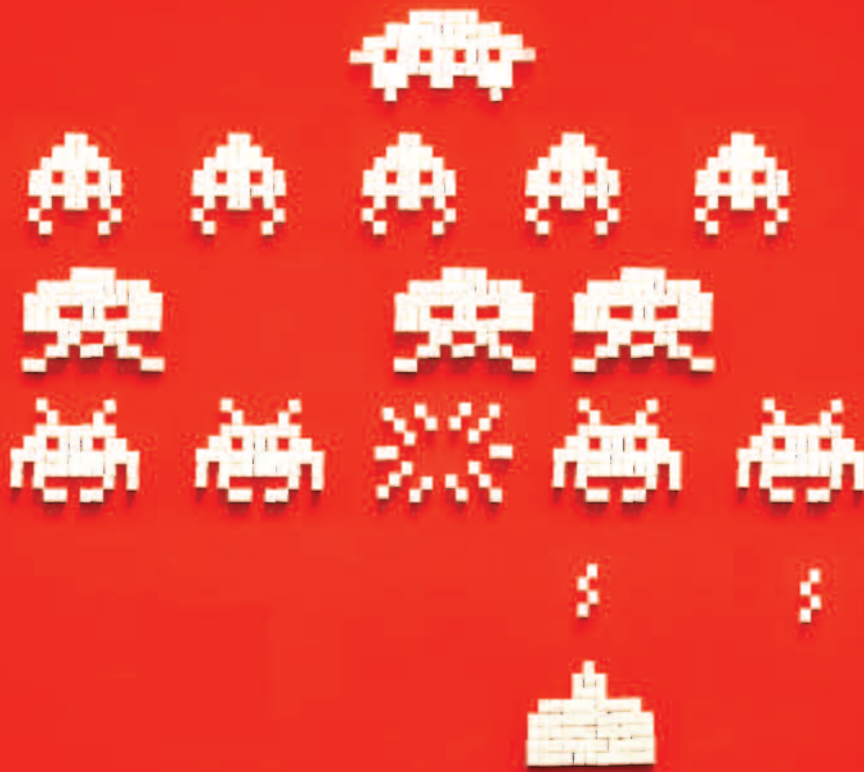


CyberWarfare

Coming to a screen near you soon • May 2011



What do we mean by **Cyber Warfare**?

Simon Milner, Partner JLT Specialty Limited

The traditional view of warfare involves people, guns, bombs, tanks, ships and aircraft mercilessly deployed with a determined purpose to cause physical destruction and death to all those that block their way, to the point of annihilation or surrender. Cyber or Information warfare is not entirely differing in its endgame or approach save that the methodologies corralled to achieve the final result involve electronic means. The power of the computer has grown exponentially since the early days of the Internet.

One single computer operating alone like one small army may win a battle but unlikely to win a war. The electronic universe is not dissimilar as demonstrated by Distributed Denial of Service attacks (DDOS). Consequently, individuals and nation states hell bent on electronic destruction seek to maximise their destructive capabilities by gathering together the collective muscle of many hundreds of thousands of computers in an attempt to achieve their nefarious goals and ambitions.

continued overleaf 



Myth or Reality

You do not need to look very far on the Internet to find examples of those who dismiss cyber and information warfare as a myth. Certain persons have opined that to have a war there needs to be death and we have yet to see any deaths from cyber warfare. Whilst it is true we have not seen death from any electronic espionage or cyber information warfare this, to me, demonstrates a

lack of understanding of the real situation at hand. Undeniably the technical knowledge exists for computers to attack other computers. Whether those computers are in hands of individuals, corporate entities or governments they can all be programmed or instructed to carry out a series of automated commands that could result in Armageddon.



Cover Article continued, What do we mean by Cyber Warfare?

There remains a distinction between information warfare and other forms or cybercrime. We should be aware that the means exist to disable the critical infrastructures that support our economy. We have known for some time now that it is entirely possible to switch off the utility functions that power our homes and businesses whether that be water, gas or electricity. All of these utility functions are controlled by computers in vast operations centres. Granted that these computers may not be linked to the Internet but that in itself merely becomes a small but completely surmountable obstacle to those cyber criminals or governments that wish to perpetrate such destructive activity.

