CENTER for STRATEGIC LEADERSHIP CSL

Issue Paper

Center for Strategic Leadership, U.S. Army War College

Volume 2-12, July 2012

Cyber Ricochet: Risk Management and Cyberspace Operations

Benjamin Leitzel

Cyber attacks can do significant harm to a country's infrastructure and should never be carried out in a cavalier manner. Offensive cyber operations are difficult to conduct with precision to avoid unintended casualties and damage to unrelated systems. If you're trying to do precision strike in cyberspace with a very high degree of confidence, that takes enormous amounts of intelligence, planning, great care and very carefully crafted cyber tools that won't boomerang against you down the road.[1]

—Rear Admiral Samuel Cox, U.S. Cyber Command Director of Intelligence

Introduction

Recent media reports of the 'Duqu', 'Flame', and 'Stuxnet' malware highlight cyberspace operations capabilities as well as emphasize the vulnerabilities of computer networks and systems. Many computer security vulnerabilities go undetected for years and once discovered vendors can take months to correct the defects.[2] Even after vendors release 'patches' to correct the problem, most users fail to update their systems immediately and completely.[3] The result is a cyberspace environment plagued with undefended systems where seams and gaps are exposed to even the most novice cyber threat actor.

Senior leaders, responsible for approving cyberspace operations, should consider options utilizing intrusions into an adversary's networks and systems that leverage computer security vulnerabilities. Cyberspace operations have the potential of achieving objectives faster, risking fewer lives, and saving money. Although cyberspace operations can cause an array of effects, this paper will focus on reports that have shown that cyberspace experts can infiltrate networks and systems to conduct intelligence collection and sabotage.[4] Cyber tools provide capabilities to achieve objectives before, during, and after hostilities while maintaining a degree of anonymity. However, as noted above, most computers are vulnerable and care must be taken to prevent these tools from being used against friendly networks and systems.

In 2010, the U.S. Army War College conducted a cyberspace operations workshop to identify critical areas for inclusion in senior leader education. Group members noted that "countering cyber threats is inherently all about risk management, as a network will always have cyber vulnerabilities and will be faced with constant cyber threats."[5] The Department of Defense (DoD) defines risk management as "the process of identifying, assessing, and controlling

1. Richard Lardner, "Cyberattacks Need High-Level Approval," April 26, 2012, *Sci-Tech Today*, http://www.sci-tech-today.com/story.xhtml?story_id=12300DQH81Y9 (accessed July 10, 2012).
2. Sue Marquette Poremba, "Why Do Software Holes Take So Long to Fix?,"May 9, 2012, *Security News Daily*, http://www.securitynewsdaily.com/1833-software-patch-lag-time.html (accessed July 10, 2012).
3. Angela Moscaritolo, "Report: Nearly all computer users running insecure programs," December 03, 2008, *SC Magazine*, http://www.scmagazine.com/report-nearly-all-computer-users-running-insecure-programs/article/121850/ (accessed July 10, 2012).
4. Mark Clayton, "Stuxnet Cyberweapon Set To Stop Operating," June 23, 2012, *Christian Science Monitor*, http://www.csmonitor.com/USA/2012/0623/Stuxnet-cyberweapon-set-to-stop-operating (accessed July 10, 2012).
5. William Waddell, David Smith, James Shufelt, and Jeffrey Caton, *Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace* (Carlisle Barracks, PA, U.S. Army War College, March 2011), 15.

Colonel (retired) Leitzel is an Information Operations Senior Analyst within the Center for Strategic Leadership.

risks arising from operational factors and making decisions that balance risk cost with mission benefits."[6] Cyberspace operations can exploit vulnerabilities in adversary systems and networks to produce effects that can accomplish objectives with the promise of limited risk. However, these 'cyber bullets' are prone to ricochet and it is difficult to predict their spread which may propagate the uncontrolled use or reengineering by unfriendly actors. Therefore, leaders must consider the possibility of a 'cyber ricochet' striking friendly networks and systems that could not only adversely affect military capabilities and operations, but also place a nation's critical infrastructure and key resources at risk.

