CYBERWAR: REALITY, OR A WEAPON OF MASS DISTRACTION?

Andrew Lee
ESET, USA

Email andrew.lee@eset.com

ABSTRACT

Over the last few years, in its insatiable thirst for the new, the security industry has increasingly co-opted military terminology for its marketing, and in return obliging government and military offices (particularly, but not exclusively in the western world) have predicted dire and terrifying scenarios. Couching the threats in the terms of modern warfare, spiced with the magic of 'Cyber', security wonks insist we exist in a new world of CyberWar, CyberTerrorism, CyberAttacks and CyberEspionage where devastation and carnage to our most sacred institutions lurk only a mouse-click away.

Following these now well-worn mantras, nation states are gearing up their budgets and their personnel to track, mitigate, offensively counter and defeat these 'new' threats. But where is the evidence? Do we really exist in this strange new world, where we must add to the usual loosely amalgamated mix of malware authors, criminals, hacktivists, jihobbyists and straight up vandals, the spectre of sinister hacker cells deployed by nation states? Or, are these ideas simply a case of paranoia fuelled by undirected angst about real-world, boots-on-the-ground warfare and the endless 'wars' on drugs and terror? Is security dialogue being hijacked by hype and political expediency? Perhaps the constant exposure to the fantasy and science fiction novels so beloved of the über-geek has fed into the security industry's hero complex wherein we become the fantastical knights in shining armour (or long leather coats, depending on your milieu), deploying our Low Orbit Ion Cannons against the evil (but faceless) phantoms of the global military industrial complex.

PART I: CYBERWAR (WHAT IS IT GOOD FOR?)

'It is an illusion to believe that because you are powerful, you must always use force.'
– Robert DuBois

There is a kind of groupthink that kicks in within the security industry each time something interesting happens that sticks out from the ordinary flood of malware that hits our labs every day. Once a 'story' malware breaks, there is a scramble by vendors to find out first, if they are detecting it; second, to reassure their customers that detection is in place; and third – and this is the nub – to provide some fresh or interesting commentary to the media or in blog form (not necessarily in the stated order). This is fairly natural, given the need to promote our companies' thought leadership, but can lead to overly speculative commentary, especially when coupled with the equal and supporting need of story-hungry journalists to have new content, or, in some cases, just more than one source for commentary.

So, Stuxnet starts out as a reasonably interesting piece of malware, with a connection to Iran. It's complex, but there are many complex pieces of malware. However, it is one of the few 'lucky' pieces of malware that gains a second life as a media meme. This spread is also viral. Should one be interested to do so, one could compare a graph of the media 'outbreak' to a typical malware outbreak graph and one suspects they would look very similar. Speculation abounds as to who is behind the malware, and some suggest that it is impossible that it could have been created without the intervention of a nation state. Why? Do governments hold the monopoly on complex software? One only need look at a typical anti-malware product to know that private companies – some of them very small – produce some of the most complex and intricate software programs in the world. Given that Stuxnet probably was state sponsored – and various sources eventually confirmed this [1, 2] – was the hype around it really justified? Is it really so surprising that in the day and age of globally connected networks, states are exploring the possibilities of using those networks for offensive purposes? But, should this sort of intervention be something that the ordinary person must worry about?

Possibly maybe

The anti-malware industry is a relatively small one in terms of number of researchers, therefore there is a constant tension between the small ecosystem that generates reasonably accurate threat information, and the less expert (in the specific matter of malware analysis), but more widely available opinion makers and pundits of the overall security industry. This means that a quote from one researcher, who may well be offering a preliminary analysis or early information, can be built up and speculated upon almost endlessly, until we have the sort of perfect storm situation that leads to something like that which we have seen with Stuxnet, or the Estonian attacks. This spiralling speculation was most recently seen (at the time of writing) with the 'Flamer' trojan/worm/toolkit. Despite few people having ever actually seen it, and fewer still having had a chance to perform a full analysis, there was rapidly escalating speculation about its source and purpose. Here we find the main danger of these sorts of pronouncements. Clearly, this is an area in which pure research – the decoding of bits and bytes and the detection of yet another threat – falls over into the domain of the political world. Politicians have seats to defend (or win), national defence organizations (and the private companies that contract for them) have money to spend/make and they all may have their reasons for promoting the idea that the government should spend more on 'CyberWar Defence'; the most promising way to achieve this end is to create spectres of fear in the media and play on the public's need for reassurance. Therefore, budgets are allocated, working groups are spun up, contracts are awarded and everyone (except the taxpayer) gets rich on Cyber WarFear.

Peace sells, but who's buying?

Unfortunately, at the point at which a debate becomes politicized, there is little that anyone, expert or not, can do to

reduce the impact that this will have. Even within the industry there are those who have clearly recognized the publicity value of building their brand on the subject of CyberWar. The proliferation of books, articles and sound bites is testament to the viral (pun intended) spread of the current interest in CyberWarfare issues.

But, can we truly classify a cyber-attack as an act of war? Under any normal description of war, I don't believe so. Thomas Rid stated:

'*Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria.*' [3].