Possibly more relevant to our daily lives is the pursuit of cybercrime. All forms of information have value to the cyber criminal. There remains within the darker recesses of the Internet a modern day version of the gangsters seen in the UK like the Krays and the Richardsons or similarly the mob in the USA as depicted by the likes of the Corleone family or Al Capone. There were numerous cases of extortion that resulted in significant revenue for the gangland fraternity. The cyber criminal seeks information that can be resold. The obvious example of this is credit card information. When this is sold in any real quantity the profits for the cyber criminal are vast. Let us not be blind to the fact that corporate networks hold other hugely sensitive information. For example these corporate entities all have customer lists which may be extremely useful to a competitor. We have seen examples of mobile telephone company employees taking information from one employer to the next which has resulted in loss of revenue for one and a great gain for another. Further, businesses hold trade secret information as well as the latest designs on the products of the future. All this has value and can be resold over the Internet or directly to foreign governments that will pay well for a technological advantage that can be easily leveraged into an economic advantage. The world of Formula 1 provided a spectacular example of industrial espionage involving two different teams. At its core was the desire to discover the technical specification that provided one team's advantage over its competitors.

Cybercrime means different things to different people. At its lower level this can be simply a single cyber criminal pursuing credit card data to earn a fast reward. At a slightly elevated level this can be industrial espionage where one company targets its competitor to endeavour to glean information as to what is known by the target. The next level involves a particular country targeting a certain business to disrupt or hinder the business activities of the target. Uppermost, presently, is the nation state targeting another nation with the aim of causing similar disruption or destruction. We have yet to see more than one nation joining forces with other nations in an attempt to conduct electronic warfare on one or more foreign powers.

There is a lot of rubbish written about what is and what is not cyber war. To the casual observer it is difficult to determine a clear understanding of what actually constitutes cyber warfare. So, it does not require the death of a person.

What are the weapons of war

If we are to have a war what weapons are at our disposal? Rootkits are potentially a very useful weapon. Rootkits allow the user the power of a deity. It allows the user the opportunity to travel anywhere through a network as there is no restriction on what can be accessed. Such travel can go unnoticed as the traveller has, by virtue of the kit, network administrator privileges. This power of the Almighty allows the user to create accounts, delete access by others to their own accounts as well as the ability to install malicious code on the network, including the destruction of data anywhere within the network. These Rootkits are available on the Internet to anyone who knows a little of the cyber underground. These Rootkits can be purchased with some ease. Like many products available to us for purchase these Rootkits come with a user manual just in case the amateur hacker is unsure how best to deploy the kit. Further, these kits also come with a 'helpdesk' function in the form of Internet chatrooms where the hackers openly discuss targets and success rates.

DDOS is short for Distributed Denial of Access. Arguably the electronic version of the weapons of mass destructions (WMD). There are countless examples of this kind of attack. The technique results in the shutdown of a network as it is unable to cope with the requests made of it. Usually, and particularly when SSL (Secure Sockets Layer) technology is operational, one computer wishing to converse with another computer will in effect go through an electronic handshake. Just in the real world when we meet someone we offer out our hand to greet or be introduced to another, often as a means for each individual to identify themselves. Within SSL technology there is a third entity that is trusted to verify that each party is who they say they are. So, when Google communicates with a server belonging to Amazon there exists a certificate that confirms the identity of Google and also confirms the identity of Amazon and not some fraudulent outfit that is trying to pass themselves off as either Google or Amazon. Consequently a DDOS is achieved by sending

millions upon millions of requests

for an electronic

handshake. The

requests are so

voluminous that

the recipient of the

request can not

cope with the

volume of requests

and consequently shuts

down. This DDOS

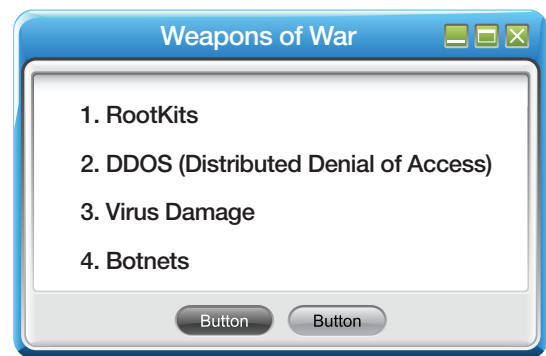
technique can be aimed at

any network with the result that the victim can be rendered un-operational for an extended period of time.