Vulnerabilities

Senior leaders must understand that computer networks and systems are vulnerable to attack, even if updated with the latest security fixes. When Richard Clarke was the Special Advisor to the President for Cybersecurity in 2003, he received updates on the activities of 'red teams' employed by the government to test government systems by hacking into them. He stated, "[e]very time the red team has attempted to hack into a sensitive government computer, the red team has succeeded. Not only has it gotten in, but it's gained total control of the networks involved, without the people who own or operate those networks in the government even knowing that it happened. Every single time."[7] In a 2008 interview, a National Security Agency representative confirmed that its red team "get[s] into most of the networks we target. That's because every network has some residual vulnerability."[8]

A computer security vulnerability is a weakness in the system or software that allows an attacker to gain unauthorized access into a network or system and subsequently compromise the integrity of that system. When a vendor discovers a vulnerability, it will attempt to create, test, and release a 'patch' or software update to eliminate the risk.[9] A zero day vulnerability refers to a software vulnerability that is unknown to the vendor at the time the software is released for use. This security vulnerability can then be exploited by hackers before the vendor becomes aware and hurries to fix it.[10]

Installing patches as soon as they are released is a primary method of protecting computer systems. Despite the routine release of patches, most users fail to perform timely updates on their systems. In a December 2010 survey, only 45% of the information technology leaders responded that they patched their corporate computer systems more than once per month.[11] Bradley Antis, vice president of technical strategy at M86 Security, stated that "the 15 software vulnerabilities that were most often exploited in the second half of 2010 could have been stopped dead in their tracks, all [of them] already…patched by their vendors."[12]

Even those few organizations that take immediate corrective actions can be at risk for an extended period of time. Vendors must first become aware of their 'zero day' vulnerabilities and only then can they start the lengthy process of creating and testing a patch. The 'Flame' malware reportedly existed on the Web for at least four years before it was detected.[13] Josh Shaul, chief technology officer of Application Security, Inc., and his team investigated the turnaround time on patching vulnerabilities. Over a five-year period, they found 60 Oracle vulnerabilities. On average, it took Oracle 17 months to develop and release a fix.[14]

Organizations might be tempted to isolate their networks from the internet to secure them from unauthorized intrusion. However, such physical barriers do not guarantee secure networks and systems. A recent example is the

6. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington DC, U.S. Joints Chiefs of Staff, November 8, 2010 [As Amended Through April 15, 2012]), 280.
7. "Vulnerability How Real is the Threat?," interview with Richard Clarke, April 24, 2003, *Frontline*, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/threat.html (accessed July 10, 2012).
8. Glenn Derene, "Inside NSA Red Team Secret Ops With Government's Top Hackers," June 30, 2008, *Popular Mechanics*, http://www.popularmechanics.com/technology/how-to/computer-security/4270420?nav=hpPrint')%3b (accessed July 10, 2012).
9. Kevin Coleman, Randy Favero, and Edward Maggio, Esq., *Cyber Commander's Handbook, The Weaponry & Strategies of Digital Conflict*, Version 3.0, 2012 Edition, 178-179.
10. Symantec Corporation, "What is a Zero-Day Vulnerability?," *PC Tools Security News*, http://www.pctools.com/security-news/zero-day-vulnerability/ (accessed July 10, 2012).
11. McAfee Incorporated, *Risk and Compliance Outlook 2011* (Santa Clara, CA: McAfee Incorporated, 2011), 8.
12. Sue Marquette Poremba, "Best Way to Avoid Virus Infection? Update Your Software," April 12, 2011, *SecurityNewsDaily*, http://www.securitynewsdaily.com/584-best-way-avoid-virus-infection-update-software.html (accessed July 10, 2012).
13. Misha Glenny, "A Weapon We Can't Control," *New York Times*, June 25, 2012.
14. Poremba, "Why Do Software Holes Take So Long to Fix?"

'Stuxnet' malware that specifically targeted the centrifuges at the Natanz uranium enrichment facility in Iran. Since the computers controlling the centrifuges were not connected to the internet, most analysts agree that it required the physical introduction of the malware into the plant.[15] While many nation-states have the capability exploit vulnerabilities in adversary systems, leaders must ensure that these tools are not used against their friendly networks and systems.

Capabilities

Over the past few years we have seen numerous reports of malware employed to take advantage of software vulnerabilities. Senior leaders should consider the benefits of employing cyber effects producing capabilities which have the potential to achieve objectives while risking fewer lives, saving money, and maintaining anonymity. Cyberspace operations "can be crafted and deployed at a tiny fraction of the cost of other forms of intervention. No aircraft carriers needed, no "boots on the ground" to be shot at or blown up by IEDs."[16]

The Atlantic Council published an issue brief on NATO's cyberspace capacity in which the authors stated "[c]yber capabilities may be able to provide military commanders the capability not only to limit the risk to their own forces but also to limit civilian casualties and damage to critical infrastructure. If cyber capabilities could disable Libyan air defenses from afar … then a military commander would be reckless to rule out cyber capabilities without even considering them."[17] Cyberspace intelligence collection and sabotage, using tools such as the 'Duqu,' 'Flame,' and 'Stuxnet' malware, are just of a few of the capabilities that can contribute to mission success and achieve strategic objectives.

