Cyber Protests:
The Threat to the U.S. Information Infrastructure

October 2001

Executive Summary

Political events and emerging international situations will increasingly lead to cyber protests. The cyber protests that have occurred thus far have had little impact on U.S. infrastructure. As computing technology becomes faster and better, and hacking tools become more advanced and easier to use, cyber protesting and hacktivism will become more significant to U.S. national interests. Cyber protesters are becoming increasingly more organized and their techniques more sophisticated but, most likely, will continue to deface web sites and perform DoS attacks. There will also be an increase in the number of apparently unrelated hacking groups participating in the cyber protests. National boundaries will not always be clearly delineated in attacks on opposing organizations. International activity will also tend to spill over into the United States. Because the United States is a multicultural, world-leading nation it will suffer from attacks on culturally related sites and structures in the future.

Generally, the most popularly targeted sites are those belonging to government, educational, commercial, and cultural institutions. However, any site with an exploitable vulnerability will be susceptible to a cyber attack. The infrastructure has been targeted in other countries in cyber protests and it is expected that it will eventually be targeted in the United States as well. Cyber protesters certainly will target infrastructure more often and exploit opportunities to disrupt or damage it.

Web sites that remain open to known hacking tools will have a higher probability of suffering defacement. Network administrators must remain educated and defenses must evolve along with the threats and offensive capabilities. Although the cyber protests seen today have already caused limited damage, the potential for future attacks could bring about large economic losses as well as potentially severe damage to the national infrastructure, affecting global markets as well as public safety.

Introduction

In the last decade, with the explosion of the size of the Internet, protests and political activism have entered a new realm.[1] Political activism on the Internet has already generated a wide range of activity, from using e-mail and web sites to organize, to web page defacements and denial-of-service (DoS) attacks.[2] These politically motivated computer-based attacks are usually described as *hacktivism*, a marriage of hacking and political activism.

In addition to the consistent activity of groups devoted to a specific long-term cause, the Internet has also seen short-term periods of intense political activity, which can be referred to as *cyber protests*. Cyber protests have become a worldwide phenomenon available to anyone with access to computers. Unrestrained by geographic boundaries, protesters have an enormous forum in which to be heard.

Cyber protesters have a wide range of goals or objectives. Some hackers want to expose government corruption or fundamental violation of human rights; others just want to hack and cause mischief for fun. It has only been since 1998 that cyber protests have skyrocketed in popularity and become commonplace in today's computerized world.

The most common type of cyber protest comes in the form of web page defacements. In such scenarios, a web site is compromised through some security deficiency and the hacker is able to alter it, many times placing propaganda, profanity, or pornographic images on it. This can range from being a nuisance and embarrassment for an organization to a major economic loss for an e-commerce business.

Protests and civil disturbances are nothing new. People unhappy with their situations have always found outlets to spread their message, be it a peaceful sit-in, letter-writing campaign, picket march, or violent gang fight. Now, with the advent of the Internet and the growing number of people online, it has become easier to organize protests. That is not to say that every web defacement is an organized event on the part of some political organization. Many defacements are perpetrated by lone hackers that have no political motivation other than to create chaos. Nation-states and their respective citizens have also been involved in cyber protests. Several countries have waged ongoing cyber battles against each other through web defacements and DoS attacks. Mail bombing is a popular form of a DoS attack. Massive amounts of e-mail or web traffic are directed

[1] Historically, groups have never had the global platform that the Internet provides today. Bulletin boards and group subscriber lists were the only computerized links protestors had from the 1970s through the early 1990s. The introduction of web browsers supporting graphics and multimedia content and the expansive growth of the Internet, coupled with the growing number of home computers, gave organizations a new outlet for distributing information or disrupting events for a political cause. The fact that many organizations have a web site has enabled them to spread their beliefs to a wider audience. It has also enabled other groups to target them for attack.

[2] Freedom of speech is a fundamental right protected by the Constitution of the United States of America that should not be taken lightly. Individuals and groups generally have the right to actively and legally support those causes in which they believe. Many protesters and political activist groups have used cyberspace to organize and advance their memberships and activities. Using computers and the Internet has greatly increased protesters' effectiveness in spreading their message and achieving their goals. This paper deals with past incidents in which cyber protests have led to the destruction of property and other illegal activities, citing, specifically, foreign protests.

against a specific site, overloading it and causing it to crash. It should be noted, however, that some parties involved in these cyber protests are not citizens of the respective countries. They might hold similar views or they might be involved just to participate in hacking different sites. Alliances can be tenuous at best for some of these groups.

