Software [In]security: Cyber Warmongering and Influence Peddling

By Gary McGraw and Ivan Arce

Date: November 24, 2010

Gary McGraw & Ivan Arce explain how the current climate of exaggeration and FUD surrounding cyber attacks does not ultimately serve the best interests of computer security research — or our country.

In a domain where statements like "attacking the phishing problem," "mitigating bugs," and "tracking worms across the world," make perfect sense only to insiders, it is little wonder that policy makers and CEOs are confused about cyber security. The (perhaps intentional) conceptual roll up of cyber crime, cyber espionage, and cyber war into the scariest of cyber boogeymen exponentiates the FUD factor, making an already gaping policy vacuum more obvious than ever before. Policy makers must approach this vaccuum warily and ponder the situation carefully. Only fools rush in where angels fear to tread.

Much of the confusion stems from the sloppy nature of cyber war discourse. In June 2010, this column took up the concept of cyber war and introduced the notion of "kinetic impact" to separate the wheat from the chaf. Then came Stuxnet, which for all intents and purposes appears to be a real cyber war offensive weapon. Still, many aspects of the cyber war discussion in the United States continue to worry even our friends and allies around the world, not to mention a few of us patriotic citizens.

It is hard even for experts to understand what is real and what is cyber chimera. How much of what we're hearing is driven by the hype that keeps money flowing through the US military industrial complex? How much of it is something that we need to worry about, and who should do the worrying?

More to the point, if the hype and fear engines ran out of fuel for a day, leaving only even-handed and well-reasoned analysis, how would we describe the current situation and begin to architect an approach for improvement?

Our aim in this article is to provide some guideposts for policy makers so that they may find their way through the fog and set policy that spares the goose that laid the golden egg.

Real Cyber War?

In June we introduced the notion of "kinetic impact" to the discussion in order to tease apart certain cyber attacks and differentiate cyber espionage, cyber crime, and cyber war. As we said, the "war" part is fairly straightforward (violent conflict between societies for political, economic, or philosophical reasons). Having tangible impact in the real (non-cyber) world seems to be an important part of cyber war. In our view, cyber war requires what war theorists call a "kinetic" aspect to be present. Put another way, an attack in cyberspace needs to have impressive kinetic impact of some sort out in the real world to be considered an act of war. So, if we can infect your command and control system with malware that gives us complete control, and then cause your predator drones to shoot at the wrong targets (a kinetic impact), that would count as an act of cyber war.

There are some well-understood examples of real cyber attacks going back decades that are worth reviewing:

- In 1982, stolen Canadian computer code (modified by the CIA) caused a Soviet gas pipeline to explode.
- In 2007, the Israelis took out the Syrian air defense system with a cyber attack before bombing a partially constructed (North Korean designed) Syrian nuclear facility to smithereens.
- In 2008, a USB drive in the Middle East was used to infect US Department of Defense command and control systems (both classified and unclassified), prompting Deputy Secretary of Defense William Lynn to say in Foreign Affairs, "…this previously classified incident was the most significant breach of US military computers ever, and it served as an important wake-up call."
- In 2010 (and perhaps earlier), the Stuxnet worm was used to attack nuclear centrifuge uranium enrichment facilities in Iran. Analysis of the Stuxnet situation continues to this day.

It is worth noting that exactly none of these cyber attacks led to a full-fledged war — cyber or otherwise — regardless of the obvious kinetic impact.

It is also worth noting that sober-minded senior thinkers in cyber security are deeply concerned about vulnerability and the risk of attack. Dr. Dan Geer, Chief Information Security Officer of In-Q-Tel — a very careful thinker indeed (and an important antidote to cyber hyperbole) — stated unequivocally, "Cyber insecurity is the paramount national security risk". We agree.

Imagined Cyber War!

Of course the net is crawling with charlatans, ridiculous stories, and warmongers as well. The most outlandish of these stories are also worth a glance:

- In 2007, the country of Estonia was subjected to deliberate distributed Denial of Service (dDoS) attacks. Cyber pundits described the attacks as very sophisticated and unprecendented, even though it is clear that the very same techniques would have proven about as irritating as a gnat to Amazon or Google. Hyperbole over simple-minded denial of service attacks does nobody any good.
- In 2009, CBS aired a segment of its 60 Minutes show that attributed several blackouts that occurred in Brazil in 2005 and 2007 to unidentified cyber attackers. Brazil's top cyber security officer denied the allegations. A few days after the show aired, a major blackout hit a Brazilian region prompting renewed speculation of cyber attacks. Within a few days, the

discovery of SQL injection bugs in the power company's website by a Brazilian IT security student provided only feeble evidence in support of the claim. In spite of clear claims to the contrary, the event fueled another bout of cyber warmongering. In March 2010, the Brazilian Electricity Regulatory Agency released its final report on the November 10, 2009 blackout. There was no mention of cyber attacks. The blackout was the much more pedestrian result of a combination of operational and procedural failures from one electric power supplier company, which was promptly fined $90M.

