14 Cyber Warfare: Surviving an Attack

By Devabhaktuni Srikrishna

Cyberspace is a new domain of warfare. Created to minimize the vulnerability of United States communications networks to a crippling nuclear first strike by the Soviet Union, the Internet that was originally envisioned to enhance U.S. security is turning into a battlefield [1] for nations or sub-national groups to launch virally spreading attacks [2] and induce network failures potentially involving critical infrastructure systems.[3]

Cyber warfare and cyberoffense [4] have been a part of U.S. military operations for decades.[5] Treaties and rules of engagement define what is off-limits during a cyberwar.[6] The more vulnerable the system is, the more policy is necessary to deter adversarial nations from launching attacks, and vice-versa.

Some cyberattacks are analogous to air forces probing one another's defenses or perhaps to espionage during the Cold War, which occurred though there was no official war and no physical harm. Cyberespionage operations of China, for example, against the United States and its allies have been going on for years and will never really end.[7]

U.S. Air Force General Kevin Chilton, former Commander-in-Chief of Strategic Command, has stated that every computer system fielded by U.S. servicemen is on the front lines of a virtual battlefield.[8] Perhaps all people should think of their computer systems (PCs, mobile devices, etc) in this manner, not just as a tool for achieving personal goals but also as a conduit for an enemy attack.

This survey of cybersecurity literature explores answers to the question of how to secure the Internet from a cyberwar.

What is Cyberwar and Cyberoffense?

Richard A. Clarke and Robert Knake offer a vivid explanation of some of the largest recent cyberattacks in their book, *Cyber War: The Next Threat to National Security and What to Do About It*. Once a virus or malware is inadvertently downloaded onto a networked personal computer (PC) by a user[9], the PC can be commandeered to perform cyberattacks ranging from electronic banking crimes, politically motivated denial of service attacks[10], email spam[11], and click-fraud[12].

The U.S. Government Accountability Office (GAO) offers a taxonomy of different types of attacks in "Cybersecurity for Critical Infrastructure Protection,"[13] – denial of service, exploits, logic bombs, sniffers, Trojan horses, viruses, and worms. Attackers also employ arbitrary combinations of these attacks as part of an integrated attack plan.

Causes of Cyber Vulnerability

In "Cyberwar and Cyberdeterrence," Martin Libicki points out that system vulnerabilities do not result from immutable physical laws, but due to a gap in theory and practice. Organizations are vulnerable to the extent they want to be and to how much they want to spend to address vulnerabilities. [14] And cyber vulnerabilities can be completely eliminated -- unlike conventional, nuclear, chemical, or biological which are permanent vulnerabilities due to laws of nature.

Aside from keeping individual PCs secure and virus-free through antivirus software [15] or having Internet providers enforce anti-virus policies on their subscribers,[16] several tools with varying degrees of sophistication exist for identifying and policing unusual behavior in real-time – for individual PCs (Bothunter[17]), enterprise networks (Damballa [18]), federal government networks (Einstein [19]), and critical infrastructure (Perfect Citizen [20]). The drawback of such systems is that creative attackers continue to find ways to circumvent them. Software must be constantly updated and will at some point be outdated when the next threat emerges.

Another option is to eliminate anonymity on the Internet through end-to-end authentication in order to prevent anonymous attackers from carrying out distributed attacks with impunity.[21] While end-to-end authentication may prevent cyberattacks and identify the culprits, it would result in the loss of privacy, individual liberties, and split the Internet into multiple Internets.

As an outstanding example of loss of privacy and violation of individual liberties, cyberattacks on hospital networks are of particular concern as they deal with patient-sensitive data. In the case of medical records, system design involves backup and distributed storage – attacks that involve data destruction can be recovered if the data is routinely backed up in multiple independent locations. The lost data can be made accessible quickly and reliably after an attack. But unless stronger data protection measures are in place, the concern remains that a cyber thief can steal sensitive data that could be used to blackmail people with certain medical conditions.

Similarly there ought to be no critical infrastructure connected to the Internet left vulnerable to cyberattack. Curiously, the nuclear power industry, known for its fail-safe engineering in reactor design, is sometimes recognized as better prepared than most other industries to withstand cyber threats. It does this through upfront planning and design for isolated or disconnected operation to avoid the worst-case scenario of a reactor being commandeered by a hacker, "The safety and control systems that operate nuclear power plants are isolated from the Internet and are protected against outside invasion." [22]

Who Are the Cyberattackers?

The same Internet that allows for billions of dollars in electronic commerce can also empower a single mobile device to control millions of personal computers (PC) around the world for electronic crime. Due to its anonymous and highly scalable nature, the Internet can also be used as a weapon to disrupt and commandeer essential services that rely or connect to the Internet.

