ENCURVE, LLC - *BUILDING INTENTIONAL SECURITY™*

Intentional - Purposeful. Deliberate. Planned.
That's what security should be.

ENCURVE

Hacktivism and Politically Motivated Computer Crime

Author: Kent Anderson, CISM
Managing Director
kea@EncurveLLC.com

Presented by:

ENCURVE, LLC
Building Intentional Security™

www.EncurveLLC.com

For more information on Hacktivism and Politically Motivated Computer Crime visit:
http://politicalhacking.blogspot.com

Abstract

The Internet has created a social revolution in which business, non-profit organizations, academia and governments have undergone a transformation in their ability to gather, share and process information. The result is an unprecedented reliance on information infrastructures. This dependency creates new opportunities for disruption.

Many politically motivated individuals and groups see the Internet as a medium to further their causes and disseminate their messages. While much of this activity is protected in Western countries as free speech, there is increasing misuse of technology as a mechanism to change or disrupt existing political, commercial and other social structures. Politically motivated computer crime covers a wide range of online activity to promote the objectives of individuals, groups or nations: Espionage Anti-globalization, trans-national conflicts, anarchists, labor disputes, environmental and animal rights.

This paper discusses the increase in politically motivated computer crime – both online protest (Hacktivism) and nationalist-based attacks. The history of the problem, types of attacks and motivations are reviewed. Two case studies investigated by the author are presented detailing the attacks and their impacts on the intended victims.

In October and November of 2000, the world media was focused on the confusion of the U.S. election and the deteriorating crisis between Israel and the Palestinian Authority. For the most part, the news media ignored another important aspect of the Israeli-Palestinian conflict – for the first time, the clash spilled into the online world of the Internet.

At the onset, these incidents were limited to defacement of websites and denial of service attacks against pro-Palestinian (e.g. Hezbollah) and Israeli government targets. Several Israeli Ministry sites and the Tel Aviv Stock Exchange were disrupted. Hezbollah's Al-Manar television station's website and other Palestinian news and information sites were also targeted.

Over the course of several weeks, the activity escalated in both scope and the type of attacks originating from both sides. One key development was the expansion of attacks to include both Internet Service Providers (ISPs) in the region and sites in the United States, Jordan, Iran and elsewhere that were not directly linked to the conflict.

On October 31, 2000, an Islamic-based activist organization known as UNITY announced a "cyber war" campaign against Israeli interests. This was followed the next day by an attack on the website of the American Israel Public Affairs Committee (AIPAC), a pro-Israeli lobby organization. The pro-Palestinian attackers not only defaced the website but broke into two databases on AIPAC's system and downloaded 700 credit card numbers and 3,500 email addresses.

Based on further UNITY calls for attacks and boycotts against American companies, US based ISPs and major corporations became targets. UNITY announced on November 4 an attack on companies such as Lucent Technologies.

The situation became so severe that political leader in both Israeli and Saudi Arabia intervened publicly. On November 3, the *Jerusalem Post* reported that Mr. Michael Eitan, head of the Knesset's Internet Committee, "expressed concern about the security of Israel's computer systems and called on the international community to take action against hackers" and, on November 9, the *Saudi Gazette* reported that Fahad al-Hewmani, director-general of the Internet Unit at King Abdulaziz City for Science and

Technology (the authority responsible for controlling Internet use within the Kingdom), issued a call to Saudi hackers asking them stop attacking Israeli and Jewish websites.

These attacks demonstrated not only the viability of online attacks to support the political agendas of the antagonists, they showed that in the virtual world of the Internet that third parties thousands of miles away from the conflict and not directly involved could become protagonists or victims of the online skirmishes. While no evidence was found of foreign powers becoming drawn in, the anonymity of the Internet certainly creates the opportunity for countries or other organizations to insert their agenda into the situation with minimal chance of detection.

It also demonstrated that the target of politically motivated computer crime is not limited to government networks: *Commercial interests are equally attractive targets*.

This activity was not an isolated event and continues to this day.

