The role of the civilian casualty - Information Warfare

David Griffiths

GIAC GSEC Certification Practical Assessment
Version 1.3
Saturday, 15 January 2005

Course taken at:
SANS Darling Harbour, Sydney, Australia, January 2002

INDEX

ABSTRACT

Throughout history there have been few events that unite a country the same way a war can. Heavy industry suspends normal operations to build weaponry, transportation is reassigned to carry armed forces, and in days gone by, scores of young people would sign up to fight for the glory of their country and to protect their way of life. These days however the same well-meaning governments, businesses and individuals have unwittingly switched sides by providing the very weapons by which they will be attacked. Computer systems in homes, offices, educational institutions and governments can, and are utilised by those wishing to do harm. This paper explores the relationship between the virtual armies of cyber protagonists and their ever-so-helpful targets, and aims to show that the line between victim and accomplice in cyberspace is very blurred indeed.

INFORMATION WARFARE VERSUS THE TRENCHES

Strategies, conventions and difficulties of waging a conventional war on another country have been known to us for centuries. The hardships of moving weapons, supplies and troops over vast distances in terrible conditions has undoubtedly prevented more wars than have succeeded despite it. There are now strong indications however that point to the possibility of a new and potentially-devastating conflict which has almost definitely already begun in some form, and that could evolve to threaten both directly and indirectly a large percentage of Earth's population.

With personal computers becoming more powerful and home internet access becoming faster, cheaper and more widespread in the developed countries the process of inflicting damage to another nation through electronic means has become an easier, cheaper and less risky option to those for whom a conventional war would be out of the question. Intelligence, misinformation and control within a foreign country can now be carried out by a determined, methodical hacker, organisation or government from anywhere on earth. Whilst a large-scale attack would require a lot of planning, considerable skill and many months, or even years to prepare, it is my opinion after researching this topic that it is not inconceivable that such an attack will one day take place.

> "Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."
>
> Dr. Ivan Goldberg

Intelligence

I will define intelligence in this case as information which, when applied to a given situation will allow understanding of the intentions and capabilities of an opposing force.
Whilst traditional intelligence-gathering activities are still used by countries to aid national security, the gathering of intelligence through remote electronic means has become an everyday occurrence that the general public is largely oblivious of. There are many forms of intelligence gathering available to an information warrior, some of which are:

"Click through" measurements on web sites -

Find out more information about your opponents by seeing which pages they look at on their favourite websites. Many large web sites now incorporate these systems to help deliver more a more customised experience for their users. To our information warrior any data about the habits, preferences and character of the intended victim can be, on a national scale revealing of strengths and weaknesses, and on a personal scale a path to blackmail and extortion in return for, as an example, access to secure systems. This latter case would be particularly dangerous if potentially-embarrassing information was discovered about a government official with high security clearance in government computer systems. This information is being collected all the time, and could be available to a determined hacker.

Traffic monitoring.

E-mail and login passwords are often sent in plain text. Whilst this is perfectly okay for many home users, it can be invaluable to our information warrior. So many actions involving the internet now involve us to log in, and so often the data path over which this happens is easily compromised by a would-be attacker. Whilst many secure systems owned by trusted organisations such as banks use technologies such as SSL to encrypt data whilst it is transferred, many sites requiring login do not. Not only can an attacker pretend to be their victim on these sites in order to gain information, but once they have access to their victims internet access account they can maybe use the trust their victim may have with colleagues and friends to gain further information about interesting targets.

As well as passwords of course, information itself is quite often sent unencrypted in the form of email, and even instant messenger traffic. These are also easily compromised by someone who is in a position to see passing traffic.

Trojan horses.

Any program that connects a computer to a centralised server for administration is capable of sending information about the user of the system back to that server. There are several instant messaging programs that do not require a proxy server to be specified in their configuration due to the fact that they can read their host PC's registry information and obtain their settings automatically. A program with this level of access could easily retrieve internet account information, personal or company details, possibly access files on the hard disk, and even record keystrokes in order to gain password information for secure systems. Any piece of software could be maliciously-written, or even modified to allow this form of intelligence gathering. A recent example is that of AOL being asked to supply 5 years' worth of messenger conversations in contribution to a court case. They have recorded these conversation without the knowledge of the service's users.