Further, acts of war typically provoke retaliation in kind. When a nation state is attacked by another, this will normally imply a state of war between the two states. But is it realistic (or desirable) to count the sort of attacks that malware is capable of, as acts of war? To quote Tony Guo:

'*The proponents of "cyber war" evoke images of large explosions, poison gas clouds, and a high degree of mortality. In reality, cyber warfare is a misleading metaphor, and has long been confused with crime and espionage. "Cyber war" is not an issue of war, but an issue of security – systems security, network security, and due diligence on the part of its operators.*' [4].

This seems like a reasonable statement. The key element here is whether there has been violent or destructive force deployed with political purpose, deliberately instigated by a nation state for the purpose of causing harm to or mortality within the population of another state. DDoSing a country for a couple of hours or breaking some centrifuges in a nuclear processing facility doesn't really count as a violent act, and it remains indeterminate as to the usefulness of the attacks in a scenario of war.

Consider the attacks on Estonia as an example (oft cited) of CyberWar. Arguably, Estonia is now in a better position than ever it was to deal with future technological interference [5]. Perhaps there really is some truth in the old epithet 'What doesn't kill you makes you stronger'. It remains to be seen whether Iran will emerge more resilient to such attacks in the future. The fact that they found Flame seems to indicate that there is at least a growing awareness. Of further interest in the case of Iran is that the attack malware used was targeted against machines running *Microsoft Windows* – a platform (along with all other US-written software) that can only have been pirated [6].

Perhaps one action that can be taken by for nation states worried about the exploitation of common software vulnerabilities as a delivery method for cyber-attacks is simply to move to other systems (which incidentally do not need to involve piracy). After all, while there has been a huge drive (often for economic reasons) to create systems that are globally communicative and interoperable, it is possible to impose more control and establish borders simply by taking different choices in deployment of hardware and software [7]. The current interoperability of our major systems equally opens the attacker to threats; given that the Internet is a global system, how can one be sure that disruption to an enemy's systems does not similarly damage the systems of other, possibly allied, nations, nor your own?

PART II: MASTERS OF WAR

In his book *America the Vulnerable*, Joel Brenner points out that '*the Kosovo conflict is sometimes described as the first war on the Internet, but Kosovo did not involve a battle to take the Internet down or control its use.*' [8].

Rather Kosovo was a traditional 'boots-on-the-ground' conflict, but one that also involved a struggle for hearts and minds in which the Internet was the main tool.

Governments and others with political motivation competed to put out their own stories and attack each other in propaganda. Hackers and activists were active in defacing web 'territories' of both sides. In a phenomenon that has become much more common in the recent decade, the people also became the media. Individuals used their blogs and email to outside journalists to describe the horrors they saw, and thereby used the global power of the Internet to make their cause known. In these days where the brutality of the Arab Spring was widely documented on *YouTube* via video made on smartphones, this hardly seems worth commenting on, but at that time, access to the Internet was an incredibly powerful tool, and it was used by both sides. Indeed, Brenner also points out that:

'*As long as NATO wanted to use the Internet, it had to allow its enemies to do so – as such there were no targets to "hit". Indeed, the Serbs did use it, spoofing bombing targets with faked decoy tanks and aircraft (some even with heat sources); the fact that NATO had real-time aerial footage of 'success' only added to the confusion. Later, studies of after-action photographs of supposedly destroyed armour would disclose the truth. By corrupting NATO's information flow, the Serbs had significantly reduced the importance of air superiority.*' [8].

Can cyber-attacks be an adjunct to more traditional warfare? Surely. If one can digitally disrupt or disable the communications and critical infrastructure of an enemy, then this can certainly be seen as useful in the presence of other attacks, but without those other attacks, what is there to distinguish cyber-attacks from, say, espionage or sabotage (neither of which necessarily implies a state of war)? Of course, our increased reliance on all things cyber also makes non-digital sabotage possible on a grand scale in the form of the electromagnetic pulse. While EMP weapons sound very sci-fi and cyber, they are nevertheless kinetic. They physically destroy digital capability and thus one can argue they don't belong in the CyberWar conversation (nation state malware may be the least of the problems faced by the target of an EMP device successfully deployed in anger, and a kinetic response would seem inevitable).

Cyber-attacks, if used carefully, certainly seem as if they could provide tactical advantage in ways that are not physically harmful and that do not require troop deployments [9].

That being said, is it helpful to consider CyberWar as a realized concept? I'm not sure that it is. Thomas Rid makes a good point:

'*Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people*.' [3].

The necessarily lax definitions of war that we must create to invoke CyberWar seem to me to be generally unhelpful. Indeed, they seem to be largely acting as a distraction. While there may be some elements of truth to the idea that nation states are attempting to develop cyber-weapons, there is a larger truth, namely that what we, as the general public, face every day in terms of exploitation by malware is far more likely to do us harm than any real or imagined threat from CyberWarfare by, say, China or Iran.