The DoD uses the term 'computer network exploitation' for cyberspace intelligence collection and defines it as "a form of surveillance and reconnaissance conducted in cyberspace that involves the use of computer networks to gather data from target or adversary automated information systems or networks."[18] Using cyberspace for surveillance and reconnaissance provides many advantages. In many cases, it decreases the risk of detection while being faster and cheaper than traditional methods. Some experts posit a future where "[w]e no longer need physical agents in place if we can now rely on artificially intelligent agents to dredge up the deepest secrets." [19]

The 'Duqu' and 'Flame' malware are excellent examples of computer network exploitation. Both programs existed on the web for several years, taking advantage of computer security vulnerabilities. John Bumgarner, a former Army intelligence officer who now serves as Research Director for the U.S. Cyber Consequences Unit, stated that 'Flame' was a "giant vacuum cleaner – sucking up information from wireless sources, turning on computer microphones, stealing files."[20] According to Symantec, 'Duqu' was employed in another espionage program that "infiltrated specific computers within key companies that had programs related to Iran's nuclear program. It was far more highly targeted than 'Flame' and came later." [21]

Sabotage, leveraging cyberspace capabilities, is another option available to senior leaders. Much like special operations, cyberspace operations are conducted in all environments, but are particularly well suited for denied and politically sensitive environments. Special operations forces may be called upon to conduct sabotage in support of direct action activities which "entail short-duration strikes and other small-scale offensive actions in hostile, denied, or diplomatically sensitive environments to seize, destroy, capture, exploit, recover, or damage designated targets."[22] Cyberspace operations share many of the same traits.

---

15. Glenny, "A Weapon We Can't Control."
16. John Arquilla, "The Cool War: Technology has made conflict cheaper, safer and faster—and the world is better for it," *Tampa Tribune*, June 24, 2012.
17. Jason Healey and Leendert van Bochoven, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow* (Washington, DC: The Atlantic Council of the United States, February 2012), 7.
18. U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington DC, U.S. Joints Chiefs of Staff, August 11, 2011), III-21.
19. Arquilla, "The Cool War."
20. Clayton, "Stuxnet Cyberweapon Set To Stop Operating."
21. Ibid.
22. U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05 (Washington, DC, U.S. Joints Chiefs of Staff, August 11, 2011), II-5.

The popular media has classified the 'Stuxnet' malware as a cyberspace sabotage tool reported to have infected Iran's centrifuges, "commanding them to run at higher and higher speeds until they broke. All this went on while Iranian technicians tried fruitlessly to stop the attack."[23] The International Atomic Energy Agency (IAEA) reported that Stuxnet "appears to have destroyed more than 1,000 of Iran's 5,000 gas centrifuges."[24] Like special operations (and traditional military operations for that matter), the successful 'Stuxnet' cyberspace operation was dependent upon intelligence, provided by the malware such as 'Duqu' and 'Flame' malware, to identify relevant targets in the Natanz uranium enrichment facility.

Risks

Cyberspace operations offer options to accomplish objectives while reducing the potential of a direct military confrontation. However, senior leaders must weigh the risks associated with these operations. Malware can 'ricochet' and spread to unintended systems or adversaries can redirect the malware back against friendly systems. In addition, vendor patches can render malware programs ineffective. These risks must be weighed against the benefits of cyberspace operations. Army Field Manual 3-21.8, *The Infantry Platoon and Squad*, states "[g]iven the uncertainty associated with combat and the threat of enemy action, leaders must understand how to reduce risks associated with fire and movement in proximity to direct and indirect fires. As a general rule, the dispersion and ricochet areas present an immediate danger to Soldiers. Observers and protective measures are therefore required."[25] This warning is also applicable to cyberspace operations and the risk of 'ricochet'.

A nation's computer networks and systems could be vulnerable to the very malware that is employed against an adversary. Many critical infrastructure facilities use Siemens industrial control systems, similar to those sabotaged at the Natanz facility. RAND National Defense Research Institute reported that "any country's infrastructure controllers (e.g., control systems for electric power, gas, water, refineries, and many other types of infrastructure) could fall victim to such a targeted worm."[26] Former White House Cybersecurity Czar Howard Schmidt stated that "[t]argeted malware of all types can be reverse-engineered, so the original creator doesn't truly have full control over it. Every time there's new malware, thousands of researchers say, 'I can reverse-engineer it.' It gets a lot of exposure really quickly."[27]

A major cause of 'cyber ricochet' is the propensity for malware to spread unpredictably across the internet. There have been several reports of computer viruses that were programmed to infect computers around the world. In 2006, the Nyxem virus used email attachments to infect over 450,000 computers in more than 200 countries.[28] Although 'Stuxnet' was reported to target only isolated computers controlling centrifuges in the Natanz facility, it spread to over 130,000 computers around the globe.[29] Cybersecurity companies Kaspersky and Symantec also discovered 'Flame' on a few thousand computers in the Mideast and on several systems outside the region to include computers in Austria, Russia, and Hong Kong.[30]