Misinformation

If you read it in email it must be right, mustn't it?? Of course it must...
A couple of days after the September 11th tragedy in the US last year I received an email quoting a Nostradamus prophecy describing, with great accuracy, the events of that day. Whilst I am usually open to new ideas, this struck me as a little coincidental. Not so however to over 5 of my friends, who sent this to me with their own exclamations of wonder at the accuracy of good old Nostradamus. This particular quote later was proved to be a hoax. Someone had simply written a paragraph in the style of Nostradamus to reflect the September 11th tragedy, and managed to fool enough people for it to be circulated.

This illustrates the ease with which our information warrior could deceive a population with false news. Not that I would suggest an entire population would necessarily agree with an opinion expressed in an email, even if allegedly reported by a reputable source. There would however be a feeling of unease if the right rumours were circulated far and wide enough. This news may be of a political, social or even racial nature, or maybe describing events in a foreign country for which no proof could be offered verifying or denying the allegations. Such information could help to change the mindset of a population to sympathise with a would-be attacker, or even trust someone they would not under other circumstances.

A good example of the effect of misinformation is the allegation the Microsoft Corporation was to merge the Vatican.
(http://www.subbrilliant.com/subarc0898.html#Vaticasoft)

Control

Being able to see someone's computer system might be useful in finding out more about them, but taking control and using their computer for your own purposes, free of charge, is much more exciting and potentially destructive.

The most powerful computers available to our information warrior can be located in government departments, the military and educational institutions. Whilst breaking in to military computers would be a risky venture indeed, many government computers may well be less secure and more easily compromised. Likewise, large computers at educational institutions can be powerful and possibly open to other outside intrusion, or use by a malicious insider.

Several outcomes can be achieved by taking over a large computer system. Some of these are:

Denial of service.
Turn off a city's power and you have caused an enormous amount of damage. Redirect or release stored water, oil or gas supplies and you have had a profound effect on the general population. Disrupt telecommunications and apart from the disruption to business and government the population will feel very much under threat. In extreme cases where emergency calls may be affected, people could die.

Many critical infrastructure items rely on distributed management systems to monitor and control them from a central location. These systems should not be directly internet-connected, but sometimes are or could be accessed through a PC that is. In this case an attacker could use an internet-connected PC they control to in turn control a larger, more secure system through a trusted network connection.

Internet communication is critical to many large businesses as well as millions of individuals. Could our information warrior bring down the internet across an entire country? Possibly. The network connections that join together homes, businesses, cities and continents have a finite capacity to carry information. This capacity, referred to as bandwidth, is vital to the fast, efficient use of the internet. Bandwidth to a home PC does not need to be high, whereas bandwidth available between cities is enormous to cope with the accumulated traffic from hundreds of thousands of homes. This works to an attacker's advantage if wanting to disrupt internet services.

Firstly our information warrior would have to gain some sort of control over a reasonable number of computers. An email virus would certainly allow the attacker to install software on a vast number of machines if done carefully. For example many currently-known viruses have been detected through their frantic and obvious use of email systems. Our information warrior may write a virus that is not obvious, does not cause any discernible damage, and in fact does not draw attention to itself in any way at all. It simply opens a new network port on the host PC, creates an out-going connection to bypass any intervening firewalls and sends a single email back to its owner with any information it can find along the way.

Using these connections an attacker could then get these machines to start sending a storm of packets from their host networks to a variety of carefully-chosen internet sites. With a large number of computers spewing out packets to limits of their available bandwidth the internet backbone connections would soon become "clogged" with the excess traffic. Tracing and shutting down a few rouge machines is not that hard, but shutting down 100,000 PCs that are showing no obvious signs of distress might be a very difficult task. Thus, the internet can be reduced to a crawl for as long as it takes to isolate the machines concerned.

Password cracking.
Any attacker wanting to crack today's high-encryption algorithms could never hope to do so in a reasonable amount of time with a home PC. Even several home PCs would take too long. 100,000 PCs is starting to get interesting though... What about 3 x university mainframes, 2 x government systems and 500,000 home PCs across the globe all working together, each analysing a particular range of keys in order to break the same algorithm? This is by no means impossible.

Again, using trojan horses in commercial, or even "free" software, backdoors could be created allowing our information warrior to use the processor in down times. A legitimate version of this is the system used by the SETI organisation which utilises a distributed network of home and business PCs to analyse signals received from space, looking for signs of artificial intelligence. Such a system would be a very powerful password cracker indeed, and gladly supplied by the owners and administrators of the infected PCs.