It is this distractive force (a weapon of mass distraction?) that is often ignored in the writing of CyberWar stories. Perhaps it is fulfilment of those dreams many of us (usually as children) imagined ourselves part of; stories of valour and adventure wherein we became heroes – now, every one of us can become a CyberWarrior, valiantly defending our nations against the evil malware empires of those who would wish us harm. The reality is, of course, more mundane – we see hundreds of thousands of new malware samples every day in our labs, and we grind through them, improving detection, updating against heretofore unseen threats and bearing the slights of the rest of the security industry who still, after 25 years, have no idea what it is our software does.

Not only that, but the need to provide PR around what it is we do does indeed fuel the need for us to find things that might be 'interesting' to a wider audience.

And now, we reach the fundamental flaw in the cyber-weapon scenario – it may have taken six months to fully analyse Stuxnet – but it probably took about five minutes to provide detection for it, and to ensure that no system protected with AV software would even be affected by it. When one imagines the number of hours that went into developing Stuxnet, it is surely quite ironic that it takes so little to undo all of that work. One does not need to understand or analyse a piece of malware to be able to detect it. As one writer put it: '*Cyber is unique in that you're giving away your weapons, tactics, the design of them, etc. simply by using them*.' [10].

The art of self destruction

Who has most to lose in a true 'CyberWar'? Is it states like Iran, who have barely dragged themselves out of the middle ages (though in part they have been held back due to the constant interference and intervention of the West), and like many third-world or developing countries still rely largely on paper-based systems, or is it states such as the USA that rely almost entirely on computerized and networked systems for every aspect of life? As Mikko Hyppönen recently noted, '*The United States has the most to lose from attacks like these. No other country has so much of its economy linked to the online world*.' [11].

This then, would be asymmetric warfare in its purest sense, and yet we are led to believe that the USA fired the first shot. Have we not now sent to the world the message that 'we are armed and ready to shoot'? Perhaps we have already 'declared war' if we are to accept that these attacks are acts of war. If so, then we have made ourselves extremely vulnerable.

While Iran may have had a few setbacks to its nuclear program, it is now perhaps 'justified' in responding in kind – perhaps the Iranian government is even now building its own cyber-strike troops. I was certainly surprised to find that Iran has a CERT: what is its purpose now? It's not hard to imagine that a major task might be to expose weaknesses in common software and develop exploits to deploy against found vulnerabilities. How about other states? It's likely that China and its client states such as North Korea are also involved in building out their cyber-missiles. Because of the nature of these 'weapons' we are vulnerable, because we have already given our enemies everything that they need to compromise us – the systems on which we run the Internet and our everyday operating systems are all available to our enemy, along with examples of our own weapons.

We are, unfortunately, experiencing something of a perfect storm. In one corner we have many security mavens who, for whatever reasons, wish to posit the idea that CyberWar is already upon us, in another we have government institutions which are always happy to find new ways to spend money on capability (both offensive and defensive) that does not necessarily involve putting expensive troops in the way of harm (this avoids the political unpopularity that conventional warfare brings to a government). These are buoyed up by contractors and vendors with 'expertise' and products to sell. In the third corner is a media hungry for the latest scare story and willing to print almost any quote about CyberWar, no matter how inane. Finally, in our fourth corner, we have a general public made nervous by the rise of militant Islam, cowed by the threat of international terrorism, and alarmed at the economic progress (however illusory) of states such as China.

In this environment the idea of CyberWar finds fertile ground and grows, fertilized by layer upon layer of increasingly shrill speculation – to a point where everyone believes it exists, simply because so many people are talking about it (and writing books and papers on the subject). It bears remembering that until very recently, despite the claims and speculations, there existed little actual evidence that Stuxnet/Duqu/Flamer were created by nation states, yet it was hard to find any article that did not mention this as 'fact'. That said, as I asked earlier: now that we have reasonable grounds for accepting that these were state-sponsored attacks, how do we separate that from the sort of normal inter-state espionage or sabotage that goes on?

If we classify something that is essentially 'spyware' (in an exact usage of that term) as a weapon, then we also need to understand that surveillance cameras (whether left in a rock on the street in Moscow [12] or attached to spy satellites and aircraft), wiretaps and global email and phone call collection systems must be classified in the same way. This takes us out of the realm of spying (which goes on all the time, even between ostensibly allied countries) and into one where we must redefine warfare as 'anything that anyone does to us that we don't like'.

Even if a government has used malware in a political context or even for some scale of sabotage I find it unhelpful to equate such activities with acts of war. What we do know is that by (admitting to) attacking an enemy who has little to lose (and who knows we are unlikely to resort to kinetic options), we have not only lost the moral high ground, but we have needlessly thrown away a key attribute of cyber-attacks – lack of attributability. It is this that we will discuss next.

I shot the sheriff (…but I didn't shoot no deputy)

One of the major reasons malware has been as successful as a tool of the criminal is that it is very hard, typically, to tell who did what. In the case of the more successful criminals, there is a trail of stolen and laundered money that can sometimes be traced back to the attacker. However, there's so much malware out there that it's hard to tell in the noise what is going on. Malware authors, hackers (at least the minimally competent ones), online activists (Hacktivists), political dissenters and others with a need for anonymity have found it in spades on the Internet – it's easy to hide, and there's so much else happening, it's also easy to plausibly deny involvement.