Corporations around the world are not adequately addressing basic IT security required to counter even simple threats such as viruses or "hacking" techniques carried out by amateur teenagers. The lack of basic protection borders on negligence. Moreover, most corporate executives are not aware of the threat posed to their organizations by individuals and groups with political agendas.

Here are a few questions that executives should consider:

- Is your organization a potential target of online protest? How do you determine if you are a target?
- What would you do if online protesters disrupted your website for a day? For a week?
- What would you do if protesters attacked your customers or investors?
- How would you react to negative media reports?
- What if there was no disruption, but the attackers made press statements to the contrary?
- How should you protect your network? Do you understand the threats and impacts in order to balance costs and risks?
- Who would you contact? Law enforcement? What if the attacks originate from several foreign countries?

What is Politically Motivated Computer Crime?

Broadly speaking, politically motivated computer crime falls into two (sometimes overlapping) categories: Support for *nationalist causes* and *online protest* also referred to as "*hacktivism*" or *electronic civil disobedience* (ECD).

The example presented above is one of support for nationalist causes. There are numerous examples including online attacks related to conflicts between China and Taiwan, South Korea and Japan and Middle Eastern countries and the United States to name a few.

The line between nationalist causes and espionage or "information warfare" is often blurred. The methods may be similar but determining motivation solely from attack analysis is difficult and often misguided. Recent incidents involving US government and defence contractors (code named "Titan Rain" and "Moonlight Maze") are commonly believed to have originated in China and Russia.

The growth in these types of attacks is driven by several factors. First, is the increase in connectivity around the world. For example, recent initiatives to expand broadband connectivity in South Korea have seen significant increases in a variety of cyber attacks originating from that country. Similar trends have been noted in Latin America and the Middle East.

Secondly, technology enables disenfranchised people to voice their opinions and frustrations more directly and, when motivated, to take action. These two factors can be seen in statistics related to the source of Internet based attacks. A recent *Symantec Internet Security Threat Report* reported a 334% increase in attacks originating from the United Arab Emirates, a 250% increase from Jordan, and a 188% increase from Cuba.

The Internet is often seen as an enabler of asymmetric conflict in which small, poorly funded groups can have significant influence and impact on large organizations and governments.

The second form of politically motivated computer crime is to support a myriad of anarchist, activist or protest movements. This activity is often called online protest or "hacktivism" – a combination of "hacking" and "activism". Another common name is Electronic Civil Disobedience (ECD). The motivations are varied and include protests related to anti-globalization, animal rights, labor movements, biotech and genetically modified foods, anti-war movements and environmental causes. These attacks are often combined with or support with action in the "real world".

A closer look at the methods used by protest groups show that they often use technology both for cyber attacks and public relations, each presenting unique threats to their intended targets.

Technology vs. Public Relations

Politically motivated computer crime differs from traditional "hacking" in that the target is chosen - and the attack is designed - to effect a change in the behaviour or activity of the victim. Therefore, a cyber attack, in isolation, most likely will not accomplish the goal of the attacker. It is for this reason that politically motivated cyber attacks are often combined with extensive public relation campaigns. Many websites and media organizations are dedicated to various activist causes; one of the most effective is Indymedia (www.indymedia.org). The goals and extent of Indymedia are best exemplified in this quote:

> "INDYMEDIA, THE 'MULTIMEDIA PEOPLES' NEWSROOM', NOW PUBLISHES IN OVER 20 LANGUAGE AND OVER 35 COUNTRIES AND ITS TRAFFIC HAS BEEN ESTIMATED AT NEARLY 50 MILLION PAGE VIEWS A MONTH. USING INFORMATION TECHNOLOGIES IN A WAY UNFORESEEN BY THE CORPORATE WORLD, THE RAPIDLY GROWING NUMBER OF INDEPENDENT MEDIA CENTERS CONTINUES TO PROVIDE AN OUTLET FOR DISAFFECTED AND DISENFRANCHISED GROUPS BY REPORTING ALTERNATIVE VERSIONS OF THE NEWS THAN THE MAINSTREAM PRESS."[1]

Because much of the online PR activity of activist groups is legitimate free speech, it is important to understand and clarify the difference between lawful and potentially illegal activity.