Virus damage remains a potent force. However, a virus is often confused with what is actually only malicious code. Malicious code only becomes a virus when an engine is attached to it. Broadly speaking any set of instructions that damages, alters or destroys electronic information (data) is simply malicious code. The key component of a virus is that it lies dormant for a period of time and that it can do nothing on its own – it is a parasite and must attach itself to something that is executable in order to move and do damage.

Historically we have seen virus contained in emails that essentially has caused mild irritation and or inconvenience.

At best this has resulted in complete shutdown of a mail server



to the extent that no email traffic may travel in either direction.

Such virus examples as 'Melissa' and 'I Love You' caused little damage by comparison to what is achievable nowadays. The malicious code known as a 'Trojan Horse' or 'logic bomb' could potentially cause more damage particularly as we continue to see web based virus emerge. These web based viruses are much more virulent and carry a far greater payload than the virus contained within emails.

Stuxnet was a good example of what can be achieved with a virus and this one did not use the Internet to deliver its payload. Indeed, it is widely believed the virus was loaded onto a USB fob that was very skilfully introduced into computers that were not connected to the Internet yet resulted in the impairment and shut down of the Iranian nuclear facility.

Botnets remain a potent force. Botnets are a series of hijacked computers that are corralled to send messages or information to another computer, otherwise known as a DDOS. When an army of computers has been gathered together their combined power can be used to bring down or render inoperable other computers. This is not a posse in the ways of the wild west in the USA before law and order prevailed. Botnets have the power to deliver an electronic tsunami.



Why we have a war ?



To truly understand the question we do not need to look far back in history to satisfy ourselves that the very nature of our existence on this planet is predicated upon our ability to be lord and master over our domain. Parking momentarily any religious conflict, since time began we lived in a world where someone has sought to dominate and rule someone else. Jumping to the present day this dog eat dog mentality is no different in the corporate arena. It does not take much of a leap of faith to appreciate that countries behave no differently. There is always one nation trying to maximise its advantage over another. We have recently seen the emergence of the potential economic power of China.

They have also begun to flex their military muscles. In previous decades China would have accepted the

combined will of the USA and European nations where today, as a result of its economic power, it is able to resist if it so wishes the previous directions handed to it by the Western world. The electronic and cyber world is no different to the real physical world. Arguably, military might is tremendously costly and why not therefore devote your energies towards electronic and cyber means which surely must be considerably cheaper. To borrow a line from a famous song, 'War! What is it good for? Absolutely nothing' may hold true in the physical world of planes, ships, guns and bombs but it does not hold true in the cyber world. Information can easily be obtained on individuals, companies and governments that can be sold or used to either make revenue or exact revenge or even embarrassment for the victim.

What are the defences available to us?

The sale and purchase of Rootkits on the Internet is most unlikely to be halted or significantly impeded.

It is difficult to defend against DDOS which is why such an attack is such a potent threat.

Some Virus threats are not adequately suppressed by anti-virus software. By its definition anti virus can only respond to those known virus signatures. Therefore, it is a game or match that can never be won by the manufacturers or anti-virus software. That is not to say we should not deploy anti virus (AV) software. Such AV is to be recommended when it comes to dealing with day to day threats and many common forms of virus.

The answer in good defense may lie in a layered approach. Many different layers of security may render a hacker attack less successful but not less likely. If information is held in different places,

physically and otherwise this may deter or impede the attacker, so having the component parts of the information held on different servers may be a good strategy.

