Cyberwarriors

Activists and Terrorists Turn to Cyberspace

DOROTHY DENNING

Harvard International Review, Vol. XXIII, No. 2, Summer 2001, pp. 70-75.

As Palestinian rioters clashed with Israeli forces in the fall of 2000, Arab and Israeli hackers took to cyberspace to participate in the action. According to the Middle East Intelligence Bulletin, the cyberwar began in October, shortly after the Lebanese Shi'ite Hezbollah movement abducted three Israeli soldiers. Pro-Israeli hackers responded by crippling the guerrilla movement's website, which had been displaying videos of Palestinians killed in recent clashes and which had called on Palestinians to kill as many Israelis as possible. Pro-Palestinian hackers retaliated, shutting down the main Israeli government website and the Israeli Foreign Ministry website. From there the cyberwar escalated. An Israeli hacker planted the Star of David and some Hebrew text on one of Hezbollah's mirror sites, while pro-Palestinian hackers attacked additional Israeli sites, including those of the Bank of Israel and the Tel Aviv Stock Exchange. Hackers from as far away as North and South America joined the fray, sabotaging over 100 websites and disrupting Internet service in the Middle East and elsewhere.

The Palestinian-Israeli cyberwar illustrates a growing trend. Cyberspace is increasingly used as a digital battleground for rebels, freedom fighters, terrorists, and others who employ hacking tools to protest and participate in broader conflicts. The term "hacktivism," a fusion of hacking with activism, is often used to describe this activity. A related term, "cyberterrorism," refers to activity of a terrorist nature. However, whereas hacktivism is real and widespread, cyberterrorism exists only in theory. Terrorist groups are using the Internet, but they still prefer bombs to bytes as a means of inciting terror.

Hacktivists see cyberspace as a means for non-state actors to enter arenas of conflict, and to do so across international borders. They believe that nation-states are not the only actors with the authority to engage in war and aggression. And unlike nation-states, hacker warriors are not constrained by the “law of war” or the Charter of the United Nations. They often initiate the use of aggression and needlessly attack civilian systems.

Hacktivism is a relatively recent phenomenon. One early incident took place in October 1989, when anti-nuclear hackers released a computer worm into the US National Aeronautics and Space Administration (NASA) SPAN network. The worm carried the message, “Worms Against Nuclear Killers.…Your System Has Been Officically [sic] WANKed.…You talk of times of peace for all, and then prepare for war.” At the time of the attack, anti-nuclear protesters were trying (unsuccessfully) to stop the launch of the shuttle that carried the plutonium-fueled Galileo probe on its initial leg to Jupiter. The source of the attack was never identified, but some evidence suggested that it might have come from hackers in Australia.

In recent years, hacktivism has become a common occurrence worldwide. It accounts for a substantial fraction of all cyberspace attacks, which are also motivated by fun, curiosity, profit, and personal revenge. Hacktivism is likely to become even more popular as the Internet continues to grow and spread throughout the world. It is easy to carry out and offers many advantages over physical forms of protest and attack.

The Attraction to Hacktivism

For activists, hacktivism has several attractive features, not the least of which is global visibility. By altering the content on popular websites, hacktivists can spread their messages and names to large audiences. Even after the sites are restored, mirrors of the hacked pages are archived on sites such as Attrition.org, where they can be viewed by anyone at any time and from anywhere. Also, the news media are fascinated by cyberattacks and are quick to report them. Once the news stories hit the Internet, they spread quickly around the globe, drawing attention to the hackers as well as to the broader conflict.

Activists are also attracted to the low costs of hacktivism. There are few expenses beyond those of a computer and an Internet connection. Hacking tools can be downloaded for free from numerous websites all over the world. It costs nothing to use them and many require little or no expertise.

Moreover, hacktivism has the benefit of being unconstrained by geography and distance. Unlike street protesters, hackers do not have to be physically present to fight a digital war. In a "sit-in" on the website of the Mexican Embassy in the United Kingdom, the Electronic Disturbance Theater (EDT) gathered over 18,000 participants from 46 countries. Hacktivists could join the battle simply by visiting the EDT's website.