Chinese Hackers

One high profile incident occurred in May 1999 after the United States accidentally bombed the Chinese embassy in Belgrade, Yugoslavia during the NATO air campaign. U.S. web sites were defaced in the name of China and massive e-mail campaigns were executed to gain sympathy and support for the Chinese cause. Government web sites were primarily targeted. The U.S. Departments of Energy and the Interior, and the National Park Service all suffered web page defacements. In addition, the White House web site was taken down for three days after it was continually mail bombed. This action was relatively unorganized in fashion, short in length, and affected a small number of U.S. sites.

Pro-Chinese hackers also acted against Taiwan during the Taiwanese presidential elections in August and September 1999. Cyber protesters and hacktivists compromised 165 Taiwanese web sites, mainly defacing them, over the two-month period. Their ultimate goal, as it was stated, was to negatively affect and bring down Taiwan's infrastructure. Among the targeted sites were electricity, economic institutions, telecommunications, and air traffic control. Although teams began to develop and organize near the end of the operations, the damage was relatively light, similar to the attacks on U.S. sites earlier in the year. Importantly, strategic targeting and some organization of forces became accepted strategies for future protests and hacks. These hackers are likely to become more organized and more successful in future incidents.[3]

In late April and early May 2001 pro-Chinese hacktivists and cyber protesters began a cyber assault on U.S. web sites. This resulted from an incident in early April where a Chinese fighter jet was lost at sea after colliding with a U.S. naval reconnaissance airplane. It also coincided with the two-year anniversary of the Chinese embassy bombing by the United States in Belgrade and the traditionally celebrated May Day and Youth Day in China. Led by the Honkers Union of China (HUC), pro-Chinese hackers defaced or crashed over 100 seemingly random web sites, mainly .gov and .com, through DoS attacks and similar exploits.[4] Although some of the tools used were sophisticated, they were readily available to both sides on the Internet.

Many defacements of U.S. sites included posting pictures of the dead Chinese pilot Wang Wei and profane messages calling for the downfall of the United States. Pro-United States hackers responded with similar defacements, messages, and damage on 300

[3] "China–Taiwan Hacker Wars," *Jane's Information Group Limited 1999.* Volume 000/2565, 21 October 1999 [online]; available from http://www.infowar.com/hacker/99/hack_102199a_j.shtml; Internet.
[4] Rose Tang, "China–U.S. Cyber War Escalates," 01 May 2001 [online]; available from http://www.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers; Internet.

Chinese web sites. Of interest is that some pro-Chinese hackers violated hacker etiquette by wiping some compromised servers. [5] The rule of thumb is to deface or crash a web site but to leave the information intact, otherwise it is considered bad form. [6]

Israeli and Palestinian Hackers

In October 2000, Israeli and Palestinian hackers engaged in adversarial hacking when the prolonged peace talks between the two groups broke down. During this difficult time, hackers seized the opportunity to attack web sites belonging to the opposition. Starting October 6, 2000, 40 Israeli web sites and at least 15 Palestinian web sites suffered defacements at the hands of opposing hackers. [7] This coincided, of course, with physical violence in the region. It was also a problem for U.S. based web sites. U.S. web sites will often fall victim, regardless of their lack of proximity or involvement in the events. For example, several U.S. sites were hacked by pro-Palestinian hacktivists, including the take down of a lobbyist group web site. The hackers then posted group membership information and credit card numbers. [8] This activity did little to affect the United States as a whole although it illustrates how a seemingly unrelated event can potentially affect U.S. sites.

The level of sophistication ranged from low-level activity using simple defacements to coordinated, relatively sophisticated attacks such as potential root access penetrations. Several hacking tools were developed specifically for this engagement. Any type of attack was considered during this time, including the perpetration of viruses, DoS attacks with e-mail bombing, and sustained, amplified pinging attacks. Web sites containing these various hacking tools were readily available for download to anyone who wanted to join the action.

Pro-Palestinian hackers hit any type of Israeli sites that they were able to compromise, many times defacing them with messages such as, "Free Palestine" or "Free Kashmir." [9] FloodNet software was a major tool used by the Israelis. The cyber protesters simply visited a site and FloodNet would repeatedly send requests to the targeted server. This type of virtual sit-in is a popular form of a DoS attack. Many of these attacks were successful as servers were bombarded and went down repeatedly. Targets included ethnic specific organizational web sites and those of financial institutions to disrupt the infra-

[5] "Chinese Hackers Concede Defeat in U.S. Hacker War, Call Cease-fire," *Agence France Presse*, 10 May 2001.

