Volume 2, Issue 11, November 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Methodological and Operational deliberations in Cyber attack and Cyber exploitation

Keshav Dev Gupta
M.Tech (IT)
Asst. Professor of Computer Science
Jayoti Vidyapeeth Women's University
Vedant Gyan Velley, Jharna
Mahal-Jobner Link road, Jaipur, Rajasthan
India--303007

Jitendra Joshi
M.Tech (IT)
Asst. Professor of Computer Science
Jayoti Vidyapeeth Women's University
Vedant Gyan Velley, Jharna
Mahal-Jobner Link road, Jaipur, Rajasthan
India--303007

Abstract: When we think of technology, what often comes to mind are televisions, communications devices such as cell phones and satellites, computers, and different modes of transportation? Various operational deliberations associated with "weaponizing" the basic technology of cyber attack. This paper is relevant both to the attacker, who uses cyber attack as a tool of his own choosing, and to the defender, who must handle with and respond to incoming cyber attacks launched by an attacker. However, there are other ways in which technology is applied, one of those being the Internet and its various components including email, chat rooms, and search engines. The list of uses for the Internet is innumerable and many corporations and universities are forcing people to make use of it. But no matter how much this new technology is forced on us, people are still resistant to it.

Keywords: Cyber Attack, weapons, technology, network control, internet

I. Introduction

Cyberspace technology is emerging as an "instrument of power" in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies. [1]

For purposes of this paper, cyber attack refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy rival computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Several characteristics of weapons for cyber attack are worthy of note:

The follow-on effects of these weapons are almost more harmful than the direct effects of the attack. (Direct or instant effects are effects on the computer machine or network attacked. Indirect or follow-on effects are effects on the systems and/or devices that the attacked computer machine or network controls or interacts with, or on the people that use or rely on the attacked computer system or network.) That is, the network or computer attacked is much less relevant than the systems controlled by the targeted computer or network or the decision making that depends on the information contained in or processed by the targeted computer or network, and indeed the indirect effect is often the primary purpose of the attack. In addition, the scales of damage of a cyber attack can span and huge range.

The results of a cyber attack are generally unsure. Minute details of configuration can affect the result of a cyber attack, and cascading effects often cannot be reliably predicted. One consequence can be that collateral damage and damage material of a cyber attack may be very difficult to estimate.

The plan and executable process are very complex of cyber attack. They can engage a much larger range of options than most traditional military operations, and because they are primarily about an attack's secondary and tertiary effects, there are many more possible outcome paths whose analysis often requires highly specialized knowledge. The time scales on which cyber attacks operate can range from the tenths of second to years.

If we compare to traditional military operations than cyber attacks are relatively inexpensive. The underlying technology for carrying out cyber attacks is widely available, easy to obtain and inexpensive. An attacker can compromise computers belonging to otherwise uninvolved parties to take part in an attack activity; use automation to increase the amount of damage

that can be done per person attacking, increase the speed at which the damage is done, and decrease the required knowledge and skill level of the operator of the system; and even steal the financial assets of an adversary to use for its own ends. . Cyber attacks are thus also well suited for being instruments of catalytic conflict—instigating conflict between two other parties. On the other hand, some cyber attack weapons are usable only once or a few times.

Computers have improved a great deal from the time that they were invented to the present. They have even improved a great deal from year to year. This may be positive, but then again it has a negative effect on society. The use and advancement of technology has increased different types of crimes like the following; terrorism, black marketing, and theft crimes. It is also responsible for the success of their respective criminal assets.

Cyber exploitations are quite different from cyber attacks mainly in their objectives and in the legal constructs surrounding them. Yet, number of technology underlying cyber exploitation is similar to that of cyber attack, and the same is true for some of the operational considerations as well. A successful cyber attack requires vulnerability, access to that vulnerability, and a payload to be executed. Cyber exploitation requires the same three things—and the only difference is in the payload to be executed. That is, what technically distinguishes cyber exploitation from a cyber attack is the nature of the payload. These technical similarities often mean that a targeted party may not be able to distinguish easily between cyber exploitation and a cyber attack—a fact that may result in that party's making incorrect or misinformed decisions. On the other hand, the primary technical requirement of a cyber exploitation is that the delivery and execution of its payload must be accomplished quietly and undetectably—secrecy is often far less important when cyber attack is the mission.

II. Theoretical Consideration

If we compare to traditional military operations than cyber attacks are relatively inexpensive. The underlying technology for carrying out cyber attacks is widely available, easy to obtain and inexpensive. An attacker can compromise computers belonging to otherwise uninvolved parties to take part in an attack activity; use automation to increase the amount of damage that can be done per person attacking, increase the speed at which the damage is done, and decrease the required knowledge and skill level of the operator of the system; and even steal the financial assets of an adversary to use for its own ends. . Cyber attacks are thus also well suited for being instruments of catalytic conflict—instigating conflict between two other parties. On the other hand, some cyber attack weapons are usable only once or a few times.