This turns out to be a much larger problem in the context of CyberWar. Who is the enemy?

The production of malware (or cyber-weapons) is very hard to detect until it has been released; typically it's an indoor activity done on closed systems disconnected from the Internet [13]. There's no way of spotting 'troop movements' or 'massing forces' on the ground. When there are tests of capability, it is hard to pull those out from the general noise, even when the attack is fairly major.

Deploying a botnet-based DDoS attack, whether for extortion or as patriotic protest, is fairly simple and largely untraceable. DDoS attacks are a widely used cyber-attack weapon and sometimes impossible to counter [14], so they are the most likely route a nation state might take to disrupt operations (e.g. banking) in another country – and nobody would ever need to know. Indeed, one can imagine situations where DDoS botnets are crowd-sourced for patriotic reasons (similarly to the way LOIC was deployed by supporters of Anonymous), with little response short of turning off your own Internet feed. While DDoS attacks are a strong weapon, they can't really be counted as a violent act and are pretty much useless for anything other than annoyance purposes. A DDoS might be an attention-grabbing protest piece (as are defacements of high-profile sites), or disruptive to some types of surveillance or reporting technology, but it's not really CyberWar.

So, this leaves more targeted attacks – attacks more like Stuxnet in character. The more effective attacks would require a high degree of targetability and thus investment, and while it may be possible to carry out such attacks with a higher degree of deniability than more conventional sabotage (lost backpackers anyone?), in general, the more targeted the more likely it is the victim will be able to discover the purpose and perhaps origin of the attacker. It has been pointed out that in CyberWar '*a country's assets lie as much in the weaknesses of enemy computer defences as in the power of the weapons it possesses*'. [15]. The more advanced the defences, the more likely detection is, thereby incurring higher risks that highly targeted attacks will be directly attributable. You can be sure that Iran is already working hard on upgrading its network defences and detection capabilities since the discovery of Flamer.

There are also issues of collateral damage and friendly fire. A conventional weapon can be very precisely targeted and the damage contained within a given area (with the exception of the fallout radiation from nuclear weapons). However, when it comes to malware, this has proved very difficult – for instance, Stuxnet even affected systems in the USA. Indeed, one might well ask why Stuxnet would ever need to replicate, since its delivery required an insider at the Nataz facility[1] [2] – the fact that it spread outside of its target area gave it undesirable detectability. Detectability comes with consequence – in this case worldwide media frenzy and the embarrassment of having to own up to having shot first, not to mention the immediate obsolescence of the deployed weapon.

The vast majority of crime and espionage enabled by the Internet goes unpunished (and indeed uninvestigated). It is only once the case becomes high profile (or embarrassing) enough, such as the Lulzsec attacks of 2011, that investigation might take place, and then it turns out that good old police detective work (and putting up the threat of jail time to enforce cooperation) is usually enough to figure out who did what. The more destructive or invasive the attack, the more effort will be put into chasing down the perpetrator. Deploying a destructive cyber-weapon brings with it the very real possibility of retaliation against the attacker, perhaps with conventional kinetic responses.

Since an act of 'CyberWar' certainly would merit investigation, we need to be prepared to act accordingly. If we classify all cyber-attacks as acts of war, then we will need to be prepared to download our kinetic forces or take military action every time a SCADA system is compromised by malware or a government website is defaced. I doubt that this is practical or desirable (unless you're the budget holder for a large government organization, or a vendor selling 'CyberWar Preventer 2012').

If something is counted as an act of war but you are not prepared to respond as if it were so, then this simply exposes your weakness – so there is little point in such classification.

Further, with the US government having 'owned up' to instigating cyber-attacks, other governments will feel little reason to withhold their own cyber-weaponry. For instance, states such as Germany have now revealed that they have 'offensive capacity' [16].

Army of me

It's worth mentioning Hacktivism here. Groups such as Anonymous (and they are groups, not a single entity) do not clearly fit into any framework, and yet they are often considered alongside the CyberWar phenomenon. Perhaps it is convenient for governments (or media) to think of them as terrorists or from a militaristic point of view, however, this is not necessarily helpful or correct. Does a group, or groups of loosely affiliated cyber-activists (or vandals, depending on your take) with a barely related set of aims, constitute a force of cyber-warriors? No matter that they might be focusing their Low Orbit Ion Cannons squarely against some embarrassingly public targets (isn't that the point of protest, that it should be visible and embarrassing?), it does not seem sensible to suggest that this is so.

We are on deeply shaky ground if we are to claim that activities which range from the silly vandalism of the young and idealistic to deeply felt and desperate acts of legitimate protest should be

[1] I seem to recall Mikko Hyppönen asking this question somewhere, but unfortunately my *Google*-fu is not up to finding where.

equated with the actions concomitant with military acts of aggression against a state. To conflate the activities of groups such as Anonymous with CyberWar is simply ridiculous (that is not to say there should be no response).

It's clear that there are political (or at least anarcho-syndicalist for you *Monty Python* fans) considerations driving those who deface government websites or conduct DDoS attacks against financial or government institutions, but it's far from clear that these attacks in themselves could in any way be considered acts of war. Conveniently, several governments have decided that it might be useful to reclassify the activities of such groups in just those terms, worried that the population might get out of control and send our economies crashing (as if they haven't already).