Cyberattacks can be carried out by anyone with the know-how and interest, and in many cases the cost of attacking is disproportionately small compared to the potential damage that can be inflicted. Groups involved in planning and executing attacks range from nations to individuals. Most nations would probably agree that attribution of a cyberattack is imperfect – whether it means identifying the nations involved, sub-groups, or motives. [23] Mistakes in attribution due to haste or inaccurate information can lead to collateral damage.

While the GAO summarizes potential attackers and motivations, [24] the range of possible groups and motives is much broader: criminal groups, hackers, hacktivists, insiders, intelligence agencies, terrorists, and virus writers.

Martin Libicki explained that attribution is difficult because: [25]

1. Cyberattacks can launch from anywhere, and computers do not leave physical traces behind.
2. A rogue employee or sysadmin presents risks similar to those of an attacker within the periphery of a closed system.
3. Code within the electronics supplied by third parties can bring down a system at a pre-specified time or in response to some system state.
4. When attribution is localized to a country or on government networks, it may be someone operating on behalf of what they perceive to be state interests without clear authorization from the state.
5. Organized criminals posing as governments, or "super-patriots" may be attacking in advance of what they perceive to be government actions.

An example of a cyber attack by a country or nation was revealed when the group WikiLeaks released a cache of confidential American diplomatic cables to the New York Times among several other news organizations. Some of these cables described a computer hacking effort against Google's computer system by the Chinese Politburo.[26]

This cyber intrusion was part of a global campaign to sabotage the multinational corporation and carried out by Chinese operatives and computer hackers hired by the Chinese government, according to news stories about the leaked cables.

The recent Stuxnet PC virus illustrates a cyberattack by an anonymous agent. The Stuxnet virus spread via PCs and was designed by its authors to infect and then destroy or sabotage the operation of a specific type of CPU made by Siemens and used for automated control in electric power plants worldwide including in North America, Iran, Pakistan, India, Indonesia, and Germany. [27]

Articles and weblog posts suggest that the U.S. and/or Israel [28] targeted Iran's nuclear program.[29] Attribution in the Stuxnet case is far from straightforward – unless a link or evidence is found.[30] In spite of international politics on nuclear proliferation, it is difficult to imagine the motive of a country like the U.S. to carry out such a sloppy sabotage attack – especially as the cyberattack affects reactors in many countries including the United States. [Editor's Note: As this article was going to press, the New York Times reported that Iranian President Mahmoud Ahmadinejad said that a cyberattack had damaged an unspecified number of Iranian centrifuges for enriching uranium. [31] Reportedly, Stuxnet caused the frequency of the spinning centrifuges to change so that the devices would spin out of control. Ivanka Barzashka, a research associate at FAS, was one of the first analysts to discover this feature of Stuxnet.[32]]

The attack was facilitated because systems deployed worldwide are (1) standardized on a vendor's product so the virus can replicate and (2) use of proprietary code used in the standardized platform – not benefiting from widespread peer-review (vs. open-sourced software/code).

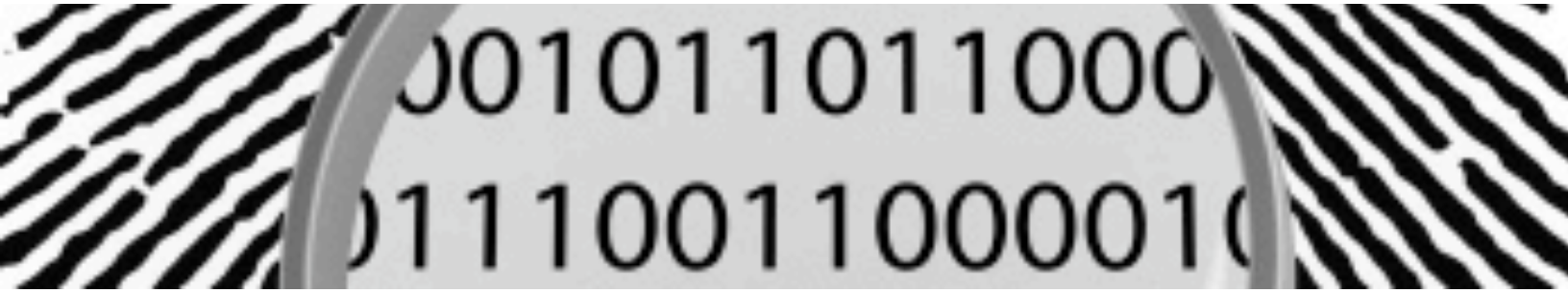
Conclusions

To secure the Internet from cyberattacks requires a combination of public policy, standardization, and market forces. Intelligent application of simple, proven engineering design principles in different situations such as end-to-end authentication, behavioral analysis, distribution (vs. centralization), backup, redundant routes (vs. single paths), fault-tolerance, diversity of supply (hardware, software, and services), and decoupling from the Internet, might eliminate the worst consequences of most vulnerabilities.