Computers have improved a great deal from the time that they were invented to the present. They have even improved a great deal from year to year. This may be positive, but then again it has a negative effect on society. The use and advancement of technology has increased different types of crimes like the following; terrorism, black marketing, and theft crimes. It is also responsible for the success of their respective criminal assets.

Cyber exploitations are quite different from cyber attacks mainly in their objectives and in the legal constructs surrounding them. Yet, number of technology underlying cyber exploitation is similar to that of cyber attack, and the same is true for some of the operational considerations as well. A successful cyber attack requires vulnerability, access to that vulnerability, and a payload to be executed. Cyber exploitation requires the same three things—and the only difference is in the payload to be executed. That is, what technically distinguishes cyber exploitation from a cyber attack is the nature of the payload. These technical similarities often mean that a targeted party may not be able to distinguish easily between cyber exploitation and a cyber attack—a fact that may result in that party's making incorrect or misinformed decisions. On the other hand, the primary technical requirement of a cyber exploitation is that the delivery and execution of its payload must be accomplished quietly and undetectably—secrecy is often far less important when cyber attack is the mission.

III. Previous Case History

- In 1982, a computer control system stolen from a Canadian company by Soviet spies caused a Soviet gas pipeline to explode. The code for the control system had been modified by the CIA to include a logic bomb which changed the pump speeds to cause the explosion.[2]
- In 1991, it was reported by the US Air Force that a computer virus named AF/91 was created and was installed on a printer chip and made its way to Iraq via Amman, Jordan.[3] Its job was to make the Iraqi anti-aircraft guns malfunction; however, according to the story, the central command center was bombed and the virus was destroyed. [4] The virus, however, was found to be a fake.[5]
- he United States has been attacked from computers and computer networks situated in China and Russia. See Titan Rain and Moonlight Maze.[6]
- In the 2006 war against Hezbollah, Israel alleges that cyber-warfare was part of the conflict, where the Israel Defense Force (IDF) intelligence estimates several countries in the Middle East used Russian hackers and scientists to operate on their behalf. As a result, Israel attached growing importance to cyber-tactics, and became, along with the U.S., France and a couple of other nations, involved in cyber-war planning. Many international high-tech companies are now locating research and

development operations in Israel, where local hires are often veterans of the IDF's elite computer units.[7] Richard A. Clarke adds that "our Israeli friends have learned a thing or two from the programs we have been working on for more than two decades."[1]:

- In 2007, McAfee, Inc. alleged that China was actively involved in "cyber attack." China was accused of cyber-attacks on India, Germany, and the United States, although they denied knowledge of these attacks. China has the highest number of computers vulnerable to be controlled, owing at least partially to the large population.[8]
- In April 2007, Estonia came under cyber attack in the wake of relocation of the Bronze Soldier of Tallinn.[9] The largest part of the attacks were coming from Russia and from official servers of the authorities of Russia.[10] In the attack, ministries, banks, and media were targeted.[11][12]
- In September 2007, Israel carried out an airstrike on Syria dubbed Operation Orchard. U.S. industry and military sources speculated that the Israelis may have used technology similar to that used by the United States Suter airborne network attack system to allow their planes to pass undetected by radar into Syria.[13][14] Suter is a computer program designed to interfere with the computers of integrated air defense systems[15]
- In 2007, the United States government suffered an "an espionage Pearl Harbor" in which an "unknown foreign power...broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information."[16]
- In 2007 the website of the Kyrgyz Central Election Commission was defaced during its election. The message left on the website read "This site has been hacked by Dream of Estonian organization". During the election campaigns and riots preceding the election, there were cases of Denial-of-service attacks against the Kyrgyz ISPs.[17]
- Russian, South Ossetian, Georgian and Azerbaijani sites were attacked by hackers during the 2008 South Ossetia War.[18]
- In 2008, a hacking incident occurred on a U.S. military facility in the Middle East. United States Deputy Secretary of Defense William J. Lynn III had the Pentagon release a document, which reflected that a "malicious code" on a USB flash drive spread undetected on both classified and unclassified Pentagon systems, establishing a digital beachhead, from which data could be transferred to servers under foreign control. "It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary. This ... was the most significant breach of U.S. military computers ever and it served as an important wake-up call", Lynn wrote in an article for Foreign Affairs.[19]
- On March 28, 2009, a cyber spy network, dubbed GhostNet , using servers mainly based in China has tapped into classified documents from government and private organizations in 103 countries, including the computers of Tibetan exiles,[20][21] but China denies the claim.[22][23]
- In July 2009, there were a series of coordinated cyber attacks against major government, news media, and financial websites in South Korea and the United States.[24] While many thought the attack was directed by North Korea, one researcher traced the attacks to the United Kingdom.[25]
- In December 2009 through January 2010, a cyber attack, dubbed Operation Aurora, was launched from China against Google and over 20 other companies.[26] Google said the attacks originated from China and that it would "review the feasibility" of its business operations in China following the incident. According to Google, at least 20 other companies in various sectors had been targeted by the attacks. McAfee spokespersons claim that "this is the highest profile attack of its kind that we have seen in recent memory."[27]
- In May 2010, In response to Indian Cyber Army defacing Pakistani websites, 1000+ Indian websites were defaced by PakHaxors, TeaMp0isoN, UrduHack & ZCompany Hacking Crew, among those were the Indian CID website, local government of Kerala, Box Office of Indian, Brahmos missile website, Indian HP helpdesk, Indian Institute of Science, and The Indian Directorate General of Shipping.
- In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.[27]
- In October 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said Britain faces a "real and credible" threat from cyber attacks by hostile states and criminals and government systems are targeted 1,000 times each month, such attacks threatened Britain's economic future, and some countries were already using cyber assaults to put pressure on other nations.[29]
- On November 26 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge of the Mumbai terrorist attack which had confirmed the involvement of Pakistani terrorists.[30]
- On December 4 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry.[31]