Of course, there is still the tinfoil hat brigade and the survivalists who will believe that the coming CyberWar will be so devastating that it will reduce us (in the USA usually) back to third world status, and bring in a new anarchic era. For instance, Stewart Baker (one of the more outspoken FUD generators) acknowledges: '*At its worst, CyberWar could reduce large parts of the United States to the condition of post-Katrina New Orleans*' [17]. Yes, this is a bad thing, but these are currently fantasies, and the reality is that the capability for bringing systems back online fairly quickly is entailed in the design of the systems. We're still a long way from *Lord of the Flies*, even if we can imagine some worst-case scenarios presented by cyber-attack, they (thankfully) don't, for instance, involve children losing their limbs to landmines[2].

Collateral damage

According to the accepted practices of war, warfare and attacks on the 'enemy' should be concentrated as far as is possible against military targets – yet, uniquely, cyber-attacks almost always target civilian infrastructure and institutions. This is a problem that will not easily be assuaged. The public Internet is shared among military and civilian populations alike and disruption to one will necessarily disrupt the other. Andress and Winterfeld in their excellent book *Cyber Warfare* state:

'*Noncombatants are a particular issue in cyber war. […] At present such activities are carried out almost universally over public networks, as these same networks are used by civilians and military equally. We cannot presently attack one group without affecting the other in an equal measure.*' [9].

Therefore, any cyber-attack entails the risk of collateral damage, but more than that, of 'friendly fire'. As discussed previously, the interconnectedness of the world is a function of its largely compatible and heterogeneous operating systems. (There are three major systems in use, and while malware traditionally has predominantly affected one platform, this is by no means exclusively so – and the relatively lower likelihood of deployed protection on the other two increases their attractiveness as targets.)

This raises a pertinent issue – how does one 'contain' a cyber-weapon? If you provide an antidote or harden your own systems against a specific threat, how do you avoid your enemy finding out and doing the same? Currently most patches to operating systems are available to everyone, whether they pirated the software or not, similarly with anti-malware updates. Detection provided before an attack will necessarily result in a lowered effectiveness as the enemy will likely have some sort of defence in place.

Likewise, if your population is running the same systems your enemy is running, then you have few ways of preventing at least some level of friendly fire – you also risk 'injuring' allied, neutral and innocent states. Although some degree of targeting is possible, it is not foolproof, as is evidenced every day in the spread of malware – it does not generally discriminate though it is often targeted.

Imagine also, the most devastating attack possible (aside from the silly scenarios of hacking nuclear launch capabilities) – one that knocked out the power throughout an entire nation – although it is certainly an inconvenient attack, how is it different from a natural disaster such as, say, Hurricane Katrina or the recent tsunami in Japan?

In fact, on a smaller scale, it is likely that this sort of attack (whether deliberate or accidental) has already occurred. The problem is cleaned up, the systems hardened and the 'attack' is over. Yes, we can imagine that there might be an increase in the number of accidents, and that services such as fire, police and ambulance could be heavily impacted, food and medicines might spoil and petrol distribution/dispensing might be difficult, however, the actual death toll would be low (though, admittedly, the psychological impact may be much higher).

To the attackers though, should they become known (and surely the desire to trace them would be intense) the consequences would be serious. Would any nation truly wish to suffer the consequences of a cyber-attack against the USA (which often seems to consider itself the most likely target)? Despite current economic conditions and the stretch of being involved in two protracted conventional wars, the military might of the US is both highly capable and devastatingly effective. What started as a power outage might provoke a conventional boots-on-the ground kinetic war, faced with which threat any nation might sensibly think twice. As has been pointed out elsewhere, '*America's cyber deterrence does not depend upon any particular cyber capability, but includes the fearsome kinetic weaponry of the US armed forces. What adversary today wants to take on America's vast arsenal of diverse military capabilities?*' [17].

Cyber-attack capabilities, then, seem most likely to be useful in the future precisely in the same ways as they are being used now: causing temporary and generally non-injurious disruption to systems, whether to embarrass, shame or disrupt organizations, or to steal useful information, and perhaps prevent or delay technological progress.

If a truly useful exploit is discovered it makes sense, from a deployment point of view, to reduce targeting to a minimum – to increase noise and reduce traceability. Therefore, the attribution will be difficult. This brings up the idea of CyberHarassment, which might in itself require governments to agree treaties. However, since the attribution of such attacks, as we have discussed above, is at best difficult, such treaties might be ignored with impunity – or as much as can be 'got away with',

[2] My Colleague Stephen Cobb posits the possibility of maliciously altering landmine GPS maps – a realistic proposition, one supposes.

and in some states where little reliance on the Internet is made, simply disregarded.

It seems likely that the most serious attacks will come from lone actors or rogue cells within a state whose sense of self-importance (or self-preservation) is out of skew, and these do not need to be cyber-attacks. Although we worry about cyber-attacks on our critical infrastructure, such actors typically want to inspire fear via a devastating act of terror – it's unlikely that they will bother with cyber-attacks.