Hacktivism is thus well-suited to "swarming," a strategy in which hackers attack a given target from many directions at once. Because the Internet is global, it is relatively easy to assemble a large group of digital warriors in a coordinated attack. The United Kingdom-based Electrohippies Collective estimated that 452,000 people participated in their sit-in on the website of the World Trade Organization (WTO). The cyberattack was conducted in conjunction with street protests during WTO's Seattle meetings in late 1999.

Another attraction of hacktivism is the ability to operate anonymously on the Internet. Cyberwarriors can participate in attacks with little risk of being identified, let alone prosecuted. Further, participating in a cyberbattle is not life-threatening or even dangerous: hacktivists cannot be gunned down in cyberspace.

Many hacktivists, however, reject anonymity. They prefer that their actions be open and attributable. EDT and Electrohippies espouse this philosophy. Their events are announced in advance and the main players use their real names.

Web Defacement and Hijacking

Web defacement is perhaps the most common form of attack. Attrition.org, which collects mirrors and statistics of hacked websites, recorded over 5,000 defacements in the year 2000 alone, up from about 3,700 in 1999. Although the majority of these may have been motivated more by thrills and bragging rights than by some higher cause, many were also casualties of a digital battle.

Web hacks were common during the Kosovo conflict in 1999. The US hacking group called Team Spl0it broke into government sites and posted statements such as, “Tell your governments to stop the war.” The Kosovo Hackers Group, a coalition of European and Albanian hackers, replaced at least five sites with black and red “Free Kosovo” banners.

In the wake of the accidental bombing of China’s Belgrade embassy by the North Atlantic Treaty Organization (NATO), angry Chinese citizens allegedly hacked several US government sites. The slogan “Down with Barbarians” was placed in Chinese on the web page of the US Embassy in Beijing, while the US Department of Interior website showed images of the three journalists killed during the bombing and crowds protesting the attack in Beijing. The US Department of Energy’s home page read:

“Protest USA’s Nazi action!…We are Chinese hackers who take no cares about politics. But we can not stand by seeing our Chinese reporters been killed which you might have know

[sic]….NATO led by USA must take absolute responsibility.…We won’t stop attacking until the war stops!”

Web defacements were also popular in a cyberwar that erupted between hackers in China and Taiwan in August 1999. Chinese hackers defaced several Taiwanese and government websites with pro-China messages saying Taiwan was and always would be an inseparable part of China. “Only one China exists and only one China is needed,” read a message posted on the website of Taiwan’s highest watchdog agency. Taiwanese hackers retaliated and planted a red and blue Taiwanese national flag and an anti-Communist slogan, “Reconquer, Reconquer, Reconquer the Mainland,” on a Chinese high-tech Internet site. The cyberwar followed an angry exchange between China and Taiwan in response to Taiwanese President Lee Teng-hui’s statement that China must deal with Taiwan on a “state-to-state” basis.

Many of the attacks during the Palestinian-Israeli cyberwar were web defacements. The hacking group GForce Pakistan, which joined the pro-Palestinian forces, posted heart-wrenching images of badly mutilated children on numerous Israeli websites. The Borah Torah site also contained the message, “Jews, Israelis, you have crossed your limits, is that what Torah teaches? To kill small innocent children in that manner? You Jews must die!” along with a warning of additional attacks.

Hacktivists have also hijacked websites by tampering with the Domain Name Service so that the site’s domain name resolves to the IP address of some other site. When users point their browsers to the target site, they are redirected to the alternative site.

In what might have been one of the largest mass website takeovers, the anti-nuclear Milw0rm hackers joined with the Ashtray Lumberjacks hackers in an attack that affected more than 300 websites in July 1998. According to reports, the hackers broke into the British Internet service provider (ISP) EasySpace, which hosted the sites. They altered the ISP's database so that users attempting to access the sites were redirected to a Milw0rm site, where they were greeted by a message protesting the nuclear arms race. The message concluded with "Use your power to keep the world in a state of PEACE and put a stop to this nuclear bullshit."

Web Sit-ins

Web sit-ins are another popular form of attack. Thousands of Internet users simultaneously visit a target website and attempt to generate sufficient traffic to disrupt normal service. A group calling itself Strano Network conducted what was probably the first such demonstration as a protest against the French government's policies on nuclear and social issues. On December 21, 1995, they launched a one-hour Net'Strike attack against the websites operated by various government agencies. At the appointed hour, participants from all over the world pointed their browsers to the government websites. According to reports, at least some of the sites were effectively knocked out for the period.