STEALTH

It's very hard to prepare for an attack you can't see coming, carried out by an enemy on the other side of the world. The battlefields of an information war could extend to every country on earth simultaneously, with no defined front lines. A group of attackers working in unison from different countries could make it very difficult for their target to detect their intelligence gathering, or even the preliminary stages of an attack. It is even likely that a well-organised group of attackers could achieve their goals, depending on what they may be, before anyone within the target nation was alerted to their influence. This is the greatest threat of information warfare, the fact that the first sign we might have of an attack is the interruption of our water supply, our phone system, our oil supply and finally our electricity.

The problem with early detection stems from the similarity between malicious traffic and that which is common-place and necessary. Intrusion detection software such as Snort, and anti-virus software of all kinds use pattern matching to determine if a packet or stream of packets is in fact malicious. In order to detect malicious code this way you must already have a sample of each instance of code from which you wish to protect yourself. You can then teach the software, for example Snort, to look for a range of signatures which will identify dangerous code or unusual behaviour and react based on what it finds. The inherent problem with pattern matching is though that you can only search for attacks you know about. A clever attacker could produce his own code, allowing him to bypass the detection rules looking for existing signatures, and even change the way his code acts to get around port scanning rules and the like.

An attack from such a person or organisation would be very hard to detect until it was too late. Swift responses from organisations such as the CERT Co-ordination Centre, the anti-virus software manufacturers and the various system administrators who would write intrusion detection rules could help to contain an attack, or limit its effectiveness immediately following the initial detection. This also though assumes that government, businesses and individuals were using these products, allowing them to counteract the threat.

Early awareness of attacks is a key area in the prevention of their spread. Organisations such as the Internet Storm Centre can assist security analysts by correlating attack detection information from around the world into a central source. A highly-distributed attack against a variety of hosts could therefore be detected more easily due to the distributed nature of the detection tools. The Internet Storm centre utilises the firewall and intrusion detection logs of over 3000 sites and displays its output at http://www.incidents.org.

Another major advantage in favour of our information warrior is that they can now easily communicate with counterparts anywhere in the world, especially within the target country. Maybe a terrorist cell is operating within the victim nation's borders and plan to take violent physical action once the information war has begun. These people could stay in constant contact with out warrior through several means including encrypted email and steganography.

Encrypted email simply encrypts the contents of email before being sent by the originating party using the recipient's public key, previously exchanged. The only person who can now read this email is the recipient, who possesses the matching private key to decrypt the message.

Steganography is a new twist on an old technology. The modern version involves the hiding of information in legitimate-looking forms such as images and audio files. This is achieved through changing the least significant bits if the image or sound data to correspond in a pre-determined way with the data to be hidden. The changes are imperceptible to the human senses, allowing quite large documents to be sent undetected. Of greater significance is that there is no easy way to tell of the very existence of encoded data. An encrypted email obviously contains data, even if a 3rd party can not read the message. Stego-modified images for example look just the same as the original images, within reason, so there is no telling that any communication has taken place at all.

Using these technologies a highly-co-ordinated attack could in theory be planned and executed by counterparts across the world with no indications of any communication having taken place. This makes our information warrior very hard to find.

NEW TARGETS FOR A NEW WAR

Who is at risk from this new threat? Conventional warfare is most devastating on the less-advanced, developing countries however they make far less-attractive targets for our information warrior. To attack a country with poor telecommunications, maybe a poor power supply and little reliance on electronic commerce or record keeping would be ultimately fruitless, and could expose the attacker to risk of being discovered relatively easily through analysis of a smaller amount of internet "noise".

The best targets for information warfare are therefore the developed nations. I know my bank stores my account information in a computer system. My country's government stores our tax records, as well as all the other personal information used to administer the country in computer systems. The telecommunications systems are computer-controlled, as are the public utilities. I read newspapers on the internet, I do research on the internet and I might even use the internet for critical business applications for which there is no easy substitute. If someone wanted to attack me, I am a great target, and possibly a sitting duck.

If a foreign army were to begin marching down my street, I would be at the very least curious. I would then probably begin to panic slightly as I started to realise the implications. There might be a resistance movement formed to counteract this new oppressive force, as well of course as the armed forces' response which would hopefully be significant. It is with great concern then that facing the possible threat of information warfare we are standing with our backs turned, hoping it will go away.

As I have mentioned earlier, home computers could constitute a great resource for a would-be attacker, however operating systems, as supplied with home PCs are not secure in any way. Internet service providers are, these days, reluctant to secure their networks with even so much as a firewall due to users' complaints that they want to use the latest messaging program, or their favourite games needs certain unusual ports to be open for network play. It's too hard for a provider to keep up with this, so they don't. No security here.