IV. Conclusion

Although ongoing research on tracking and tracing cyber-attacks is promising, existing track and trace capabilities are primitive compared with the capabilities of attackers. Subtle attacks by sophisticated attackers can be extremely difficult to detect and virtually impossible to trace using current technology. However, improvements to current Internet technology, including improved protocols, cannot succeed without an in-depth understanding and inclusion of policy issues to specify what information can be collected, shared, or retained, and how cooperation across administrative, jurisdictional, and national boundaries is to be accomplished. Nor can policy alone, with only high-level agreements in principle, create an effective tracking and tracing infrastructure that would support multilateral technical cooperation in the face of attacks rapidly propagating across the global Internet.

References:

[1] "The Joint Operating Environment", Report released, Feb. 18, 2010, pp. 34-36
[2] "Cyberwar: War in the fifth domain". *The Economist*. 1 July 2010. http://www.economist.com/node/16478792?story_id=16478792&fsrc=rss. Retrieved 4 July 2010.
[3] Smith, George. "Iraqi Cyberwar: an Ageless Joke." SecurityFocus. 10 Mar. 2003. Web. 11 Oct. 2009. <http://www.securityfocus.com/columnists/147>.
[4] <http://www.securityfocus.com/columnists/147>.
[5] <http://www.securityfocus.com/columnists/147>.
[6] Jim Wolf,"U.S. Air Force prepares to fight in cyberspace", Reuters, November 3, 2006
[7] "Israel Adds Cyber-Attack to IDF", *Military.com*, Feb. 10, 2010
[8] "China has .75M zombie computers' in U.S.". http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/. Retrieved 2007-11-30.
[9] "War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?". *The Economist*. July 1, 2010. http://www.economist.com/node/16478792. Retrieved 2010-07-02. "Important thinking about the tactical and legal concepts of cyber-warfare is taking place in a former Soviet barracks in Estonia, now home to NATO's "centre of excellence" for cyber-defence. It was established in response to what has become known as "Web War 1", a concerted denial-of-service attack on Estonian government, media and bank web servers that was precipitated by the decision to move a Soviet-era war memorial in central Tallinn in 2007."
[10] Estonia accuses Russia of 'cyber attack'
[11] Ian Traynor, 'Russia accused of unleashing cyber war to disable Estonia", *The Guardian*, May 17, 2007
[12] BBC: Cyber-war a growing threat warn experts
[13] Fulghum, David A. "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week & Space Technology*, 2007-10-03. Retrieved on 2007-10-03.
[14] Fulghum, David A. "Israel used electronic attack in air strike against Syrian mystery target", *Aviation Week & Space Technology*, 2007-10-08. Retrieved on 2007-10-08.
[15] David A. Fulghum, Michael A. Dornheim, and William B. Scott. "Black Surprises". Aviation Week & Space Technology. http://www.aviationnow.com/avnow/noys/noys_story.jsp?id=news/02145p04.xml. Retrieved 2007-10-05.
[16] "Cyber War: Sabotaging the System". *CBS News*. November 6, 2009. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.
[17] Website of Kyrgyz Central Election Commission hacked by Estonian hackers, Regnum, 14 December 2007
[18] Danchev, Dancho (2008-08-11). "Coordinated Russia vs Georgia cyberattack". ZDnet. http://blogs.zdnet.com/security/?p=1670. Retrieved 2008-11-25.
[19] The Washington Post: Pentagon computers attacked with flash drive
[20] AP: Researchers: Cyber spies break into govt computers
[21] CTV News: Video clip
[22] Foreign Ministry Spokesperson Qin Gang's Remarks on the So-called Chinese Cyber-Spy Ring Invading Computers in Countries
[23] embassy scoffs at reports of cyber spying
[24] BBC News: New cyber attacks hit South Korea
[25] Williams, Martin. UK, Not North Korea, Source of DDOS Attacks, Researcher Says. PC World.
[26] "A new approach to China". Google Inc.. 2010-01-12. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html. Retrieved 17 January 2010.
[27] AFP: Stuxnet worm brings cyber warfare out of virtual world

[28] Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Sept/Oct. 2010, pp. 97-108
[29] The Globe and Mail: Britain faces serious cyber threat, spy agency head warns
[30] The Lipman Report, Oct. 15, 2010
[31] "Cyberwarrior Shortage Threatens U.S. Security" *NPR*, July 19, 2010

