek Europe*. http://www.techweekeurope.co.uk/news/mps-isps-block-porn-default-73519.

CBC News. (2012, 13 February). Online surveillance critics accused of supporting child porn. http://www.cbc.ca/news/technology/story/2012/02/13/technology-lawful-access-toews-pornographers.html.

Clayton, M. (2010, 30 November). Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program. *Christian Science Monitor*. http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program.

The Daily Yomiuri. (2012, 3 January). Govt working on defensive cyberweapon / Virus can trace, disable sources of cyber-attacks. http://www.yomiuri.co.jp/dy/national/T120102002799.htm.

The Economist. (2010, 1 July). War in the fifth domain. http://www.economist.com/node/16478792.

Ernesto. (2012, 18 March). The Pirate Bay attacks censorship with low orbit server drones. *TorrentFreak*. http://torrentfreak.com/the-pirate-bays-attacks-censorship-with-server-drones-120318/.

Ernesto. (2010, 30 November). BitTorrent based DNS to counter US domain seizures. *TorrentFreak*. http://torrentfreak.com/bittorrent-based-dns-to-counter-us-domain-seizures-101130/.

Faiola, A., & Nakashima, E. (2012, 2 April). Britain weighs proposal to allow greatly increased Internet 'snooping.' *Washington Post*. http://www.washingtonpost.com/world/europe/britain-weighs-proposal-to-allow-greatly-increased-internet-snooping/2012/04/02/gIQAOerQrS_story.html.

Fassihi, F. (2012, 6 January). Iran mounts new web crackdown. *Wall Street Journal*. http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html.

Friess, N., Aycock, J., & Vogt, R. (2008). Black market botnets. *MIT Spam Conference*, 8pp.

Gruber, J. (2010, 9 September). A taste of what's new in the updated App Store license agreement and new review guidelines. http://daringfireball.net/2010/09/app_store_guidelines.

Herley, C., & Florêncio, D. (2008). A profitless endeavor: Phishing as tragedy of the commons. *New Security Paradigms Workshop*, pp. 59-70.

International Telecommunication Union (ITU). (2011). The world in 2011: ICT facts and figures. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

Judge Advocate General, National Defence Canada, (2012). Combatant Status. Chapter 3 in *Law of Armed Conflict at the Operational and Tactical Level*. http://www.forces.gc.ca/jag/publications/oplaw-loiop/loac-ddca-2004/chap03-eng.asp. Last modified 2 February 2012; retrieved 22 June 2012.

Keizer, G. (2012, 23 April). Google boosts web bug bounties to $20,000. *Computerworld*. http://www.computerworld.com/s/article/9226476/Google_boosts_Web_bug_bounties_to_20_000.

MacKinnon, R. (2011, 15 November). Stop the Great Firewall of America. Op-ed, *The New York Times*. http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html?_r=4.

McAllister, N. (2010, 3 June). How to get rejected from the App Store. *InfoWorld*. http://www.infoworld.com/d/developer-world/how-get-rejected-the-app-store-854?page=0,0.

McCaney, K. (2012, 10 April). Iran building a private, isolated Internet, but can it shut out the world? *Government Computer News*. http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx.

McCaskill, S. (2012, 20 February). UK government to demand data on every call and email. *TechWeek Europe.* http://www.techweekeurope.co.uk/news/uk-government-to-demand-data-on-every-call-and-email-61583.

McCullagh, D. (2012, 18 January). How SOPA would affect you: FAQ. *CNET News*. http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/.

Miller, R. (2012, 19 March). Low-orbit servers? Or a Pirate prank? *Data Center Knowledge.* http://www.datacenterknowledge.com/archives/2012/03/19/low-orbit-servers-or-a-pirate-prank/.

New York Times. (2012, 8 March update). Anonymous (Internet group). http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous_internet_group/index.html.

Ollmann, G. (2009). Botnet communication topologies. Damballa white paper. http://www.damballa.com/downloads/r_pubs/WP_Botnet_Communications_Primer.pdf.

OpenNet Initiative. (2009, 15 June). Internet filtering in China. http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf.

OpenNet Initiative. (2010). Australia and New Zealand overview. http://opennet.net/sites/opennet.net/files/ONI_AustraliaandNewZealand_2010.pdf.

Paul, R. (2012, April). Iran moving ahead with plans for national intranet. *Ars Technica*. http://arstechnica.com/tech-policy/news/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative.ars.

Salusky, W., & Danford, R. (2007, 13 July). Know your enemy: Fast-flux service networks. Honeynet Project. http://www.honeynet.org/papers/ff/. Last modified 16 August 2008.

Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., & Wang, X. (2011). Soundcomber: A stealthy and context-aware sound Trojan for smartphones. *18th Annual Network and Distributed System Security Symposium*.

Schmidt, S. (2012, 13 March). Copyright bill to clamp down on digital-lock pickers. *Postmedia News*. http://www.canada.com/news/Copyright+bill+clamp+down+digital+lock+pickers/6296108/story.html.

Snell, J. (2010, 9 September). Apple's App Store guidelines go deeper than Adobe. *Macworld*. http://www.macworld.com/article/1153993/app_store_guidelines.html.

United States. (2001). Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) act of 2001. Public Law 107-56, 107th Congress.

Wiens, K. (2012, 15 March). New iPad teardown. http://ifixit.org/1843/new-ipad-teardown/.

Wired. (2006, 17 May). AT&T whistle-blower's evidence. http://www.wired.com/science/discoveries/news/2006/05/70908.

Woods, B. (2012, 29 February). Schmidt: UN treaty a 'disaster' for the internet. *ZDNet UK*. http://www.zdnet.co.uk/news/regulation/2012/02/29/schmidt-un-treaty-a-disaster-for-the-internet-40095155/.