Cyber War:
An Emerging Threat In An Increasingly Connected World

ARJUN VENKATRAMAN

Introduction

In a world where inflation strikes everything, waging warfare is also becoming increasingly expensive. The value associated with individual human life is increasing, making it impractical and undesirable for nations to engage in long drawn physical conflict. At the same time, the rise of the global supply chain and the global internet have created a new battleground and a new set of tactics, which allow for warfare of a nature for which traditional defence establishments are thoroughly unprepared. Cyber warfare is part of this new breed of conflict, a type of information warfare. Information warfare is simply the use and management of Information and Communication Technology (ICT) to gain a competitive advantage over an opponent. This article attempts to speak about the expanding scope of cyber war, the response of different nations to this threat and to look at some of the latest global trends in cyber war and analyse their relevance to India.

Cyber War is Not Just Hacking

Cyber warfare has been described as "politically motivated hacking to conduct sabotage and espionage". Traditionally, the word "hacking" is used in the technological world to describe the quest for better and more elegant solutions to existing problems through improvisation and experimentation. In recent times, the sensationalist media has misappropriated the term and limited it to describe computer crime. The word cyber, however, refers to systems of control. Therefore, any attack on a system of control may be considered a cyber attack. Hacking as a discipline is simply a mechanism to push the envelope of control systems and to break those limits in order to extend the system to its next level. Hacking, even in the context of computer security, may be used for both offensive or defensive purposes. Cyber war incorporates elements of computer hacking but is not limited to it. Physical surveillance, espionage, social engineering and propaganda all play an equally large role in cyber war.

Physical surveillance, espionage, social engineering and propaganda play an equally large role in cyber war.

Where the Threats Are

Physical Infrastructure

The most intuitive example of cyber war at the physical level is Electronic Warfare (EW). EW involves the use of the electromagnetic spectrum and/or directed energy to impede, damage or defend against an opponent. EW may be directed at both military and civilian targets. Most modern economies are heavily reliant on unimpeded access to the electronic spectrum. Therefore, conflict in this sphere can have an adverse impact on the defensive as well as the economic interests of a nation. EW includes the elements of attack, protection and intelligence gathering. Electronic attack and protection are typically expected to be seen only in physical conflict theatres or border regions since making large impacts from the spectrum perspective is expensive and difficult over long ranges. However, electronic intelligence is a segment of EW that has significant relevance to supremacy in a cyber conflict. The identification of enemy transmissions and other electromagnetic emissions is called Electromagnetic Intelligence (ELINT) or Electronic Intelligence. The interception and analysis of communications is known as Communication Intelligence (COMINT).

Since World War II, the United States has consistently been the global leader in EW capability. The beginning of this decade saw the US usher in a new breed of attack altogether – the non-military drone strike. On February 04, 2002, the Central Intelligence Agency (CIA) first used a drone for a targetted killing in Afghanistan, in the Paktika province near Khost. This is relevant from an EW standpoint, since it marks the shift in the trend of desired outcomes from

EW. While erstwhile missile strikes were intended for large scale destruction, inviting international pressure and the near certainty of full scale war to follow immediately, drone strikes allow for much more precise and contained damage, allowing opponents to target specific areas, buildings or sometimes even individuals remotely. Today, almost every international military power is working on a UAV (Unmanned Aerial Vehicle) programme with the United States and China leading the pack. While drones and aerial surveillance are at the forefront of EW concerns, there is another far more vulnerable area which often evades scrutiny.

As industrial and infrastructural automation increases, large facilities rely more and more on Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems, being originally designed for the purpose of process automation, do not often give much thought to security in the design phase. When these systems are deployed and then connected to networks to allow remote management, they represent a serious vulnerability that can be exploited by both foreign and domestic elements. The Stuxnet worm that ruined almost 1/5th of Iran's nuclear centrifuges starting in 2010 was allegedly a joint US-Israeli defence project. This worm apparently exploits zero-day vulnerabilities in the Microsoft Windows operating system and networks to infect a system and then seeks out the Siemens Step-7 software which is a SCADA software. Once it has control of a SCADA system, a worm of this nature can be used to operate automated equipment in ways that its parameters do not cover, resulting in, at worst, industrial disasters of the ilk of Union Carbide and Chernobyl, or worse, consistently cause wear-out due to mismanagement in industrial equipment, driving up the costs of production. It is interesting to note that Microsoft Windows and Siemens Step-7 are both closed source software programmes developed in the West and protected by international intellectual property rights, rendering it difficult if not impossible for even customers to fully understand and appreciate the security risks concealed in the source code.

