Fighting the 'Good' Internet War

Dan Cvrček[†] and George Danezis

[1] University of Cambridge, UK & Brno University of Technology, CZ.
[2] Microsoft Research, Cambridge, UK.

Abstract. We review the current strategies to counter Internet threats under the light of the classic strategy literature. The literature often advocates proactive action, and dominance of the (virtual, in our case) battlefield, which is the opposite from what we see defenders deploy today. Their actions are instead reactive and exclusively defensive. We propose strategies for defenders to regain the initiative and push security solutions far beyond the reach of current security tools – yet those strategies start mirroring the actions and technologies of the bad guys, and confront us with important technical, legal and moral dilemmas.

"*He who fights with monsters should be careful lest he thereby become a monster*"

Friedrich Nietzsche — Beyond Good and Evil, Chapter IV: Apothegms and Interludes

1 Looking For the Adversary...

Security engineering textbooks [1] teach us that the most prevalent and damaging enemy comes from within an organisation. Yet in the PC and the Internet era not everyone is part or protected by an organisation, or by its system administrators. Huge numbers of home users are left on their own to fend off a number of attackers. They are left exposed to attack by their ignorance of the existing threats, inadequate technical knowledge, the overwhelming dangers stemming from anonymity of Internet, and the huge gap between user interface and correct functionality.

Their vulnerability is not the users' fault, as they cannot be expected to be technical experts, to browse the Internet, send emails, or play games. They make up a huge group of people and machines that without being malicious easily become hostages of real attackers, and a fertile ground from which attacks are launched.

The real Internet enemy are small groups of highly technically skilled people that use innocent and unaware users to carry out their criminal, and usually highly lucrative, activities. Some easily visible signs of their existence include the huge quantities of spam, phishing sites or large-scale operations attracting users to anchor on pages packed with malware, to turn their machines into bots.

These all are observable signs of the enemy's existence but still, the enemy itself is well hidden. Our goal, in this paper, is to suggest strategies and tactics to uncover them.

2 Waging War – History Lessons and Internet Warfare

Humanity has a long history of military conflicts, from which we can learn. This section picks some interesting ideas from several famous military strategists, namely Carl von Clausewitz [CvC] [2], Antoine-Henri Jomini [AHJ] [4], Sun Tzu [ST] [6], Mao Ce-Tung [MCT] [5], and Maurice's Strategikon [MS] [3]. Ideas that we find useful for even a warfare in a digital environment – it shows that some military principles go way above military actions.

[†]Dan is partially supported by the Research Plan No. MSM, 0021630528 – Security-Oriented Research in Information Technology.

2.1 Military Strength

Some key elements of strength are outlined from Carl von Clausewitz's [CvC] work:

- Strength of forces is not only defined by numerical strength and their organisation, but also with their relationship to "country and terrain", i.e. they should take the environment into account. The relative strength of the forces can be improved by advanced guards and outposts, proper lines of communication, and the command of heights [CvC].
- The defence is built around several types of elements: militia (armed population that can be effectively used to defend enemy), fortresses (strongholds that offer protection but also gain influence), the people, and allies. [CvC]
- The defence in physical sense comprises of: defensive position (it cannot be bypassed), flank position (can be bypassed by the enemy, but it holds), defence of special types of terrain (swamps, flooded areas, forests, ...). [CvC]

Internet. Attackers are well aware of the importance of terrain: they overtake weakly defended machines, to use them as a multiplier of their strength. Hiding behind those hosts also makes them invulnerable to direct technical or legal attacks. This behaviour, and the logical extension to [CvC] suggestion is the foundation of *guerrilla warfare*, the study of which is of some importance in the context of Internet conflict.

The fortresses can be viewed as security vendors and their services offering protection mechanisms – probably a common view today. Their infrastructure, be it incident handling, virus reverse-engineering, signature updating, or monitoring should be strengthened against attempts to disable it.

The militia are the security aware Internet users, that deploy security software, sometimes aid in the monitoring of threats or debugging of applications, as well as apply security patches. Their role is not offensive, it is rather to make it difficult for the adversary to gain more ground from which it can launch attacks. Their coordination can happen through security vendors, as well as on a peer-to-peer level.