Use, Misuse & Offensive Use

Politically motivated online activity can be broadly classified into three categories – *Use, Misuse* and *Offensive Use*.

Use is simply utilizing technology to facilitate communication or organization. In most western countries, this is protected free speech.

[1] Tarmen, Glen, "Digital Activism, the WTO and International Trade Rules", Trade Justice Movement, September 5, 2003.

Misuse is action that disrupts the activity of the intended target. An example of misuse is denial-of-service attacks. In the physical world, most protests are allowed; however, if the protests disrupt other functions of society such as access to private property, it is considered a (minor) crime.

Offensive Use is activity resulting in actual damage or theft. The physical world analogy would be a riot. An online example would be the disruption of the Israeli Stock Exchange website as discussed in the opening example.

History

Contrary to many media reports, politically motivated computer crime is not a new phenomenon. Some of the earliest incidents are attributed to German "hacker" groups such as the Chaos Computer Club (CCC) and the Bayerischer HackPost (BHP)[2]. Specific examples include:

- In the late 1980's, members of the CCC and other "hacker" groups were investigating and discussing how computers and networks could support the German Greens Party and the GAL (The *Grüne Alternative Liste* in Hamburg).
- In 1987, the BHP attempted to attack German government computer systems storing census information in the belief that the government should not collect personal information.
- In 1989, five German nationals with ties to the CCC were arrested and three convicted on espionage charges related to computer intrusions into a variety of commercial and military systems on behalf of the Soviet Union.
- In September of 1995, the CCC attempted to disrupt the French telecommunication infrastructure in protest to French nuclear testing[3].

Early politically motivated computer crime was not limited to German groups. For example, before the Persian Gulf War in 1990, Dutch intruders penetrated non-classified US Department of Defense computer systems searching for sensitive information related to US operations in the Middle East[4]. It was later alleged that the intruders attempted to provide stolen, non-classified military information to the Iraqis to support the antiwar effort.[5]

It is sometimes difficult to determine if an attack is politically motivated. In 1989, malicious software called the "WANK" worm was released in the internal network of Digital Equipment Corporation and later in the NASA / SPAN networks. This was jokingly named by the Australian authors as "Worms against Nuclear Killers" and has been misreported in several publications as an example of political hacking[6]. However, the authors had no political motive in these attacks and were playing on the British meaning of the word "wank"[7].

---

[2] Information on the CCC and BHP are taken from the author's personal notes recorded in 1987 and 1988 during investigations of activity of these and other individuals while assisting the German BKA (federal police).

[3] Chaos Computer Club, "Stop the Test", http://www.zerberus.de/texte/aktion/atom/ , September 1, 1995.

[4] Brock, Jack L., Jr., Testimony before the United States Senate Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, November 20, 1991.

[5] de Leede, Mike and Elings, Johan, "Data Terrorism", Penthouse Dutch Edition, September, 1992 (in Dutch).

[6] Denning, Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Conference on the Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking, San Francisco, December 10, 1999.

[7] Information on the motivation behind the release of the WANK worm is taken from the author's personal notes written in assisting the Australian Federal Police and the Norwegian Serious Fraud Squad.

The late 1980s saw the evolution of activist groups using networks and bulletin boards to communicate and share ideas. Examples include PeaceNet, Spunk Press and Econet.

Online political activity increased sharply in 1995 with the emergence of information warfare studies by the RAND Corporation and others.[89] Many activist and anarchist groups began to see the Internet as a medium not only to communicate but as a mechanism to break or change the existing political, commercial and other social structures.

The first large-scale example of effective, online political activism is the use of the Internet by the Zapatistas and their supports. At first, these groups used technology for organization and public relations.