Neelabh Rai, the consultant for information security at Pyramid Cyber Security and Forensic Private Limited, was quoted in a *Tech Target* article as saying that Stuxnet may be a major security threat for India, since most of the industrial control systems in the country that run manufacturing plants, power generation and distribution plants, refining water treatment plants, and oil and gas plants use Siemens' SCADA systems. Even worse, the Indian Space Research Organisation's INSAT-4B satellite, also uses the Siemens S7-400 PLC and SIMATIC

WinCC and is considered a target for Stuxnet. It is interesting to note that the page referring to this concern was not available except as a cached copy (see refs).

Connected Population

Apart from the spectre of wide scale industrial damage, and no less concerning, is the potential of cyber warfare against ordinary citizens. Duqu, also a member of the Stuxnet family, attacks Microsoft Word, a programme used by a large majority of computer users globally as a word processor. Duqu's purpose is to gain information about industrial control systems and other valuable resources and provide services to external attackers. This sort of tactic is used to convert regular computers into drones to be used in distributed denial of service attacks.

Yet another example of cyber warfare against ordinary citizens is the Flame virus. The Flame malware, which is being used for espionage activities in the Middle East, can utilise a regular computer and turn it into a very effective automated agent. It can take screenshots, record audio, collect keyboard activity and network traffic. Flame also attacks Microsoft Windows-based operating systems. Meanwhile, from the Chinese side, the People's Liberation Army (PLA) Unit 61398 has been accused by the US of commercial espionage activities. Some of the operations it has been credited with include the Operation Shady RAT (Remote Administration Tool) that was used to target athletic oversight organisations during the 2008 Summer Olympics by using a paradigm normally employed for remote management of computer resources to gain control of their systems.

Operation Aurora that was used to illegally access *inter alia* the Google accounts of Chinese dissidents and steal intellectual property from several American Information Security Providers (ISPs) such as Rackspace, Adobe and Juniper Networks. Operation GhostNet, sends contextually relevant information to target organisations (typically government bodies) via e-mail with malicious attachments, which, when downloaded, also render the target computer under the control of the attacker. It is important to note that systems compromised by the GhostNet attack have been discovered in Indian government establishments as well. All of PLA Unit 61398's attacks listed above appear to primarily target Microsoft Windows-based systems. Now South Korea is also purported to be developing its own breed of Stuxnet-like viruses. To those of us in the open source hacker world who have been observing trends for the past 10-15 years, the fact that these serious threats target Microsoft products came as no surprise as Microsoft's links to the US intelligence establishment have been the subject of heated debate and analysis in hacker forums for at least that period. This link has been further established by the revelations of the Snowden leaks, which allege that Microsoft shared sensitive user data with the National Security Agency (NSA). The link between zero-day vulnerabilities and closed source software is also of importance to the cyber war discussion.

The mutual dependence of the global supply chain and the global internet has created a new battlefield, with new targets.

Denial of Service and Distributed Denial of Service

The mutual dependence of the global supply chain and the global internet has created a new battlefield, with new targets. One class of targets is online services. A significant portion of a nation's economy today depends on online services such as communications, banking, transportation, travel *et al.* Denial of Service (DoS) attacks render an online service inaccessible by, or too busy to process, bona fide service requests from genuine users by making a large volume of spurious requests from an automated source. In plain terms, this is similar to a travel agent hogging a ticket window and preventing regular customers from purchasing tickets. A Distributed Denial of Service (DDoS) is an extreme form of denial of service, where the automated attack comes from multiple sources, typically spread over a vast geography. DDoS is the worst nightmare of the cloud computing industry. Cloud computing is an increasingly popular paradigm in the world of online services, wherein economies of scale are employed to provide basic mass user services such as email, social media, content sharing *et al* at a global scale from centralised data centres located in serviceable, economic, well connected areas. However, the nature of the internet being distributed, centralised resources simply represent desirable targets for attackers. Protection measures include mechanisms to identify bonafide requests, sharing of information and blacklisting of attack sources between service providers, advanced spam detection algorithms *et al.*

Information Attacks

Apart from directly damaging computers and other systems, an entire range of attack possibilities exists in the realm of content. Since Edward Bernays misappropriated Freud's theories for use by corporations and political interests by inventing the profession of public relations, mass information media has been used by large interests to direct public opinion. Advertising and mainstream media have begun to render people unable to make logical decisions independently by outsourcing the decision-making process to purported "experts" whose credentials cannot be verified. This has resulted in an overdependence on information systems, opening new avenues of vulnerability. With the advent of the internet, social media and process automation, it is today possible for even ordinary citizens to have a reach at par with the world's largest corporations. This means that information from the internet must be used with great care.