Once the malware 'ricochets' to computers around the globe, adversaries can reengineer and direct it against other systems. Immediately after Iran admitted to being a victim of 'Stuxnet', it created a new Cyber Command of its own

23. Arquilla, "The Cool War."
24. R. Scott Kemp, "Cyberweapons: Bold steps in a digital darkness?," 7 June 2012, *Bulletin of the Atomic Scientists*, http://www.thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness (accessed July 10, 2012).
25. U.S. Department of the Army, *The Infantry Platoon and Squad*, Army Field Manual 3-21.8, (Washington, DC: Department of the Army, March 28, 2007) 2-9, 2-10.
26. Isaac R. Porche III, Jerry M. Sollinger, Shawn McKay, *A Cyberworm That Knows No Boundaries* (Santa Monica, CA: RAND National Defense Research Institute, 2011), 2.
27. Kelly Jackson Higgins, "Former White House Cybersecurity Czar Calls For Security Action," June 13, 2012, *Dark Reading*, http://www.darkreading.com/advanced-threats/167901091/security/news/240002026/former-white-house-cybersecurity-czar-calls-for-security-action.html (accessed July 10, 2012).
28. David Moore and Colleen Shannon, "The Nyxem Email Virus: Analysis and Inferences," November 18, 2008, *The Cooperative Association for Internet Data Analysis*, http://www.caida.org/research/security/blackworm/ (accessed July 10, 2012).
29. Clayton, "Stuxnet Cyberweapon Set To Stop Operating."
30. Mark Clayton, "Beyond Stuxnet: massively complex Flame malware ups ante for cyberwar," May 29, 2012, *Christian Science Monitor*, http://www.csmonitor.com/USA/2012/0529/Beyond-Stuxnet-massively-complex-Flame-malware-ups-ante-for-cyberwar (accessed July 10, 2012).

and threatened, "to fight our enemies in cyberspace and Internet warfare."[31] The expertise to reengineer malware is not always limited to the target of the malware but can be used by hackers, terrorists, and other nation-states. R. Scott Kemp, in the *Bulletin of the Atomic Scientists*, asserted that "[a] Stuxnet-like attack can now be replicated by merely competent programmers, instead of requiring innovative hacker elites."[32] Indeed, *Technology Review* reported that software code used in 'Stuxnet' was discovered in a botnet that has infected millions of PCs.[33] The impact is similar to a nation that fielded a stealth bomber that was invisible to all radar (including its own) and then after the first mission gave the aircraft and design to its adversaries.

Senior leaders should also consider the limits on malware reuse after vendors and computer security companies discover and create patches for the compromised vulnerabilities. As described above, most users fail to update their systems with the latest patches in a timely manner. However, once a nation-state discovers an intrusion on a critical system it will be more likely to implement corrective measures immediately. F-Secure Security Labs projected that it took over 10 man-years to develop 'Stuxnet.'[34] If true, this was a significant effort since Microsoft patched the compromised 'zero day' vulnerabilities in the Windows operating system shortly after they were reported. The analogy to the stealth bomber is once again fitting in that giving away the aircraft and design could provide adversaries with the tools to improve their radar systems and gain the capability to detect stealth aircraft.

Conclusion

Senior leaders will continue to be challenged with difficult decisions in today's complex global environment. Cyberspace operations can provide previously unrealized options to achieve objectives faster, risk fewer lives, and save money. However, leaders must consider the risk of a 'cyber ricochet' spreading to networks and systems around the world with likely impact on friendly systems.

When considering cyberspace operations for intelligence collection or sabotage, leaders need detailed information of the risks and benefits to make sound decisions. Before authorizing an intrusion into an adversary's network or system, a leader can identify and assess these critical factors by insisting on answers to the following questions:

- What is the cost and how long will it take for the cyberspace operation to accomplish objectives?
- What are the diplomatic ramifications if the identity of the source of the cyberspace operation is revealed?
- Are friendly systems vulnerable to the malware used against the adversary?
- What can be done to control the unintended spread of the malware?
- Will adversaries be able to reengineer the malware and use it against friendly systems?
- What can be done to protect friendly systems against reuse?

****

31. Kemp, "Cyberweapons: Bold steps in a digital darkness?"
32. Ibid.
33. Christopher Mims, "How Obama Was Dangerously Naive About STUXNET and Cyberwarfare," June 1,2012, *Technology Review*, http://www.technologyreview.com/view/428061/how-obama-was-dangerously-naive-about-stuxnet-and/ (accessed July 10, 2012).
34. F-Secure Security Labs Blog, "Stuxnet Redux: Questions and Answers," November 23, 2010, http://www.f-secure.com/weblog/archives/00002066.html (accessed July 10, 2012).