However, in 1997 the first primitive attempts to organize electronic attacks took place to support the Zapatista movement against the Mexican government. An anonymous communiqué was issued stating:[10]

> "THE FOLLOWING CALL FOR A NETSTRIKE FOR ZAPATA ON THURSDAY, JANUARY 29, COMES FROM THE ANONYMOUS DIGITAL COALITION IN ITALY. IT CALLS FOR SIMULTANEOUS WORLD-WIDE VIRTUAL SIT-INS AT FIVE MEXICO CITY FINANCIAL INSTITUTION'S WEB SITES.
>
> RARELY HAVE GRASSROOTS GROUPS EXERCISED CYBERPOWER IN THIS WAY. CLEARLY PEOPLE IN ITALY ARE USING THEIR CREATIVITY AND IMAGINATION. THIS IS A UNIQUE OPPORTUNITY TO MOVE INTO NEW TERRAIN FOR COORDINATED WORLD-WIDE ACTION. BE PART OF WHAT IS PROBABLY THE FIRST GLOBALLY COORDINATED VIRTUAL SIT-IN!"

At this same time, a group known as the Electronic Disturbance Theater (EDT) was founded by a small group of people to support and develop more effective techniques. In two seminal papers[11], Stefan Wray, an EDT founder, developed the basis for what he called electronic civil disobedience which he defined as "acting in the tradition of non-violent direct action and civil disobedience, proponents of Electronic Civil Disobedience are borrowing the tactics of trespass and blockade from these earlier social movements and are applying them to the Internet".

In order to facilitate these ideas, the EDT developed a Java applet known as *FloodNet* to allow activists around the world to participate in denial-of-service attacks. With its release, politically motivated attacks on computers entered a new era.

Support for nationalist causes has also increased in recent years. In general, this activity ebbs and flows with the level of press converge or activity on the ground related to the conflict.

Examples of recent international conflicts with associated cyber attacks include:

- The recent call on an Islamic website for the creation of "Jaish al-Hacker al-Islami" or Islamic Hacker's Army[12]

---

[8] Wehling, Jason, "Netwars and Activists Power on the Internet", March, 1995. http://www.spunk.org/library/comms/sp001518/Netwars.html

[9] "I guerriglieri della rete", il manifesto, 26 April 1995 (in Italian), published in English as "Guerrillas on the Net", Italian COUNTERINFO #11, May 3, 1995.

[10] "Call for Virtual Sit-ins at Five Mexico Financial Web Sites", January 19, 1998. http://old.thing.net/wwwboard1/messages/650.html

[11] Wray, Stefan, "On Electronic Civil Disobedience", Paper Presented to the 1998 Socialist Scholars Conference, New York, March 20-22, 1998. http://www.thing.net/~rdom/ecd/oecd.html and Wray, Stefan, "The Electronic Disturbance Theater and Electronic Civil Disobedience", June 17, 1998. http://www.thing.net/~rdom/ecd/EDTECD.html

[12] Waterman, S., "Islamists seek to organize hackers' jihad in cyberspace", *The Washington Post*, August 26, 2005 http://washingtontimes.com/national/20050825-111136-2852r.htm

- China and Japan (related to WWII history books and anti-Chinese websites in Japan)[13][14]
- Serbia and Kosovo
- Korea, China and Japan (concerning reparations for WWII)
- Palestine, Israel and the United States

Types of Attacks and Impacts

As noted above, politically motivated attacks use two broad methods to attack an intended target: Technical cyber attacks and public relations.

Historically, technical cyber attacks are have been limited in scope and impact and are based on rather primitive techniques. The most common forms of attack include distributed denial of service (DDoS) attacks, web hijacking or defacement, spam and limited attempts to introduce viruses (usually via e-mail payloads).

There are examples of more sophisticated intrusions into the systems and networks of the target. The motive is often theft of information to embarrass the victim or to prove alleged wrong-doing by the targeted organization.

Surprisingly, analysis of these attacks indicates that many (though not all) have limited to no operational impact on the targets network or operations. DDoS attacks have the potential to be quite disruptive as demonstrated by attacks carried out for other motives such as extortion using "botnets". Historically, denial of service attacks carried out for political protest have not been well organized or utilized techniques such as botnets.

With this said, the techniques and methods used are continuously improving and have the capability for more significant disruption. There is no technical reason not to use these techniques for politically motivated attacks. The same methods used by organized crime groups, spammers and could be used by hacktivist groups to create significant disruption. *Organizations cannot be complacent when evaluating this risk*.

In many cases, the more effective form of attack (i.e. changing the victim's behavior or actions) is public relations, often in conjunction with technical cyber attacks.