Perhaps the biggest challenge is to create secure practices for individuals and organizations that are easy to understand, adopt, and apply when designing and operating networked computer systems. [Editor's Note: FAS will continue to research this issue and provide practical policy recommendations.] **FAS**

ENDNOTES

1. Bruce Schneier, *Crypto-Gram Newsletter*, "The Risks of Cyberterrorism", June 15, 2003: http://www.schneier.com/crypto-gram-0306.html; See Schneier on Security, a blog covering security and security technology, "Cyberwar", June 4, 2007: http://www.schneier.com/blog/archives/2007/06/cyberwar.html.
2. *Christian Science Monitor*, "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?" by Mark Clayton, September 21, 2010: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.
3. *Wired- Threat Level* (a blog about privacy, crime and security online), "Report: Critical Infrastructures Under Constant Cyberattack Globally" by Kim Zetter, January 28, 2010 http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/.
4. *United Press International*, "Analysis: USAF's Cyber Offense Capability" by Shaun Waterman, May 15, 2008: http://www.spacewar.com/reports/Analysis_USAFs_cyber_offense_capability_999.html, and *Armed Forces Journal,* May 2008, "Carpet bombing in cyberspace: Why America needs a military botnet" by Col. Charles W. Williamson III, http://www.armedforcesjournal.com/2008/05/3375884. See also *The Economist*, "Cyberwar", July 1, 2010: http://www.economist.com/node/16481504.
5. *Foreign Affairs*, November/December 2009, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses" by Wesley K. Clark and Peter L. Levin: http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.



ENDNOTES

6. *The Washington Pos*t, “15 nations agree to start working together to reduce cyberwarfare threat” by Ellen Nakashima, July 17, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html; *The New York Times,* “Step Taken to End Impasse Over Cybersecurity Talks” by John Markoff, July 16, 2010: http://www.nytimes.com/2010/07/17/world/17cyber.html; See also the news release on a special report from the Council on Foreign Relations, “U.S. Must Take Stronger Leadership Role to Protect Interests at Risk in Cyberspace, Says Council Special Report”. The *Council Special Report, Internet Governance in an Age of Cyber Insecurity,* is by CFR Fellow Rober K. Knake: http://www.cfr.org/publication/22880/us_must_take_stronger_leadership_role_to_protect_interests_at_risk_in_cyberspace_says_council_special_report.html ; *Arms Control Today*, June 2010, “Multilateral Agreements to Constrain Cyberconflict” by James A. Lewis: http://www.armscontrol.org/act/2010_06/Lewis.
7. The Parliament of Canada, Library of Parliament, Parliamentary Information and Research Service, “Cybersecurity and Intelligence: The U.S. Approach” by Holly Porteous, February 8, 2010: http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0926-e.htm; National Journal, “China’s Cyber-Militia” by Shane Harris, May 31, 2008: http://nationaljournal.com/member/nationalsecurity/china-s-cyber-militia-20080531; *The Register [UK],* "IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled" by Dan Goodin of San Francisco, January 14, 2010: http://www.theregister.co.uk/2010/01/14/cyber_assault_followup/ ; *The Washington Post*, "Google China cyberattack part of vast espionage campaign, experts say" by Ariana Eunjung Cha and Ellen Nakashima, January 13, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.
8. *The Register [UK]*, “Cyber attack could bring US military response” By Robert Lemos, May 13, 2009: http://www.theregister.co.uk/2009/05/13/us_cyber_attack_response/.
9. *PC World*, “Beware the Botnets” by Brian Krebs, January 24, 2010: http://www.pcworld.com/article/187532/beware_the_botnets.html.
10. *The Register [UK]*, “Botnets linked to political hacking in Russia” by John Leyden, December 14, 2007: http://www.theregister.co.uk/2007/12/14/botnet_hacktivism/.
11. *The New York Times,* “Thieves Winning Online War, Maybe Even in Your Computer” by John Markoff, December 5, 2008: http://www.nytimes.com/2008/12/06/technology/internet/06security.html.
12. UBM TechWeb’s Dark Reading website, “The Top 10 Enterprise Botnets” By Kelly Jackson Higgins, February 17, 2010: http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=222900762 .
13. See Table 9: Types of Cyberattacks, “Cybersecurity for Critical Infrastructure Protection” http://www.gao.gov/new.items/d04321.pdf.
14. Weblog, Information Security Resources, “Debunking Cyber Deterrence as a Strategy” by Richard Stiennon, October 31, 2009: http://information-security-resources.com/2009/10/31/debunking-cyber-deterrence-as-a-strategy/.
15. StopBadware, http://stopbadware.org/.
16. On March 2, 2010, during the Microsoft Corporation’s RSA Conference in San Francisco, Scott Charney (Corporate Vice President for Trustworthy Computing) presented a keynote address titled “Why don't we think about access providers who are doing inspection and quarantine, and cleaning machines prior to access to the Internet?” http://www.microsoft.com/presspass/exec/charney/2010/03-02rsa2010.mspx.
17. Security Focus, "BotHunter aims to find bots for free" by Robert Lemos, November 25, 2008: http://www.securityfocus.com/brief/861; *The New York Times*, “Thieves Winning Online War, Maybe Even in Your Computer” by John Markoff, December 6, 2008: http://www.nytimes.com/2008/12/06/technology/internet/06security.html; *PC World,* “Monitor Botnet Threats Your Antivirus Can't See” by Robert Vamosi, February 17, 2009: http://www.pcworld.com/businesscenter/article/159706/monitor_botnet_threats_your_antivirus_cant_see.html; http://www.bothunter.net/.
18. Damballa® stops breaches by botnets and advanced persistent threats that exploit networks for illegal activity. http://www.damballa.com/.
19. See the Government Information Security website. This article was adapted from testimony presented to the House Committee on Homeland Security on the current state of the U.S. Computer Emergency Readiness Team, “Einstein Presents Big Challenge to U.S.-CERT” by Richard L. Skinner (Inspector General of the Department of Homeland Security), June 22, 2010: http://www.govinfosecurity.com/articles.php?art_id=2677; United States Government Accountability Office, Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House Committee on Homeland Security, “Cyber Analysis and Warning,” July 31, 2008: http://www.gao.gov/new.items/d08588.pdf.
20. *Wall Street Journal*, “U.S. Plans Cyber Shield for Utilities, Companies” by Siobhan Gorman, July 8, 2010: http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