Do we secure our electronic borders the same way we secure our airports and shipping terminals? Not really. Even if governments monitor traffic and flag that which they deem concerning for further investigation they can do little to actually stop an attack in time to prevent damage. They firstly have to realise there is an attack, and such things take time to verify. Attacks could last a fraction of a second and be damaging on a national level if our information warrior were to simply trigger malicious code they have placed on critical machines.

Back to our developing nations. There is in fact a means by which they can make a contribution to an information war that would help bypass any security present on the internet connections between countries. It is not uncommon for multinational companies to set up manufacturing facilities in developing countries where labour is cheaper than at home. In order to do this they might set up an office facility with its internal network, PCs and servers, possibly an internet connection through a good ISP, and maybe even a leased line to their head office. This last device is of greatest concern. An ISDN or frame relay connection will allow administrators of the remote office's computer systems to integrate them seamlessly with those in their headquarters in the company's head office. Whilst there are significant gains from this, an enormous national security gap is also created; there are no longer any borders. If our information warrior were to gain access to such a facility either physically or remotely they could have not only a devastating effect on the systems used within the victim company, but use their superior internet access overseas to launch attacks from within the company's nation of origin. Such an attack could be very difficult to thwart due to time zone differences, language differences and sheer distance.

Again, think back to how much a large company can rely on its computer systems. You don't have to destroy a system to render it useless, and in fact it could take a minimum effort to realise a financial impact on a company. Every minute that someone spends fixing a problem costs money. Every minute that a company can not trade with its suppliers or customers costs it money. Imagine a scenario where an attacker could change a shipping schedule, or modify ordering for a manufacturing plant. An inability to supply products on time could be catastrophic to a corporation who has to meet contractual obligations, and with the increasing reliance on just-in-time delivery many manufacturers could find themselves sitting dead in the water for weeks. In this way the attacker has affected the integrity of the company's data, possibly without ever gaining access to read it.

THE SOLUTION

So how do we fix this problem? How can we secure ourselves against the threat of a possible information war?

Whilst a military assault can be met with a military response, an assault against our personal computers in our homes or at work must be met with a response at that level. This does not mean that we must become militant in our daily lives, nor does it mean that we must not trust the technology we have, as a society, worked so hard to invent and refine.

Awareness

The single biggest contribution we can make to counteracting information warfare is our awareness of the problem. Without an understanding of the risks at an individual computer user level the practises that will help defend us against such an attack will never be put in place. The subject of computer and network security is however starting to become a popular talking point in the media. Whilst this does not provide the level of information necessary to protect anyone's computer systems, it is at least an "ice breaker" that will open the general populations' minds to the concepts and possibilities, and maybe cause them to think twice about their predicament.

Training

Once we are aware of a problem we can start to prevent it. Individuals who use computers at work are now becoming familiar with the basic rules of protecting a computer; Don't share your system password, don't open suspicious email attachments, check floppy disks for viruses before reading them etc... This form of training, whilst truthfully ignored in some cases as is evident by the spread of email-born viruses, is at least a good start towards using computers in a responsible manner. People know the difference between right and wrong, but sometimes need a good reason to choose the former.

Defences

A home computer user can do only so much to protect their machines from being attacked. The best will in the world won't stop an attacker exploiting a vulnerability in your system's operating system, or maybe one of your internet-related applications. In this case there needs to be an electronic defence that will assist in preventing malicious activity at the electronic level. For home PCs such programs are ZoneAlarm by ZoneLabs, The Tiny Firewall, Norton personal firewall and BlackIce Defender. Windows XP and Redhat Linux specifically also contain firewalls that are loaded along with the operating systems. This class of software will provide the minimum defence against internet attacks if set up correctly. This may well be beyond the skill set of a home computer user, but the products are becoming easier to use and more effective with minimum set-up.

Detection

As Eric Cole of SANS will tell you most enthusiastically, "prevention is ideal but detection is a must!!" Do your best to keep the bad guys out, but if they do get in you need to know about it. Many firewalls can be breached by an attacker who really wants to by using various forms of packet fragmentation to bypass the firewall rules. Once inside a network the attacker is in a much better position to create a back door for themselves for future use, so it is vital that their presence is detected. Software packages such as Snort can assist by looking for suspicious traffic within a network segment, or travelling to or from a specific host. This last case, known as host-based intrusion detection, is of greater use to home computer users who may only have one internet-connected computer. These intrusion detection systems (IDS) compare incoming and outgoing packets to a set of known signatures that may help indicate and identify malicious activity. Viruses can be difficult to detect this way, but events such as an attacker scanning for listening ports on your PC will be detected. Programs such as Snort can be set up to drop (disallow) malicious traffic, as well as notify the user of the attack.