The concepts of hacktivism and nationalist attacks can quickly gain the attention of the media so that even when the actual attack has little operational impact on an organization, the associated media coverage creates a more significant problem for the victim.

To better illustrate these concepts, two case studies are presented based on actual incidents. The first presents an analysis of a typical denial-of-service attack by online protesters. The second looks at the impact of public relations in combination with an online attack.

[13] Faiola, A., "Anti-Japanese Hostilities Move to the Internet", *Washington Post Foreign Service*, May 10, 2005
http://www.washingtonpost.com/wp-dyn/content/article/2005/05/09/AR2005050901119.html

[14] Park, S., "Chinese Hackers Might Hit Japanese Websites via Korean Servers", *Dong-a Ilbo, July 14, 2005*
http://english.donga.com/srv/service.php3?bicode=040000&biid=2005071460188

A Case Study – Denial-of-Service Attack[15]

Most hacktivist groups claim to have significant operational impact during their actions. However, a close examination shows that often most of the common tools and methods used have minimal technical consequences on the intended target. In many cases, the victim is not even aware that an attack is occurring.

The analysis below is from an actual attack in which the author advised and assisted the intended victim. This particular attack demonstrates common patterns in both methodology and the impact to network operations. Figure 1 shows a report generated by a network analyzer during a portion of the attack. This graph shows a classic pattern: Network scanning, the main attack and, finally, sporadic scans and attacks that taper off over a period of time.

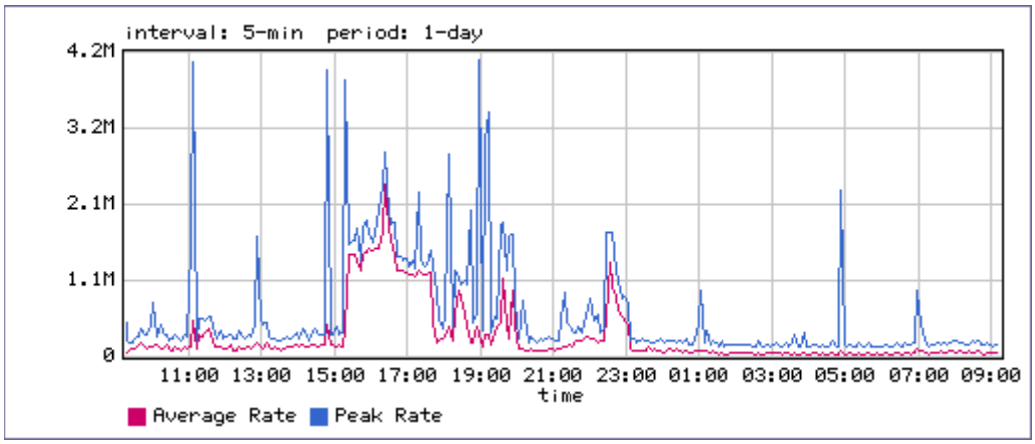

Figure 1 - Typical Pattern of Protest Attack

The first indications of activity are usually some form of network scanning. These scans help the attackers understand the external topology of the target network and look for common security vulnerabilities such as open ports or software with known security flaws.

The bandwidth spikes occurring at 11:00 and 13:00 were scans originating from sources in different countries apparently working independently of each other.

The main denial-of-service attacks began at approximately 15:00 and lasted through the evening. The activity at 05:00 and 07:00 was other network scans.

Figure 2 and Figure 3 show the details of a single scan followed by two separate ICMP DoS attacks. Note the two ICMP attacks at 19:36 and 19:50: In both cases, the effectiveness of these attacks degrades over time. This is because every router in the network between the attacker and the target must process the ping commands. In many cases, this can involve 20 or more systems – each one an innocent victim of the attack. As these systems become overloaded, the effect on the target in minimized.

[15] Information for this case study is taken from the author's personal notes and data collected while advising the victim during the attack.