To quote Maj. Gen. Shaw:

'*Cyber capabilities won't replace more conventional capabilities. The people we should really fear are extremist groups operating in underdeveloped parts of the world with little or no effective state authority, or a lone wolf terrorist with no technological dependence on cyber at all*.' [18].

Such people have little to lose, plus there is no useful infrastructure in a country like, say, Somalia that any retaliatory cyber-attack would affect. Not only that, but since the people who carry out such attacks typically have little interest in preserving their own lives or the lives of others, there's not much deterrence offered by cyber capabilities. Charles Dunlap sums up this thought particularly succinctly:

'*Does anyone think that those disposed to set off bombs in markets crowded with children would be deterred by a threat to cybernetically shut down hospital incubators somewhere? Cruelly enough, such adversaries just don't care that much about dead babies. It really is that simple…[m]oral considerations aside, the 21st century is replete with examples that prove too many of our most dangerous adversaries are rather indifferent to the fate of civilians, including their own people*.' [17].

PART III: THE BATTLE OF EVERMORE

Dirty deeds done dirt cheap

Currently, while the tools that allow the easy creation of malware are cheap and readily available, this is not true so much for the defence. Computer security in general has become a huge industry, with many vested interests. The sad fact is that, while the general security industry is happy to point out the failings of the anti-virus industry, it often fails to provide any cogent response of its own, and even if it does, all too often the measures are not in place (that is not to say that the anti-virus industry is without its problems or that AV is a panacea). Unfortunately, things have come to such a pass that we will likely see the militarization of civilian behaviour, and proponents of CyberWar may actually be creating a self-fulfilling prophecy.

- First, redefine what it means to be a combatant (this effectively has been done; US law provides for Hacktivists and other protestors to be held indefinitely – much as was done with 'enemy combatants' held at Guantanamo – who, importantly, were distinct from prisoners of war so that the Geneva conventions did not need to be followed).
- Secondly, create a justification in the minds of the public – nationalism and playing on xenophobia is frequently employed to this end; and cede budget control to the military (as has happened in the US [19]).
- Thirdly, ensure the 'enemy' is an indefinable concept such as 'terrorism', to ensure a state of perpetual war can exist.

Unfortunately, this constant pushing of the threat of CyberWar has a fatiguing effect on the public psyche. We become numb to the reality of what is going on around us, and if the real 'threat' is CyberWar, then, because we see little evidence of it in our daily lives, we feel that we can safely ignore it. This removes the threat from our consciousness and puts it into the realm of 'things happening over in another country that I can't do anything about, but might feel bad about if I find out that someone got hurt'. Meanwhile, we do face an unprecedented number of attacks and threats from more mundane criminal behaviour. This in turn reduces the public trust in our institutions and Internet-enabled technologies.

Wake up time for freedom

Eugene Kaspersky, a strong advocate on the side of the CyberWar believers, recently made an interesting comment. He suggested that the biggest threat to democracy in the future could come from malware [20], as people would no longer be able to trust the voting systems – which could be affected (as has been demonstrated many times in various attacks on electronic voting systems e.g. [21]) by malicious actors injecting malware and thereby fixing the votes. This is certainly a possibility, though it seems oddly ironic that he suggests that this possibility of unfairness will kill democracy in the future, when he himself lives in a country that appears to be able to have any president or prime minister that it wants, as long as his name is Medvedev or Putin.

Again, though, humour aside, would this constitute an act of war? It might certainly be an interesting (and less expensive or bloody) route to regime change. One can imagine that, should enough pressure be brought to bear on a state to hold elections (or should a current government prove unpopular enough to other states), an actor from another state government (or any given internal faction) could deliberately sway the results of an election. However, this hardly requires the intervention of malware – which ultimately is one of the more detectable means of intervention in such systems. This seems to be a key factor – we can always detect malware once we know about or suspect its existence. Andress & Winterfield again:

'*The principle behind defence in depth is, through the multiple layers of security measures, to hinder our attackers sufficiently so that our elements of detection will discover their activities or so they will decide that our security measures are too great and give up on their attacks.*' [9].

At the point at which an attack is detected, it is clear that any election result skewed in such a manner would be immediately discredited (along with the elected government). So while one might conceivably see that malware could be used for this purpose, governments are already quite happily fixing and swaying their own election results, without any need for the added effort (and risk) of adding malware to the system, particularly as those systems improve.

If democracy is to be distrusted or threatened, it is more likely to be due to existing causes such as voter indifference, dead voters voting, heavy lobbying from corporate interests and plain old corruption.

Having said that, there is a good point in that one of the challenges of ensuring public confidence in Internet-enabled technologies is to convince them that they are safe. People are certainly concerned that the current systems already in use are a threat to their privacy and that any compromise of same could severely impact their lives. And yet, we use them, often in an incredibly insecure manner.

Careful with that axe, Eugene

It is important, in all of this, to be aware of the Dunning-Kruger effect, which shows that it requires a degree of expertise in a subject to be able to evaluate the expertise of another person in that subject [22]. At this point, I should state unequivocally that I am not an expert in CyberWarfare, nor do I claim to be, I have merely tried to educate myself deeply on the subject. However, I am an expert in malware.