Developing economies like India are particularly vulnerable to propaganda, since the information sources are controlled by directed interests, rendering the average users powerless to exercise their own logic and discretion. This trend is being exacerbated by the increasing dependence being built on the cloud and mobile systems, since these are all centrally managed. A centrally managed system, as mentioned before, presents a very juicy target to attackers and once compromised, damage is more widespread and costly. It would be far more effective to build reliance on distributed, localised means of communication linked with each other using multiple pathways, so that in the event a primary pathway is compromised, alternative routes continue to function. However, this will imply a paradigm shift and with the new economy's liking for the mobile and cloud industries, it is expected that we will repeat many of the mistakes of the developed economies.

Participation of Non-State Actors

The participation of elements of civil society in cyber war is a major concern area, or at least should be for any defence establishment. Both the dominating powers in the cyber warfare arena, i.e. the United States and China, regularly utilise cadres of cyber attackers and defenders from their regular populations. These cadres typically operate on the fringe of legality and are similar to the pirates of the high seas in olden times in this regard. Just as pirates sometimes received temporary or permanent fiat from different states at different times to accomplish tasks that would be illegal by international law or may be simply too risky to commit state resources to.

The Chinese appear to have become better at this form of warfare than any of the other superpowers. The Honker Union and the Red Hacker Alliance are of note in this regard. The word honker – 红客 (hongke) – is a name that means "red guest". The word is a play on the Chinese term for hacker – 黑客 (heikei)

– translates to “black guest”. The substitution of red for black in the name is assumed to reference the connection with the People’s Liberation Army (PLA). The Honker Union is known for its attacks against Japanese and Taiwanese websites. They came to note in 2012 and 2013 for their sniffing of Japanese targets after Japan’s announcement of its intention to purchase the Senkaku Islands. The Red Hacker Alliance, which at one time had 80,000 members, is known to be one of the largest hacker alliances in the world. It is currently merged with the Honker Union and was reported to be involved in a planned DDoS attack on CNN.com in 2008. A new entity in the non-state sector, believed to be of Chinese origin is the Elderwood project, which is a group of attackers who share and reuse exploits and knowledge of vulnerabilities for maximum impact. They are believed to have provided the vulnerability information that supported the 2009 attacks on cloud providers such as Google. A notable hacker group in the West is the Anonymous Collective, known for its attacks on large targets such as the Church of Scientology and child pornography websites among others. Anonymous is known to espouse the causes of internet freedom and democracy as understood from a Western perspective.

While analysing the presence of hacker alliances on the internet, it is important to note the role of language. A substantial portion of the internet is in English, and search capabilities in other languages are still in their evolutionary stages. Since English speaking hackers have control of the majority of the internet, they tend to present themselves as the heroes and the Chinese as the villains. The true picture is not so simplistic. Therefore, it is important for countries like India whose core language is neither English nor Chinese to develop an independent perspective of its own regarding the nature of internet security. The large majority of Western hacker websites claim to espouse the cause of internet freedom. The vast majority of Chinese speaking hacker websites claim to be resisting the imperialism of the West. In this conundrum, India would be best advised to establish its own indigenous policy for cyber security. While measures have begun in the form of the National Technical Research Organisation and the Computer Emergency Response Team, it is imperative that more scalable initiatives also be undertaken.

Recommendations

Encourage Technical Skill Building at the Grassroots Level: Average Indians are very susceptible targets for cyber warfare, since the level of technical skills available to them is very limited. To remedy this, low cost mechanisms must be employed to introduce technology at the primary school level, so that young Indians can grow up with a familiarity with technical equipment. This will enable more responsible usage as adults and equip them to make better decisions and stay safe while navigating the maze of information technology that this generation is busy creating for them to inherit.