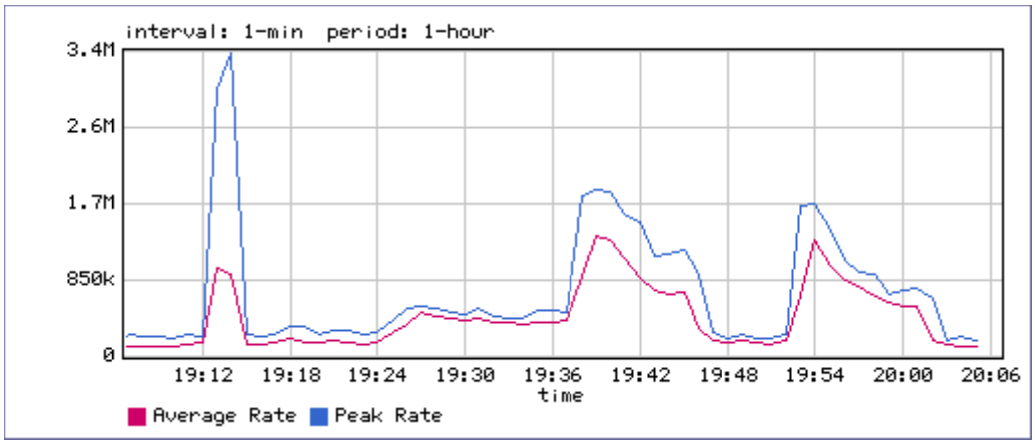

Figure 2 - ICMP (Ping) Attack

Figure 3 shows the overall bandwidth impact (less than 25%) during the attacks.

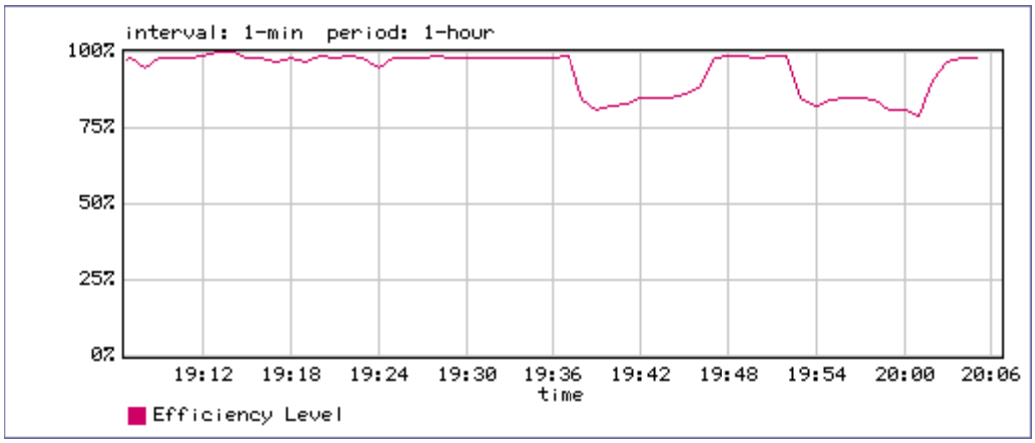

Figure 3 - Impact of ICMP Attack on Network Efficiency

These examples are representative of many DoS attacks orchestrated by hacktivist groups. They are rarely as coordinated as is commonly believed and often have little to no operational impact on a properly configured and protected network. What little disruption does occur is usually of limited duration.

If the target network is of any complexity, attacks are often misdirected against systems not directly supporting the subject of the protest since the attacker fails to analyze fully the network topology.

Public Relations – A Case Study

As previously stated, effectiveness of online attacks can be measured in how the attacks (or the threat of an attack) influence the targeted organization. Most protest groups have strong public relation skills (often superior to their technical skills) and release information before, during and after an attack. In many cases, this press coverage has a greater impact on the victim that any operational disruption caused by technical attacks.

This does not occur by accident. The relationship and dependence on media attention is articulated in the following quote[16]:

> "VIRTUAL POLITICAL ACTIVISM IS OBJECTIVE BASED, ACTION DRIVEN AND COMMUNITY ORIENTED. ITS OBJECTIVE IS TO ACHIEVE POLITICAL CHANGE THROUGH ATTENTION GAINED IN THE PRESS AND THROUGH DIRECT INTERVENTION IN CYBERSPACE AIMED AT A CORPORATE OR GOVERNMENT NETWORK ENTITY."