What is less certain to me is where, in a range of expertise on the subject of malware within the anti-malware industry, I sit. I am aware of many I would consider more expert (certainly when it comes to reversing or analysing malware code), but I am also aware of many who are less expert outside of the direct AV space, and unfortunately within the general security sphere. That is not to claim superior intelligence, it's more to state that, when it comes to malware, there are relatively few people in the general populace, or in the security industry more widely who can truly claim expertise in understanding malware.

Eugene Kaspersky (as I've used him as an example earlier, I'll continue to do so here) is an acknowledged expert on malware, which does make it very interesting when he claims that CyberWar via the aegis of malware is an existential threat to our lives and freedoms [23]. What is less clear though, is whether Eugene, or I (or, for that matter, any given person) is able to evaluate our knowledge in a wider sphere where we might not have such direct expertise (e.g. assessing the cyber-capability of another government or state). That we can analyse malware and speculate about its origins and the intentions of its writers is a given, but that we can extrapolate that into a theory about the likelihood of CyberWar becoming a reality is less so. This is particularly hard for the media to understand, who will often oversimplify subtle and complex points.

I am certainly fascinated by the possibilities and scenarios that have been suggested by Eugene and others, but I struggle with a cognitive dissonance when trying to fit them into a framework of what is conventionally known as warfare. I am also aware that as a British CEO of a US company with headquarters in Slovakia, I may not be in the best position to fully understand the security posture or concerns of, say, the USA or any other given country, and there may well be incidents that I am not aware of. However, I have also sat in a room with senior members of (US-based) three-letter organizations and had them tell me that they believe the threats are overhyped, and that they dislike the term CyberWar.

Of course, as I've said above, we can simply redefine terms as needed – our definitions of war are centuries old – to encompass such acts into our definition of war, but then we risk diluting the usefulness of those terms, to a point where we will in fact live in a constant state of war, against a faceless and indeterminate enemy, which has a direct effect on our lives and how we are governed. As Robert Clark has pointed out, '*If policy-makers are only informed by the catchphrase and not the definition, they will make bad policy*.' [24].

This may yet happen – George Orwell seems to have written the policy manual for western governments – but the greater threat seems to be falling victim to a sort of intellectual sloppiness that allows us to group together the sorts of acts carried out by Stuxnet, with the reality of bleeding children on the streets of, say, Syria.

In fear of fear

Ultimately, we – and I say we, as I believe the anti-malware and security industries have been to some degree complicit in spreading the fear, uncertainty and doubt that have allowed the concepts of CyberWar to take hold – should try to avoid inflating the problem (and our own egos) by constant speculations and statements about a coming apocalypse.

I once saw a quote on a poster in a doctor's surgery that said '*The best diet for a person with diabetes is the same as the best diet for anyone else*' – applied to security, what is good for CyberWar defence is good for security defence in general. This is the simple reality – we need to improve our security defences across the board.

There are certainly threats out there in cyberspace, some of them more likely to cause harm than others, but the great majority of these are made with criminal intent – and are avoidable with good CyberHygiene and a sensible approach to defence. By focusing on a threat that most people can do little about, we risk distracting them from taking steps that would ultimately make all of us safer. We need to start them asking the right questions; Maj. Gen. Shaw recently stated that:

'*Bad cyber hygiene is the biggest threat to us in the short term. How safe are you in your personal behaviour? How safe is your intellectual property that resides in industrial supply chains?*' [25].

This paper is not really about technologies – but it falls on all of us to improve things in whatever way is possible. We also have a responsibility to ensure that we do not desensitize people to real, future threats. While we may not be in the all out 'CyberWar' scenario right now, we do not know what the future holds. It is possible that nation states developing offensive cyber capabilities is, as Eugene Kaspersky says, the harbinger of a new age of CyberWarfare [23]. Perhaps by openly discussing the threats now and observing them in a neutral and non-hyped fashion we may be able to derail or decelerate the possibility that in the long term these threats encompass the sort of fatality and harm that kinetic warfare currently brings[3].

That said, we need to take care that when we are talking to a generalist audience, we avoid using misleading or easily

[3] Thanks to a conversation with Joe Telafici for this thought.

misunderstood concepts (of course, I accept that journalists tend to pick and choose what to quote), and we try instead to educate people about the very real threats that they currently do face. Along with that, writing software with more built-in resilience, improving our own code review and pen-testing capabilities, perhaps encouraging insurance companies to get involved (they're very good at forcing safety changes – not wearing a seatbelt? You're not insured…), and ultimately, teaching people about properly managing the risks of using today's technology will have much more effect on us than dire warnings of a war that no one will be able to see or feel. It would be hard to sum it up better than this:

'*It would be a huge mistake if we led people to believe that they don't need to do anything about cyber issues, because the big brother military will sort it all out. I prefer to be talking about how to live in a digital age. That is the challenge facing us all*.' [18].