Encourage Citizen Participation in Cyber Defence: Citizens are currently discouraged from participating in cyber defence by the manner in which information laws are being implemented. The state would be well advised to encourage people to learn cyber defence skills so as to better secure their own digital lives as well as to help secure the internet as a whole. This involves subjective training on content analysis and response as well as operational training on defensive technologies.

Establish the Defence Establishment as the Appropriate Source of Defence Training: Since the defence establishment has the operational experience and expertise on threat response, rather than surrendering the training in cyber defence to the increasingly commercial educational machinery, it would be more effective to establish the defence establishment as the source of cyber defence training. The delivery of this training could be done through civil society institutions such as polytechnics and Indian Institutes of Technology (ITIs) as well as through vocational training programmes already in operation through civil society organisations. The connect to the defence establishment will also allow Civil Society Organisations (CSOs) to interact meaningfully with the defence establishment to better understand the security concerns of the establishment and to propagate relevant information about mitigating the same to civil society.

Reduce Reliance on Closed Source Software and Externally Mass Produced Proprietary Equipment: As mentioned earlier, there is heavy reliance in the defence industry on closed source technology and proprietary equipment. While this is unavoidable for weapons of physical warfare, in the realm of cyber war, it seems inappropriate. Closed source software is software that is sold as it is, without the underlying design and implementation details being shared with the end user. Microsoft Windows, Microsoft Office, Siemens-7 and other SCADA systems mentioned earlier in this article are all closed source software systems. Closed source software systems, besides being inscrutable, also have the added disadvantage that the period between the discovery of a zero-day exploit and a fix is longer, since the number of developers is limited. A zero-day exploit or vulnerability is a vulnerability in software that is discovered after release,

Military establishments must develop indigenous capacity for cyber defence.

giving the programmer zero days to fix the problem. A vulnerability ceases to be a zero-day vulnerability when a fix is released.

Open source software has a quicker time to zero-day fixes because the source code being available to the public at large, it is scrutinised more and fixed more often. Moreover, the availability of the source code to the end user ensures that better localised customisations can be employed, making the product more suitable to the local use case than an off-the-shelf system. Moreover, most closed source software giants are multinational corporations, making it difficult to analyse their political leanings. At this time, most of the defence establishment runs Microsoft Windows at the end user level, which, as mentioned before, is vulnerable to malware such as Stuxnet, Duqu and Flame, which are all national security risks. Almost identical concerns apply to mass produced technology equipment imported from overseas (typically from China). Huawei and ZTE, the companies that produce the largest number of USB modems purchased in India, have both been under investigation by US intelligence agencies for industrial and political espionage.

Build Indigenous Capacity: Rather than outsourcing cyber defence to private contractors, it would be best for military establishments to develop indigenous capacity. While this is difficult while relying upon closed source and patented technology, an open source approach would allow for freer domestic innovation. This approach should not be limited to software but should apply also to hardware. If the question of innovating new indigenous information and communication technologies is left open to the citizens of this country and appropriate encouragement is provided at the policy and implementation levels, we will be able to overcome our reliance on external products and build a new and more inclusive paradigm for technological advancement.

Conclusion

The digital arms race is expected to continue indefinitely, or at least until Moore's law holds good in the computing world: "Moore's law is the observation that, over the history of computing hardware, the number of transistors in a dense integrated circuit doubles approximately every two years." This essentially means that the computing power available at any given level of the economy is expected to double every two years, or rather 18 months to be exact. The veracity of this law can be analysed by observing the rapid rate at which the average users change their personal electronics for newer versions.

What this also means is that computers at the end user level are expected to become more and more powerful over time. Given that Moore's law cannot be expected to hold good indefinitely, it is expected that by 2020, we will have reached saturation point on the number of transistors that can be packed into a circuit. Beyond that, there are computing paradigms being explored that make use of biological, chemical and neural processes, but these being largely experimental, it can be expected that there will be a period of approximate parity between military grade and user grade electronic equipment, particularly given the time lag in procurement for public purposes. It is, therefore, important for military establishments to begin reducing dependence on superior processing power and information obfuscation as a means to dominate in cyber warfare. How the equipment and information is used will determine who dominates.