No network is completely secure, there is no equivalent of Fort Knox in the digital and electronic world. After all, for people and computers to communicate information has to be accessible and available. We are all cognisant of the need to have the information remain confidential but keeping it that way remains as elusive as the Holy Grail or the Scarlet Pimpernel



How do we build an army?

An army is needed to deliver a DDOS. To build an army of ten of thousands or even millions of computers is something that can be achieved by those with the appropriate knowledge. Simply put a hacker or 'bot herder' can surreptitiously place a piece of code of any computer, often without the victim knowing the code has been placed. The infected computer becomes known as a 'zombie'. This code allows the 'bot herder' to take control of the infected computer and thus enables the 'bot herder' to have control of the infected computer thereby permitting the infected computer to send messages and data to any other computer that the 'bot herder' wishes to attack.

What evidence exists?


Stuxnet is a recent example of what can be achieved by one nation waging electronic attack on another nation. Stuxnet came to light in 2010. It is widely regarded as the first known virus designed to target the physical infrastructure of a nation, in this case Iran. The intended specific targets were the industrial nuclear facilities and in particular the uranium enrichment centrifuges at Natanz. Recent analysis of the virus revealed that it successfully targeted computers running SCADA (supervisory control and data acquisition) on Siemens manufactured machines. What remains intriguing is that the Stuxnet virus or worm targeted computers that were not connected to the Internet. Any nation wanting to attempt to keep certain information or processes more secure would achieve a much higher degree of security when such computers are not connected to the Internet. Whilst it remains unconfirmed most commentators acknowledge and agree that the level of sophistication of the attack was not something achievable by a rogue gang or common bunch of cyber criminals. Certain other Middle eastern nations were thought to be behind the attack as they perceived Iran posed a threat to security in the region if Iran was able to successfully produce nuclear weapons.

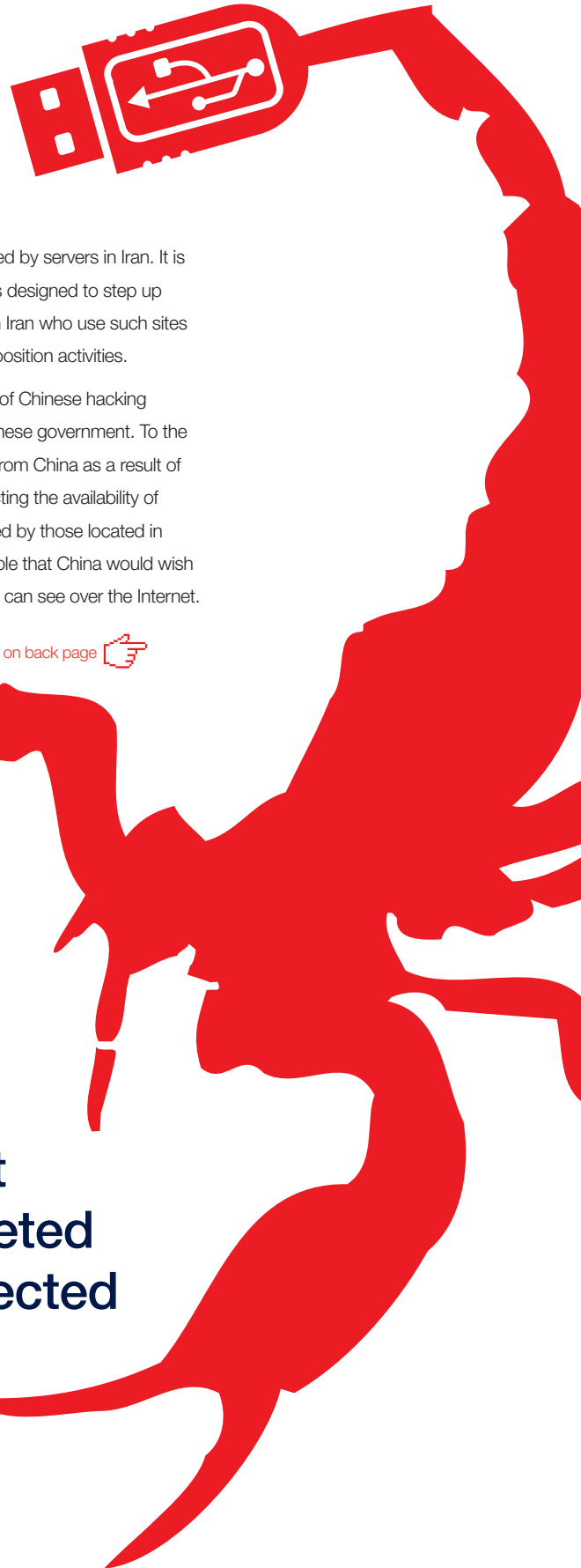
The virus contained PLC code (Programmable Logic Control) that permitted the functionality of the computers to be changed. This had the effect of disrupting and or shutting down the uranium enrichment program