REFERENCES

[1] Goodin, D. Confirmed: Flame created by US and Israel to slow Iranian nuke program. June 19, 2012. http://arstechnica.com/security/2012/06/flame-malware-created-by-us-and-israel/.

[2] Sanger, D. Obama Order Sped Up Wave of Cyberattacks Against Iran. June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[3] Rid, T. Think Again: Cyberwar. March 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar.

[4] Guo, T. Shaping Preventive Policy in 'Cyber War' and Cyber Security: A Pragmatic Approach. 2012. http://works.bepress.com/tony_guo/2.

[5] Wingfield, T.C. International Law and Information Operations. Chap. 10 in Cyberpower and National Security, edited by Franklin D Kramer, H Stuart Starr and K Larry Wentz, 525-542. Washington DC: Potomac Books, 2009.

[6] Jackson Higgins, K. Stuxnet, Duqu, Flame Targeted Illegal Windows Systems In Iran. June 19, 2012. http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240002364/stuxnet-duqu-flame-targeted-illegal-windows-systems-in-iran.html.

[7] Rattray, G.J. An Environmental Approach to Understanding Cyberpower. Chap. 10 in Cyberpower and National Security, edited by Kramer, Starr and Wentz, 256. Washington DC: Potomac Books, 2009.

[8] Brenner, J. America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare. New York: Penguin Press, 2011.

[9] Andress, J.; Winterfeld, S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Syngress, 2011.

[10] Anghaie, A.-R. STUXNET: Tsunami of Stupid or Evil Genius? June 1, 2012. http://www.packetknife.com/stuxnet-tsunami-of-stupid-or-evil-genius.

[11] Hyppönen, M. A Pandora's Box We Will Regret Opening. June 5, 2012. http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/a-pandoras-box-we-will-regret-opening.

[12] UK diplomats in Moscow spying row. http://news.bbc.co.uk/2/hi/europe/4638136.stm.

[13] Libicki, M. Setting International Norms on Cyberwar Might Beat a Treaty. June 8, 2012. http://m.rand.org/commentary/2012/06/08/USNEWS.html.

[14] Stiennon, R. Surviving Cyberwar. Plymouth, UK: Government Institutes, 2010.

[15] Glenny, M. A Weapon We Can't Control. June 24, 2012. http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=2.

[16] Fischer, M.; Blank, J.; Dernba, C. Germany confirms existence of operational cyberwarfare unit. June 5, 2012. http://www.stripes.com/news/germany-confirms-existence-of-operational-cyberwarfare-unit-1.179655.

[17] Baker, S.A.; Dunlap, C.J. Jr. What Is the Role of Lawyers in Cyberwarfare? May 1, 2012. http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare.

[18] Maj. Gen. Shaw, J. The Once and Future War. World Policy Journal 28, no. 3 (September 2011): 45-51.

[19] Mills, E. Wording in cyberwar bill begs question: Who's in charge? May 11, 2012. http://news.cnet.com/8301-1009_3-57432259-83/wording-in-cyberwar-bill-begs-question-whos-in-charge/.

[20] Head, B.; Kaspersky, E. World Teeters on Cyber-War Brink. May 22, 2012. http://www.itwire.com/business-it-news/security/54865-world-teeters-on-cyber-war-brink.

[21] Goodin, D. Diebold e-voting hack allows remote tampering. Sept 28, 2011. http://www.theregister.co.uk/2011/09/28/diebold_electronic_vote_tampering/.

[22] Lee, C. Revisiting why incompetents think they're awesome. May 25, 2012. http://arstechnica.com/science/2012/05/revisiting-why-incompetents-think-theyre-awesome/.

[23] Kaspersky, E. Expert warns of cyber war threat. March 18, 2012. http://www.disasternews.net/news/article.php?articleid=4518.

[24] Team Register. Stuxnet ≠ cyberwar, says US Army Cyber Command officer. May 16, 2012. http://www.theregister.co.uk/2012/05/16/stuxnet_was_not_cyberwar/.

[25] Muncaster, P. Ministry of Defence cyber chief urges UK to follow Estonian example. Nov 9, 2011. http://www.v3.co.uk/v3-uk/news/2128527/ministry-defence-cyber-chief-urges-uk-follow-estonian-example.

[26] Schwartz , M.J. Schwartz On Security: Zombie Internet 'Kill Switch'. October 28, 2010. http://www.informationweek.com/news/228000213.

[27] Smith, G. An old cyberwar April Fool's joke proves durable, finds new rubes. March 20, 2012. http://sitrep.globalsecurity.org/articles/120320838-an-old-cyberwar-april-fools-jo.htm.

PLAYLIST

War: Edwin Starr

Possibly Maybe: Bjork

Peace Sells, But Who's Buying?: Megadeth

Masters of War: Bob Dylan

The Art of Self Destruction: Nine Inch Nails

I Shot the Sherriff: Bob Marley

Army of Me: Bjork

Collateral Damage: Muse

The Battle of Evermore: Led Zeppelin

Dirty Deeds Done Dirt Cheap: ACDC

Wake Up Time For Freedom: The Cult

Careful with that Axe, Eugene: Pink Floyd

In Fear of Fear: Bauhaus