2.2 Initiative

Clearly, the side that is more active is also able to enforce the rules of the warfare. This is important for any type of warfare and also extensively covered.

- Aggressive action will deprive enemy of time. It will make him do quick decisions and increase the chance of strategic errors [ST].
- All the resources must be engaged, and the purpose of the engagement is one of: destruction of enemy, conquest of locality, conquest of object [CvC].

Internet Every action on the digital battlefield must be carefully prepared, because the actions will be instantaneous, responses automated, and the fight very short. Aggressive action may force the enemy to alter their tools and procedures, omit some precautions, to become nervous. The goal will be to create pressure on speedy actions that are not routine and require manual interventions.

What are the goals of our fight? It will differ from time to time. Probably, we will want to conquest an object – a botnet operated by the enemy. We may want to clean users' machines, but we would then be forced to defend an area, which would require a lot of resources. We want to hit heads and cut them from the rest of the enemy's army (botnets). Finally we may want to destroy the enemy – find the operator of the bot net, and who they work for, and secure a conviction against them.

2.3 Tactics

We believe that tactics used to combat malicious parties on the Internet are always a step behind and a strategy does not really exist. However, Jomini stated several centuries back that the key to warfare is strategy. Let us start with several notes from history.

– There is an asymmetrical relationship between attack and defence. One should try to reverse the asymmetry whenever possible. Attacks have several decisive advantages of attack: surprise, benefit of terrain, concentric attack, popular support, and moral factors [CvC].
– Divide and conquer, a particular tactics that further developed e.g. by Matyas Rakosi for Hungarian Communist Party in the late 1940s as salami tactics, uses alliances to increase political power [AHJ].
– If you use a common sense, you are inevitably doing a bad strategy choice [ST].
– Inner line of operations, i.e. operations inside the enemy's army will allow for fighting separate parts of the enemy's forces [ST].
– Divide forces to arouse the masses, concentrate forces to deal with the enemy. Red Army fights by conducting propaganda among the masses, organising them, arming them, and helping them to establish ... power [MCT].
– Mobilisation of the whole nation forces the enemy to "defend the area" and we can pick the right time and the right place to fight battles [MCT].
– Ambushes are of the greatest value in warfare. The most powerful is an ambush from both sides and the timing should be precise to maximise the effect [MS].

Internet We believe that we can make use of most of the tactics used above. The most proper seem to be Mao Ce-Tung's principles.

Yet the most neglected advice when it comes to Internet conflict, is the focus on offence. Defenders make no attempt to 'reverse the asymmetry' and instead believe that security shall come by digging deeper trenches around the few secured hosts. This gives the adversary full strategic advantage to attack when, where and how she wishes.

2.4 The Power of Information

Many commanders have quickly realised the power of information and careful planning. Interestingly, there are more rules related to concealment of own actions and strengths.

– Hiding real purpose of actions is an important element in strategy [CvC].
– Conceal your plans, or plan for several steps ahead [ST].
– One should not engage enemy in combat or show their strength before learning the enemy's intentions [MS].
– One should prevent hostile reconnaissance and thereby conceal the second line of their forces [MS].

Internet There is a warfare already and so we can learn a bit about our enemy and study their behaviour. We can design new tools and use them in the war but no-one is really doing any plans. We are fighting isolated battles and loosing the war.

The plans are very easy to read if anyone bothered to do that, as the threat posed by them is very small.

The organisation of the enemy consists of a head, support groups (organise specific crimes), and working units. The working units will cover the following activities: vulnerability discovery, exploit design, spam management, managing DNS records, coding, web site building and managing, managing botnets, sales agents.

The most activities are offline and the enemy goes on-line only the manage the botnets and web sites, and sales agents). It is also possible to detect the on-line malicious activities – the actual attacks. We can learn from the way the bot-nets are commanded and organised, but our tools must be equally stealthy so they cannot become easy targets in the wars of bot-nets.

3 Battleground

The battleground is already set by the enemy – organised crime groups. We cannot change it and we do not want to change it, in fact. It is formed by users that are most vulnerable. These are not actively trying to get rid of the negative effects the enemy's activity has on their machines, but they could be easily persuaded to join the warfare by providing their computing resources.

3.1 Enemy

The organised groups use a very flexible structure and hide their on-line activities among unaware Internet users.