as the virus changed the instructions that the computers were supposed to carry out.

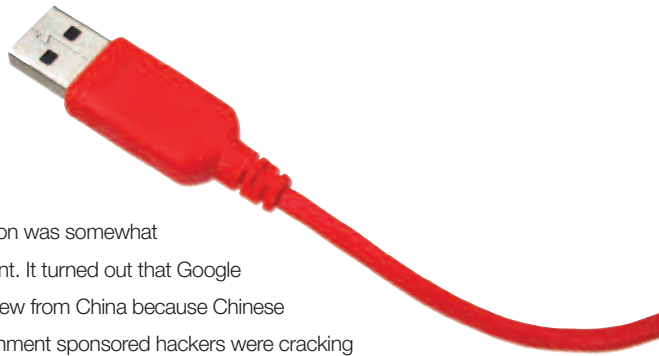
In a different attack Iran has been accused of passing itself off as Google, Yahoo Skype, Mozilla and Microsoft. The trick was to convince the users of these sites that they were real when indeed they have been mimicked by servers in Iran. It is thought that the mimicking was designed to step up scrutiny of opposition groups in Iran who use such sites as Google to organise their opposition activities.

In 2009 Google was the victim of Chinese hacking activities sponsored by the Chinese government. To the wider public Google withdrew from China as a result of the Chinese government restricting the availability of certain websites being accessed by those located in China. It is wholly understandable that China would wish to restrict what Chinese people can see over the Internet. However, the reality of the

continued on back page 



‘What remains intriguing is that the Stuxnet virus or worm targeted computers that were not connected to the Internet.’



situation was somewhat different. It turned out that Google withdrew from China because Chinese government sponsored hackers were cracking Google's databases to gather information on what Chinese nationals had been viewing on the Internet and what information had been exchanged.

There have been reports that a Russian security company plans to release an upgraded exploit package that targets SCADA systems. These systems are used in factories, utilities and other kinds of industrial activities.

All the brouhaha concerning Wikileaks confirms the ability of one organisation to access the information held by governments. This in many ways is the reverse of industrial espionage in that here the victim is the government and not the corporate entity. The hacker group known as 'Anonymous' who supported Wikileaks participated in a number of cyber attacks dubbed 'Operation Payback' which culminated in several denial of service attacks.

Estonia, which is one of the most connected countries in the world today, suffered a series of attacks in 2007. Many in the country were under the impression they were under an electronic

invasion. The leading banks were under siege and the attack crippled ATM's in Tallinn. The country's leading newspaper, which is often read online, could not be accessed. Government communications systems were down and rendered inoperable. Whilst the cause of the attack might have been internal unrest it was clear that the electronic traffic was coming from abroad, Egypt, Vietnam and Peru were among the electronic invaders. Whilst the attacks on Estonia were carried out by 'script kiddies' it demonstrates what is readily achievable should a foreign government wish to perform a similar electronic invasion.

The Pentagon has stated that its systems are probed for weaknesses many millions of times a day. Whilst we can accept that on most of these occasions the probing is executed by the lone cyber criminal only a complete fool would not accept the US was not being probed by other nations. So, we are probably already at war, an information warfare, but we just do not know it yet!

'Estonia, which is one of the most connected countries in the world today, suffered a series of attacks in 2007'