Company internet connections

Securing a company network against attack is a reasonably straightforward process on paper, although one that requires time, some capital outlay and the expertise of an experienced network security professional. Whilst a single firewall between the company network and the internet may provide a level of protection, as mentioned earlier it is far from perfect. There are however two other types of systems that can assist a standard packet filtering firewall in its job.

Immediately behind the internet-connected firewall would be a "stateful firewall". This device keeps a table of current incoming and outgoing connections with the aim of denying any from either side that do not meet the TCP/IP protocol standards regarding initiation of such connections. For example a company may deem that port 80 be open on the firewall to allow outgoing connections. This would be a common situation these days as port 80 will allow web browsing from within the company. A stateful firewall will keep track of the source and destination addresses associated with each established connection and deny requests that do not originate from an expected source.

A further level of defence would be a proxy server located between the firewalls and the company's network. A proxy is different to a firewall in that the packets are reassembled at the IP layer rather than simply modified at layer two and retransmitted as a packet filtering firewall does. This helps prevent many forms of fragmentation attacks that rely on a packet fragment containing host and port information being overlaid onto an original packet in order to change the actual destination.

These three systems, combined with a network IDS and host-based IDS on each important host can significantly increase the level of security for even a small company. Whilst the top-end solutions for all of these functions are quite expensive, there are many freeware products that perform very well in combination to provide an level of security, with maybe some compromise in usability, ease of configuration or support.

The big picture

If every individual, company, government department and educational institution with internet exposure took measures such as these the chance of a successful information war against a nation would be greatly reduced. Attacks would still be possible and damage may still be done, but the critical infrastructures that we as a technology-based society have come to rely upon would stand a much better chance of working after the dust had settled.

Such a mass adoption of technology could require legislation, and due to the potential costs involved it could be a hard political decision for a government. In the meantime it is up to us to do what we can until a more comprehensive solution is introduced and agreed upon. I'm not holding my breath.

Summary

With the emerging technology-driven society we are becoming more vulnerable than ever to attacks by electronic means. Every computer system that is connected to the rest of the world through the internet should be secured in even the most minimal ways to help prevent a large-scale attack. Users should be made aware of the threats and trained accordingly, and companies should own the responsibility of securing their own, and their clients' information from malicious use. In equipping ourselves for a world of electronic convenience, we have also provided the weapons by which it could be destroyed. We must now be careful that we do not sit idle, accomplices to our own undoing.

Citations

Tzu, Sun. "The Art Of War." URL: http://www.sonshi.com/suntintro.html

President's Commission on Critical Infrastructure Protection, "Critical Foundations, Protecting America's Infrastructures, Final Report." 13/10/1997 URL: http://www.ciao.gov/PCCIP/PCCIP_Report.pdf

Wilson, Vice Admiral Thomas R. "Global Threats and Challenges Through 2015." 07/02/2001. URL: http://www.dia.mil/Public/Press/statement01.html

Centre for Strategic & International Studies. "Cyber Threats & Information Security." (14/12/2000). URL: http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf

Bush, George W. "Executive Order Critical Infrastructure Protection in the Information Age." URL: http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html

National Cyber Security Alliance. "Stay Safe Online Web Site". URL: http://www.staysafeonline.info/index.adp

Kopp, Carlo. "Part 1 A Fundamental Paradigm of Infowar." Information Warfare. 30/03/2000 URL: http://www.infowar.com/info_ops/00/info_ops033000b_j.shtml

Goldberg, Dr. Ivan "Definition of Information Warfare." Director of the Institute for the Advanced Study of Information Warfare. URL: http://www.psycom.net/iwar.1.html

Libicki, Martin. "WHAT IS INFORMATION WARFARE?" August 1995. URL: http://www.ndu.edu/inss/actpubs/act003/a003.html

Moteff, John D. "CRS Report for Congress." February 4 2000. URL: http://www.iwar.org.uk/cip/resources/pdd63/crs-report.pdf

General references.

http://www.sans.org

http://www.zonelabs.com

http://www.snort.org

http://www.incidents.org

http://www.packetstormsecurity.com

http://www.astalavista.com

http://www.cert.org/

http://cve.mitre.org/

http://www.c4i.org

http://www3.cm.deakin.edu.au/~vstagg/infowar/

http://www.infowar.com/

http://www.iwar.org.uk/