- Heads of operations – they are on-line only for short periods of time, and there are no limits regarding the place of their Internet connections.
- Information gathering servers – must be on-line for considerable amount of time (at least hours) but they can be physically moved around. The connection is provided via updated DNS records.
- Bots – users' machines that are taken over by the group and used for various types of hostile activities. These are not directed against owner of the machine, thus decreasing incentives for the owner to deal with the situation.

It is very hard to find the heads or the servers gathering information. The only chance is to find the machines forming the botnets. So what is the goal of the war?

3.2 Current Tactics and Strategy

The good guys are so far reasonably predictable and the organised crime groups made provisions against them. We can see two basic approaches the good guys use:

1. Develop and sell security mechanisms
2. Identify dangerous websites and provide the information to interested users

Obviously, neither approach is trying to fight the enemy directly. They only protect those users who are vigilant and aware of security threats. When we take into account the size of this niche security market and compare it with the total number of the Internet users, we can see that it does not hurt the enemy the least. The basic problem of the above mentioned approaches is that they target different subset of users from those targeted by bad guys. What is the structure of the enemy's army?

The approach for an effective fight would be similar to the Mac Ce-Tung approach – to use "the people" and to create the "militia". First of all, however, we have to learn and find the enemy.

3.3 Reaching the Battleground

The key problem for securing systems today is to reach the digital battleground and to encounter the enemy at all. Current defence strategies are reactive: poorly fortified systems are lame ducks, to attacks launched from behind the crowd of innocent yet compromised machines. While feeling the full might of the adversary, our only reaction is to mend our shields in the hope they will resist the next round of offensive technology innovation. No one is surprised when in the long run they break!

The main problem is the communication channels the good guys employ. Security vendors expect customers to fly to them and pay good money to be afforded any protection. Unfortunately most home users not only do not seek those products but are definitely not ready to pay for them, even in the rare cases they are aware they exist.

The adversary, on the other side, is targeting exactly those users that security vendors fail to attract. Using spam or search engines as their communication channel, they attract security unaware users and turn their machines into part of the digital battleground.

Defenders will never effectively fight the enemy until they are able to reach, one way or the other, those users. This will involve distributing security software in innovative ways to meet the adversary.

- The most obvious way to reach users who follow-up links and get infected through spam is to *use spam*. Some may object to this tactic, by arguing that it might train users to click on spam even more. We do not advocate running an advertisement or awareness campaign promoting the of untrusted software. At the same time we have to recognise that the only way to reach users that have not been moved by campaigns with the opposite message is through this channel.

– A second vector of infection are unpatched machines running services with known vulnerabilities that are waiting to, or are already, infected with malware. It is only a question of time until those are turned to weapons against third party systems. Clearly the most forward way of reaching those machines is exploiting the vulnerability to install software. Again, many objections can be raised including legal and technical ones. The first objection is that overtaking an unpatched machine may lead to financial damage or may affect its stability. This is undoubtedly true, and only a matter of time until this damage is caused by a malicious user taking over the machine for nefarious purposes. It is all good keeping our hands clear, and arguing that at least the damage was not caused through our actions; yet on the utilitarian balance sheet we have let a greater evil take place: the machine being infected and the computer being used for further mischief.
– Similar strategies can be deployed using any infection or propagation vector that malware utilises, as well as vulnerabilities in the malware itself, that is often not of the highest quality. Web-pages serving infected files, search engine poisoning, phishing sites, etc. Those strategies can also be deployed against networking equipment that stands unpatched and vulnerable, such as cable modems or wireless routers that are misconfigured or buggy.

A common objection to the *efficacy* (leaving aside the numerous objections as to the *morality* of the matter) of this deployment strategy is that intrusion detection systems, antivirus software or security services will detect and neutralise our deployment attempts. Hosts that deploy those counter-measure should be deemed safe, and would not the least benefit from the active attempts to block the adversary described above. Yet if those protection systems would be universally deployed and effective we would not be witnessing the levels of compromises we do today – the day they are the proposed deployment approach would be unneeded, at the safe time it stops being effective.

3.4 Identifying the Enemy

Once we have found means to deploy software on the digital battleground that is comprised by infected machines, the battle is just starting. It may be tempting to be too earnest at this point, patch a single security vulnerability and vacate the ground. This strategy is naive, since a vulnerability is probably indicative of a pattern of security neglect typical of a user and a machine, rather than a one-off incident.