ENDNOTES

21. *The Washington Post*, "Mike McConnell on how to win the cyber-war we're losing" by Mike McConnell, February 25, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.
22. *Global Security Newswire* [The National Journal Group], "Nation's Nuclear Power Plants Prepare for Cyber Attacks" by Martin Matishak, August 27, 2010: http://gsn.nti.org/gsn/nw_20100827_1692.php.
23. *Technology Review*, published by the Massachusetts Institute of Technology, "Russia's Cyber Security Plans" by David Talbot, April 16, 2010: http://www.technologyreview.com/blog/editors/25050/
24. U.S. General Accounting Office, Technology Assessment, see Table 6: Threats to Critical Infrastructure Threat Description, "Cybersecurity for Critical Infrastructure Protection," May 2004: http://www.gao.gov/new.items/d04321.pdf.
25. RAND Corporation, Monograph Series prepared for the U.S. Air Force, Project Air Force, "Cyberdeterrence and Cyberwar" by Martin Libicki, pages 18-21 and 71-72, 2009: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
26. *The New York Times*, "Leaked Cables Offer Raw Look at U.S. Diplomacy" by Scott Shane and Andrew W. Lehren, November 28, 2010: http://www.nytimes.com/2010/11/29/world/29cables.html
27. *Christian Science Monitor*, "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?" by Mark Clayton, September 21, 2010: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.
28. *Wired*, "New Clues Point to Israel as Author of Blockbuster Worm, Or Not" by Kim Zetter, October 2010: http://www.wired.com/threatlevel/2010/10/stuxnet-deconstructed/.
29. *Bloomberg/BusinessWeek*, "Computer Worm May Be Targeting Iranian Nuclear Sites" by Arik Hesseldahl, September 24, 2010: http://www.businessweek.com/news/2010-09-24/computer-worm-may-be-targeting-iranian-nuclear-sites.html; *The Economist,* "A worm in the centrifuge," September 30, 2010: http://www.economist.com/node/17147818.
30. *Global Security Newswire,* "Iran Could Limit Uranium Enrichment, Ahmadinejad Says," September 27, 2010: http://gsn.nti.org/gsn/nw_20100927_5440.php.
31. *The New York Times,* "Bombings Hit Atomic Experts in Iran Streets" by William Yong and Robert F. Worth, November 29, 2010: http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html.
32. *The Washington Post*, "Stuxnet Worm Possibly Made to Cripple Iran Centrifuges" by Glenn Kessler, 16 November 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/15/AR2010111506768.html.

Devabhaktuni "Sri" Srikrishna was the founder and Chief Technology Officer of Tropos Networks, which builds metro-scale wireless broadband (Wi-Fi) systems based on cellular mesh technology and is deployed in several cities across the United States. Srikrishna is a member of the FAS Board of Directors.

His publications have spanned quantum computing, parallel computing, wireless data communications, and nuclear detection.

"Cyberattacks can be carried out by anyone with the know-how and interest, and in many cases the cost of attacking is disproportionately small compared to the potential damage that can be inflicted. Groups involved in planning and executing attacks range from nations to individuals."