In 1998, EDT took the concept a step further and automated the attacks. They organized a series of sit-ins, first against Mexican President Ernesto Zedillo's website and later against US President Bill Clinton's White House website, the Pentagon, the US Army School of the Americas, the Frankfurt Stock Exchange, and the Mexican Stock Exchange. The purpose was to demonstrate solidarity with the Mexican Zapatistas. According to EDT's Brett Stalbaum, the Pentagon was chosen because "we believe that the US military trained the soldiers carrying out the human rights abuses." For a similar reason, the US Army School of the Americas was selected. The Frankfurt Stock Exchange was targeted, Stalbaum said, "Because it represented capitalism's role in globalization utilizing the techniques of genocide and ethnic cleansing, which is at the root of the Chiapas' problems. The people of Chiapas should play a key role in determining their own fate, instead of having it pushed on them through their forced relocation.…which is currently financed by Western capital."

To facilitate the strikes, the organizers set up special websites with automated software. All that was required of would-be participants was to visit one of the FloodNet sites. When they did, their browser would download the software (a Java Applet), which would access the target site every few seconds. In addition, the software let protesters leave a personal statement on the targeted server's error log. For example, if they pointed their browsers to a non-existent file such as "human_rights" on the target server, the server would log the message, "human_rights not found on this server."

When the Pentagon's server sensed the attack from the FloodNet servers, it launched a counter-offensive against the users' browsers, redirecting them to a page with an Applet program called "HostileApplet." Once there, the new applet was downloaded to their browsers, where it endlessly tied up their machines trying to reload a document until the machines were rebooted. The Frankfurt Stock Exchange reported that they were aware of the protest but believed it had not affected their services. Overall, EDT considered the attacks a success. "Our interest is to help the people of Chiapas to keep receiving the international recognition that they need to keep them alive," said Stalbaum.

Since the time of the strikes, FloodNet and similar software have been used in numerous sit-ins sponsored by EDT, the Electrohippies, and others. There were reports of FloodNet activity during the Palestinian-Israeli cyberwar. Pro-Israel hackers created a website called Wizel.com, which offered FloodNet software and other tools before it was shut down. Pro-Arab hackers put up similar sites.

The Electrohippies have been criticized for denying their targets' right to speech when conducting a sit-in. Their response has been that a sit-in is acceptable if it substitutes the deficit of speech by one group with a broad debate on policy issues and if the event used to justify the sit-in provides a focus for the debate. The Electrohippies also demand broad support for their actions. An operation protesting genetically modified foods was aborted when the majority of visitors to their site did not vote for the operation.

Denial-of-Service Attacks

Whereas a web sit-in requires participation by tens of thousands of people to have even a slight impact, the so-called denial-of-service (DoS) and distributed denial-of-service (DDoS) tools allow lone cyberwarriors to shut down websites and e-mail servers. With a DoS attack, a hacker uses a software tool that bombards a server with network messages. The messages either crash the server or disrupt service so badly that legitimate traffic slows to a crawl. DDoS is similar except that the hacker first penetrates numerous Internet servers (called "zombies") and installs software on them to conduct the attack. The hacker then uses a tool that directs the zombies to attack the target all at once.

During the Kosovo conflict, Belgrade hackers were credited with DoS attacks against NATO servers. They bombarded NATO's web server with "ping" commands, which test whether a server is running and connected to the Internet. The attacks caused line saturation of the targeted servers.

Similar attacks took place during the Palestinian-Israeli cyberwar. Pro-Palestinian hackers used DoS tools to attack Netvision, Israel's largest ISP. While initial attacks crippled the ISP, Netvision succeeded in fending off later assaults by strengthening its security.

Automated e-mail bombings represent another way of disrupting service. In what some US intelligence authorities characterize as the first known attack by terrorists against a country's computer systems, ethnic Tamil guerrillas swamped Sri Lankan embassies with thousands of e-mail messages. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications." An offshoot of the Liberation Tigers of Tamil Eelam, which had been fighting for an independent homeland for minority Tamils, was credited with the 1998 incident.