- In 2010, ridiculous and dangerous stories of a Chinese mistake with BGP protocol management were hyped into some kind of malicious "hijacking" of 15% of US-based Internet Traffic. Not only were the actual traffic numbers in question inflated, misused, and stretched well past the breaking point, sadly the US Congress seems to be taking the story seriously. (For the real and much more boring numbers, see Arbor Network's analysis.) BGP is broken and needs to be fixed. Assigning malicious intent to mistakes using BGP is foolhardy and ignorant.
- Even non-events such as the spotting of a jet contrail off of the coast of California are picked up and twisted into cyber attacks based on not one iota of evidence.

The problem with these kinds of stories is that they have somehow worked their way to the halls of policymakers who repeat them without critical analysis. For every careful Dan Geer there are ten shrieking cyber security talking heads busy stirring the pot saying things like, "We may call it espionage, but it's really warfare. They're planting logic bombs," while offering no actual evidence of such.

Because of all this, security pundit and firewall inventor Marcus Ranum has a well-traveled talk entitled, "Cyberwar is Bullshit." But is it?

A View from Outside the States

Iván Arce (guest co-author of this month's column) lives in Argentina. Gary McGraw regularly travels overseas. We note with some concern that the cyber war discussion is an issue that almost exclusively emanates from US policy makers and media outlets and it is largely tailored for domestic US consumption.

In that context, it is understandable — although questionable — that participants resort almost exclusively to the rhetoric of war to discuss cyber security. Further, they debate the issue as a matter of elucidating domestic policies that balance the demands of the US military-industrial complex, the US intelligence community, and the burgeoning IT and cyber security industry.

What makes us particularly skeptical is the intentional blurring of the lines that helped to distinguish the military, the intelligence community, and the cyber security industry — a direct result of US government pouring of billions of dollars into the burgeoning maw of perpetual cyber security initiatives.

In all modern countries the prospects of war serve as rallying cry; a call to action that galvanizes the people towards the common goal of mutual defense. The US embarked on two simultaneous wars during most of the last decade, and is clearly aligned against other identified foes (Iran, North Korea, and, quite possibly, China) — so conceptualizing cyber security as a constituent of warfare doctrine seems only natural. In this context, a call to arms for cyber war — albeit based on the flimsiest of evidence — makes sense as a tactic to mobilize the large pool of resources required to tackle the problem.

To foreign spectators, however, this sole focus is rather odd.

First of all, cyber security is not only and solely a military problem but rather a complex network of intertwined economic, cultural, diplomatic and social issues. Ignoring myriad dimensions by over-focusing on military aspects alone looks to be a losing strategy.

Second, cyber security is global and international in nature. The Net recognizes no geographical or sovereign boundaries, and simply does not follow the rulings of various individual real world nation-states. This point is particularly salient when we consider a few facts: less than 15% of Internet users are actually US citizens; a large portion of the US information technology and security work force is composed of foreign nationals; and, the supply chain for the global IT market is not actually a chain but rather a complicated web heavily weighted towards non-US actors.

Third (and most important in the grand scheme of things), the vast majority of the world's population (and proportionally its Internet users) seems to be totally uninterested in giving anything more than passing attention to cyber security if it is perceived as equal parts US cyber war doctrine and US domestic political debate.

All these things being said, some guidance is probably better than no guidance at all. However, considering cyber security an exclusively military affair thus setting US policy on the matter on collision course with reality is an unlikely way to achieve success.

Cyber War Cheerleaders, Economics, and Broken Analogies

Some people believe that the kinds of cyber warmongering that we're currently witnessing is all about money. They point out that those beating the cyber war drums the loudest are at least partially responsible for the sorry state of affairs in computer security. Retired Director of National Intelligence (DNI) Admiral Mike McConnell bears the brunt of this criticism, as do one-time NSA Director and Deputy DNI General Mike Hayden, and one-time cyber czar Richard Clarke. We know all of these men and they are all honorable and careful. Like us, they are all capitalists as well.