Mr **Arjun Venkatraman** is an engineer, solutions architect and social entrepreneur. He is the Managing Trustee of the Mojolab Foundation, a non-profit organisation engaged in developing low cost technology for grassroots application in developing economies

References

1. "21 Steps to Improve the Security of SCADA Systems", http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
2. "Improving SCADA Security" – InfoSec Institute - http://resources.infosecinstitute.com/improving-scada-system-security/
3. "Stuxnet Infected the Network of Russian Nuclear Facility – Security Affairs," http://securityaffairs.co/wordpress/19604/malware/stuxnet-russian-nuclear-facility.html
4. Results of SANS SCADA Security Survey - SANS Institute Reading Room – http://securityaffairs.co/wordpress/19604/malware/stuxnet-russian-nuclear-facility.html
5. "Security for Critical Infrastructure SCADA Systems" – SANS Institute Reading Room – http://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644
6. "Huawei Routers Riddled with Vulnerabilities – Slashdot", http://beta.slashdot.org/story/172739
7. Inside Huawei, the Chinese tech giant that's rattling nerves in DC – Cnet – http://www.cnet.com/news/inside-huawei-the-chinese-tech-giant-thats-rattling-nerves-in-dc/
8. "The Company that Spooked the World" – Economist – http://www.economist.com/node/21559929
9. "The Elderwood Project" – Symantec, http://www.cs.cornell.edu/courses/CS6410/2014fa/slides/Symantec_ElderwoodProject_2012.pdf
10. "Is Elderwood the Digital Arms Dealer that Fuelled Attacks on Google?" – *The Guardian* –

http://www.theguardian.com/technology/2014/may/15/elderwood-digital-arms-dealer-google

11. "The Elderwood Project" – Symantec – http://www.symantec.com/connect/blogs/elderwood-project
12. "Elderwood Project Behind Latest Internet Explorer Vulnerability" – Symantec – http://www.symantec.com/connect/blogs/elderwood-project-behind-latest-internet-explorer-zero-day-vulnerability
13. "Flame Virus Explained", RT.com - http://rt.com/news/flame-virus-cyber-war-536/
14. "Operation Olympic Games" – Wikipedia – https://en.wikipedia.org/wiki/Operation_Olympic_Games
15. "OSI to Provide SCADA System to TATA Power in Mumbai", Automation.com http://www.automation.com/automation-news/project/osi-to-provide-scada-system-to-tata-power-in-mumbai SCADA Systems Security – InfoSec Writers – http://www.infosecwriters.com/text_resources/pdf/SCADA.pdf
16. "The Use of the SCADA System in Water Management of Shatt Al-Hilla in Iraq", *International Journal of Environmental Monitoring and Analysis* – http://article.sciencepublishinggroup.com/pdf/10.11648.j.ijema.20130105.19.pdf
17. "Stuxnet Worm Attack – Are Indian SCADA Systems Ready?" – Techtarget – http://searchsecurity.techtarget.in/news/2240023035/Stuxnet-worm-attack-Are-Indian-SCADA-systems-ready
18. "The Century of the Self" – BBC – http://en.wikipedia.org/wiki/The_Century_of_the_Self
19. "Understanding SCADA System Security Vulnerabilities" – RipTech – http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf
20. "SCADA in Indian Power Systems" – Electricity India – http://www.nrldc.in/docs/documents/Articles/SCADAinIndianPowerSystem_PKA.pdf
21. "South Korea Concocting Stuxnet-like Virus to Infect Enemies" – NakedSecurity – http://nakedsecurity.sophos.com/2014/02/24/south-korea-concocting-stuxnet-like-virus-to-infect-enemies/
22. "Stuxnet Attack was an Illegal Act of Force", Wired.com http://www.wired.com/2013/03/stuxnet-act-of-force/ The Repository of Industrial Security Incidents - http://www.securityincidents.org/
23. "Building a Cybersecure Plant" – Siemens – http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/
24. "Exploring Stuxnet's PLC Infection Process" – Symantec - http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process
25. "Stuxnet Malware Targets SCADA Systems", Trend Micro http://about-threats.trendmicro.com/us/webattack/54/STUXNET%20Malware%20Targets%20SCADA%20Systems
26. "Stuxnet Far More Dangerous than Originally Thought", BusinessInsider http://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms
27. "Microsoft Handed the NSA Access to Encrypted Messages", Guardian http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
28. "Huawei Targetted by NSA Espionage Program" – FierceWireless – http://www.fiercewireless.com/tech/story/huawei-targeted-nsa-espionage-program/2014-03-23