The e-mail bombing consisted of about 800 e-mails a day for about two weeks. William Church, managing director of the Centre for Infrastructural Warfare Studies (CIWARS), observed that "the Liberation Tigers of Tamil are desperate for publicity and they got exactly what they wanted.… Considering the routinely deadly attacks committed by the Tigers, if this type of activity distracts them from bombing and killing, then CIWARS would like to encourage them, in the name of peace, to do more of this type of 'terrorist' activity."

Future Prospects

As the Internet continues to grow, its popularity as a digital battleground for hacker warriors is likely to increase. There will be more targets to attack and more people to attack them. Many regions of conflict in the world have only recently joined the Internet. When they have, the conflict has followed them on-line. It seems likely that every major conflict in the physical world will have a parallel operation in cyberspace. Further, there may be cyberspace battles with no corresponding physical operations.

Cyberdefenses will improve, but they are unlikely to fend off all attacks. New vulnerabilities are continually uncovered at a faster rate than ever before. Security lags behind.

Cyberwarriors, therefore, will have little difficulty finding weak systems to attack. Hacking tools will become more powerful and easier to use.

Although hacktivism is certain to be a part of the picture, it is harder to predict the extent to which terrorists might engage in attacks with potentially lethal or catastrophic consequences. While many hackers have the knowledge, skills, and tools to attack computer systems, they generally lack the motivation to cause violence or severe economic or social harm. Conversely, terrorists who are motivated to cause violence seem to lack the capability or motivation to cause that degree of damage in cyberspace.

In August 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, issued a report entitled “Cyberterror: Prospects and Implications.” Their objective was to articulate the demand side of terrorism. Specifically, they assessed the prospects of terrorist organizations pursuing cyberterrorism. They concluded that the barrier to entry for anything beyond annoying hacks is quite high and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Cyberterrorism, they argued, was a thing of the future, although it might be pursued as an ancillary tool.

The Monterey team defined three levels of cyberterror capability. The first level is simple-unstructured: the capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

The second is advanced-structured: the capability to conduct more sophisticated attacks against multiple systems or networks, and possibly to modify or create basic hacking tools. The organization possesses elementary target analysis, command and control, and learning capabilities.

The third is complex-coordinated: the capability to coordinate attacks capable of causing mass disruption against integrated, heterogeneous defenses (including cryptography). The organization has the ability to create sophisticated hacking tools. They possess a highly capable target analysis, command and control, and organizational learning capability.

The Monterey team estimated that it would take a group starting from scratch two to four years to reach the advanced-structured level and six to ten years to reach the complex-coordinated level, although some groups may get there in just a few years or turn to outsourcing or sponsorship to extend their capability more rapidly.

The study examined five types of terrorist groups: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremist. The authors determined that only the religious groups are likely to seek the most damaging capability level, as it is consistent with their indiscriminate application of violence. New Age or single-issue terrorists, such as the Animal Liberation Front, pose the most immediate threat. However, such groups are likely to accept disruption as a substitute for destruction. Both the revolutionary and ethno-nationalist separatists are likely to seek an advanced-structured capability. The far-right extremists are likely to settle for a simple-unstructured capability, as cyberterror offers neither the intimacy nor the cathartic effects that are central to the psychology of far-right terror. The study also determined that hacker groups are psychologically and organizationally ill-suited to cyberterror-ism, and that it would be against their interests to cause mass disruption of the information infrastructure.

For a terrorist, digital battles have other drawbacks. Systems are complex, so controlling an attack and achieving a desired level of damage may be harder than using physical weapons.

Unless people are injured, there is also less drama and emotional appeal. Further, terrorists may be less inclined to try new methods unless they see their old ones as inadequate, particularly when the new methods require considerable knowledge and skill to use effectively. Terrorists generally stick with tried and true methods. Novelty and sophistication of attack may be much less important than the assurance that a mission will be operationally successful. Indeed, the risk of operational failure could be a deterrent to terrorists. For now, the truck bomb poses a much greater threat than the logic bomb.

The next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyberterrorism than do the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists, the Timothy McVeighs of cyberspace. Some might be moved to action by cyberpolicy issues, making cyberspace an attractive venue for carrying out an attack. Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled, with a greater number of physical devices attached to the Internet. Some of these may be remotely controlled. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a website is today.

Although cyberterrorism is likely to be at least a few years into the future, hacktivism is here today and likely to stay. Cyberspace is now much more than a place for electronic commerce and communication. It has become a digital battleground for hacker warriors.