At the very least, all three men understand how much dependence we have on systems riddled with security defects. Unfortunately, by and large, they posit mirage solutions based on defending networks and building better cyber weapons instead of proposing that we build better systems in the first place. This is like walking right up to the elephant in the room, turning away to the bar, and mixing yourself a martini.

For years in computer security, we have been attempting to protect the broken stuff from the bad people by placing a barrier between the bad people and the broken stuff. We have failed. Instead, we need to fix the broken stuff so that attacking it

successfully takes far more resources and skill than is currently the case. Discerning new ways to exploit the broken stuff or hunt and kill the bad people more rapidly will not alleviate our dependence on vulnerable cyber systems.

Perhaps the most concerning problem from a policy perspective is the default ceding of the entire cyber domain to the Department of Defense. Way back in July 2009, this column singled that very move out as the one thing that the US government should not do. The argument against such move was based on two concerns:

1. The potential inability of the National Security Agency (and the rest of the Intelligence Community) to recognize and enforce a separation of duties and to effectively de-conflict cyber offense from cyber defense. Simply put, putting the same people in charge of securing the very systems they are currently exploiting for spycraft is crazy.
2. Vast cultural differences exist between the DoD/NSA and the rest of the civilian government/corporate America. The lack of a very clear command and control structure and chain of command in the civilian/corporate world makes adopting the military approach to computer security much less likely to work.

Nobody seems to have listened.

We now have a fully operational Cyber Command focused on reactive security and stood up to protect the networks of the military industrial complex in the US. The strategy emphasizes development of an impressive offense capability (the cyber equivalent of the F-22) sometimes referred to as cyber sharpshooters.

One of us (McGraw) put the separation of duties question straight to General Hayden during a public meeting and he replied that in his view, cyber power is like air power where separation of duties leads to failure. For what it's worth, this is a classic US Air Force belief with which we do not agree.

Meanwhile, civilian networks which account for at least 90% of our cyber exposure are left swinging in the wind. The problem is that even Cyber Command is focused on reactive computer security — protecting networks, seeking out bad guys and malware, and attempting to protect our broken stuff more effectively than the enemy protects theirs. Nobody in the government seems to be devoting much time and effort to carrying out an agenda of security engineering, software security, and building things properly. Meanwhile we all suffer the consequences of broken, vulnerable systems. We are exposed.

Guideposts for Policy

Confusion among policy makers when faced with the enormity of the cyber security problem is no surprise. We offer these simple guidelines to help:

- Cyberspace has a completely different physics than any other domain. It is impossible to "take and hold" cyberspace. Cyberspace is a dynamical system that runs at super human speed. There is no there there; and the clocks run near light speed.
- A good offense is NOT a good defense. Instead, a good defense is the ONLY defense. Throwing a better, more accurate rock in a glass house is still throwing a rock. Our systems are so permeated with problems that even an untrained child can exploit them.
- Divide and conquer will not work. Civilian, government, and military systems are so deeply entangled that they cannot be separated and protected distinctly. The nature of the entanglement is the people who interact with the systems. Just as military and civilian social groups mix in complex and unpredictable ways, so too do the information systems that those people use.
- Cyber crime and cyber espionage are more important than cyber war. The (very) bad news is that shiny new cyber weaponry will be repurposed for crime and spycraft — reason enough to take pause before charging ahead with offense.
- The good news is that fixing the broken stuff will help simultaneously combat crime, war, and espionage.Public/private partnerships pander politically but they do no real good. As it turns out, security is not a game of ops centers, information sharing, and reacting when the broken stuff is exploited. Instead, it is about building our systems to be secure, resilient, survivable, and trustworthy.
- No security is perfect and problems will happen. Even if a large portion of taxpayer money and collective know-how is dedicated to the task of building better, more secure systems, mistakes will still be made and systems will still be attacked and compromised. Cyber security policy must be built on the assumption that risk cannot be completely avoided, meaning that systems must continue to function even in sub-optimal conditions.
- If it sounds like bullshit or magic, it's probably not true.

In final analysis, cyber security policy needs to focus its attention on solving the software security problem and fixing the broken stuff. Multiple verticals in the commercial marketplace have already made great progress on this problem, much of which has been measured and described by the BSIMM. The government is years behind — even the military. When bits are money, the invisible hand will move to protect the bits. Of course, the invisible hand must be guided by the sentient mind and slapped hard to correct the grab reflex if and when it happens. There is an active role for government in all this, not just regulation, but monitoring and enforcing due process and providing the right incentives and disincentives. In the end, somebody must pay for broken security and somebody must reward good security (only then will things start to improve). Determining who is who, which is which, and how best to apply these concepts is a matter for government.