[6] This highlights the fact that although web defacements usually cause minimal damage, they indicate a very serious breach in security. A web defacement is, by definition, the manipulation of a web server's data by gaining unauthorized access to that server. It must be determined if the hacker installed a back door, introduced malicious code, or affected the server in any other way. A seemingly low-level hack could result in future problems if systems administrators do not take positive actions to stop future intrusions and restore the server to its previous condition.

[7] Larisa Paul, "When Cyber Hacktivism Meets Cyberterrorism," *Sans Institute*, 19 February 2001 [online]; available from http://www.sans.org/infosecFAQ/hackers/terrorism.htm; Internet.

[8] "Hacktivists Take Conflict to Internet," *Associated Press*, 4 November 2000.

[9] "Hacktivists Take Conflict to Internet," *Associated Press*, 4 November 2000.

structure. E-commerce sites crashed and there was an economic impact reflected in the Israeli markets. It was, however, the root access attempts that were most dangerous for the defenders. Hackers who can gain root access to sites give them unlimited freedom to do whatever they wish. This is the highest level of penetration possible although no successful root access penetrations were reported.

These events attracted a wide variety of hackers eager to join the fight. Both sides were well-organized and used reconnaissance and intelligence gathering techniques to maximize their effectiveness. Even outside hacking groups, such as G-Force Pakistan, joined forces with the Palestinians to lend a helping hand. This is increasingly common. Some outside groups join an effort because they have similar political or ethnic motivations, however, this is not always the case. Some groups participate in hacks simply for the desire to hack or the publicity, not out of a sense of loyalty.

Overall it can be expected that Israeli and Palestinian hackers will be active whenever a stumbling block appears in the road to possible peace between the groups. On the other hand, increased hacking might also occur when the Israelis and Palestinians are close to a peace agreement. System administrators must remain vigilant and focused on providing effective network security.

Indian and Pakistani Hackers

Another example is India and Pakistan engaging in a cyber protest caused by national and ethnic differences. After a cease-fire in the Kashmir Valley hackers took it upon themselves to continue the hostilities. In 2000, pro-Pakistani hackers defaced more than 500 Indian web sites. Conversely, only one known Pakistani site was hacked by the Indians. This illustrates a large difference in technical, hacking abilities or the willingness to use the skills to strike at an adversary. In this event the apparent level of sophistication on both sides is relatively low. Web site defacements are the leading form of this protest. The group G-Force Pakistan was the most active group claiming involvement in the events.[10]

Japanese Incidents

Recently, Japan has been targeted twice in online protests. During the first week of April 2001, pro-Korean hackers attacked Japanese organizations responsible for the approval of a new history textbook. The textbook glossed over atrocities committed by Japan during World War II and the occupation of China and South Korea. The perceived reluctance of Japan to accept responsibility for its actions triggered these events. The main participants in this incident were Korean university students, who used e-mail bombs in a DoS attack. The students crashed several web sites, including Japan's Educa-

[10] Kaajal Wallia, "Indians, Pakistanis Play Patriotic Games on Net," *The Times of India*, 06 January 2001.

tion Ministry, Liberal Democratic Party and the publishing company responsible for the textbook.[11] These attacks were neither long lasting nor were they largely organized.

In early August 2001, pro-Chinese hackers targeted Japanese web sites after Japan's Prime Minister visited a controversial war memorial, the Yasukuni Shrine. In a brief period of time, hackers defaced several web sites belonging mainly to Japanese companies and research institutes.[12] This indicates the continuing willingness of pro-Chinese hackers to use cyberspace and hacking tools as a platform for protests and cyber civil disobedience, as well as for displaying a strong sense of patriotic nationalism.

Conclusions

While the cyber damage thus far has been minimal, the infrastructure will certainly be a target of cyber protestors and hacktivists in the future, with the potential goal being intentional destruction rather than public embarrassment or purely political statements. Pro-active network defense and security management are imperative to the prevention of more serious damage to infrastructure assets. International cooperation and private–public cooperation within the United States is necessary to ensure the ongoing function of the critical infrastructure.

[11] Stuart McMillan, "Cyber Attackers Remind Japan of its Infamous Past," *The National Business Review, 2001*. 04 April 2001 [online]; available from http://www.infowar.com/hacker/01/hack_040501a_j.shtml; Internet.
[12] "Chinese Hackers Attack Japanese Web sites over Shrine Visit," *Agence France Presse*, 14 August 2001.