Instead of doing a quick cleaning job the position represented by the machine should be fortified and the defenders should be ready to hold their ground. This means deploying effective tools to allow us to carry out tactical decisions and plans. The tools should implement tasks within the main strategic plan: reconnaissance, analysis of information, elimination of the enemy's activity, as well as trace the enemy.

The reconnaissance activity should be able to retrieve as much useful information as possible. At the same time, the tools used on the battleground must be hard to detect and circumvent – it's necessary to use stealthy and polymorphic technologies, as well as hard to detect communication channels. The adversary who owns the compromised territory acts as a defender that might have deployed sophisticated systems to prevent us from reaching it and freeing it.

One could envisage the following components being needed:

– Monitoring capabilities being deployed reporting and aggregating information on lists of processes, start-up processes, outbound and inbound network connections and their details, or unusual system activity. Defenders can use these to detect out breaks, vulnerable services, as well as track attackers.
– Since the adversary will attempt to disrupt communications a robust, and DoS resistant networking infrastructure has to be constructed. This involves allowing the defensive software to create a peer-to-peer mesh and use it for robustness as well as hiding the command and control centres of the defensive operation.
– The deployed software itself should be hardened against any detection mechanisms the adversary might have deployed on compromised hosts. This mandates the use of polymorphic code, stealthy root-kits as well as obfuscated binaries.

– Finally the back-end system – databases for storing important data, analysing observations from robots, and issuing commands – have to be hardened against attacks, or even better hidden using covert communications.

It is obvious that if one is serious about conquering back the infected ground that the adversary controls, they cannot limit themselves to conventional technologies. They have to be ready to put on their offensive hat, to defeat a well motivated and security aware defender – in this case the adversary.

Yet no strategy deployed should be at the detriment of prudent security practices. The offensive deployment strategies described here should gracefully fold back in case the user installs proper protective software or a serious patching regime is followed. It is not acceptable to try to disrupt those, merely to allow for offensive propagation to still be possible – this is *a key moral distinction* between those that offensively deploy software as a self-defence strategy versus the adversary that does it for malicious purposes.

4 The Permanent War Economy

No conflict is ever settled for good. Any resolution is based on political strategy that depends hugely on economic interests and the relative power of all parties. (No one will negotiate as long as they think they can unconditionally win.)

The cost of law enforcement has to always be compared to the significance of the crime. This significance from the social point of view is different from the profitability of the crime that would be limited. Economic tools can be used to model equilibriums but it is unlikely that crime can be completely eliminated so long as there is an economic incentive for it. Hence it is unlikely that defenders will ever stop their activities, and there is a need to find sustainable ways to finance the perpetual defence effort.

The money for waging the war should not be received from the "battleground", from users allowing us to use their machines. Although it is probably possible to differentiate offered services to attract some reward: monitoring a machine can be for free, but a fee can be charged for the removal of malware.

A secondary source of revenue may be entities interested in data about the state of Internet threats to assess overall potential dangers. We could inform potential targets of e.g. DDoS attacks about the danger and negotiate a price of further services if they find the information valuable. Or if an attack cannot be blocked, we may be able to identify the source of the attack and allow thus future crime prosecutions.

The general idea would be to build the business model on the revenues from big players and potentially services for common users (Robin Hood strategy).

Acknowledgements. We thank the research institutions that employ us and that in no way share the views expressed in this paper.

References

1. R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley, 640p, 2001.
2. Carl von Clausewitz. *Principles of war.* London, John Lane, 64p., 1943.
3. Maurice, emperor of the East. *Maurice's Strategikon: handbook of Byzantine military strategy / translated by George T. Dennis.* Philadelphia, University of Pensylvania Press, 178p, 1984.
4. Antoine-Henri Jomini. *The art of war.* London: Greenhill Books, Calif.: Presidio Press, 1992.
5. P. Paret, G. A. Craig, F. Gilbert. *Makers of modern strategy: from Machiavelli to the nuclear age.* Princeton, N.J.: Princeton University Press, 941p, 1986.
6. Sun Tzu. *The Art of War.* available on-line, http://www.sonshi.com, 2008.