And in this definition of hacktivism given by the online magazine, The Hacktivist[17]

> "THE METHODOLOGY OF HACKTIVISM IS BEING DEVELOPED AND THUS SUBJECT TO CHANGE. HACKTIVISM COULD BE AS SIMPLE AS POSTING BANNED OR CENSORED MATERIAL ON THE INTERNET. HOWEVER, THE MEDIA RARELY REPORTS SUCH EVENTS AND HACKTIVISTS HAVE TAKEN TO "BENDING" THE LAW IN ORDER TO ATTRACT ATTENTION TO PARTICULAR CAUSES."

In almost all cases, the hacktivist groups exaggerate both the potential and actual impacts. Even mainstream media publications exaggerate and exploit the hype".

As a second case study, the World Bank, a common target of anti-globalization protests, decided in 2001 to hold a conference online to avoid the potential disruptions associated with a physical meeting. When this was made public, various groups (such as Greenpeace) issues press statements and gave interviews calling for the online disruption of the conference. The BBC, building on the hype, predicted that hacktivists would cause significant disruption[18]:

> "THE SERVERS WHICH WILL BE HOSTING THE ONLINE CONFERENCE HAVE JUST BECOME THE NUMBER ONE TARGET FOR THE LARGE AND GROWING COMMUNITY OF ONLINE COMPUTER HACKERS - THE 'HACKTIVISTS.' THEY WILL BE PROBED FOR SECURITY HOLES AND WHEN THESE ARE FOUND - AS THEY ALMOST CERTAINLY WILL BE - THEY WILL BE BROKEN INTO AND PERHAPS EVEN DAMAGED.
>
> "ON THE DAYS OF THE CONFERENCE ITSELF WE CAN EXPECT TO SEE A 'DENIAL OF SERVICE' ATTACK, WHERE OTHER INTERNET-CONNECTED COMPUTERS BOMBARD THE WORLD BANK SERVERS WITH FAKE REQUESTS FOR INFORMATION WHICH EFFECTIVELY BLOCK REAL USERS FROM RECEIVING ANY DATA. AND WE MAY EVEN SEE SOME NAME DOMAIN-NAME HIJACKING SO THAT VISITORS WHO WANT TO REACH THE CONFERENCE SITE ARE INSTEAD TAKEN TO ONE OF THE MANY PROTEST SITES."

The Guardian newspaper similarly carried boisterous comments[19]:

> "'ONE SKILLED IT PROTESTER COULD EASILY CRASH THE WHOLE EVENT. IT MAY BE SEEN AS A CHALLENGE TO SCUPPER THE CONFERENCE', SAID ONE PROTESTER/HACKER WHO SPECIALISES IN IT PROTESTS.
>
> "CYBER-PROTEST IS A WELL-DEVELOPED TOOL OF PROTEST GROUPS WHO USE COMPUTERS TO EXCHANGE INFORMATION, ORGANISE DEMONSTRATIONS AND BOMBARD POLITICAL LEADERS WITH DEMANDS. GREENPEACE HAS MORE THAN 100,000 SUPPORTERS PREPARED TO USE THEIR

[16] Morgan, J., "Virtual Political and Cultural Activism", *Switch*, CADRE Laboratory for New Media. http://switch.sjsu.edu/v7n1/james.html

[17] "Hacktivism", *The Hacktivist*, http://www2.iisg.nl/id/Systematik.asp?cat=7&id=3453

[18] Thompson, B., "Banking on Virtual Reality", BBC Online, June 2001.

[19] Vidal, J, and Denny, C. "Cyber War Declared on World Bank", The Guardian, June 20, 2001. http://www.guardian.co.uk/globalisation/story/0,7369,509697,00.html

> COMPUTERS AS A PROTEST WEAPON AND CLAIMS NUMEROUS SUCCESSES PERSUADING CORPORATIONS TO CHANGE POLICIES AFTER SUBJECTING THEM TO A BARRAGE OF EMAIL."

Despite several denial-of-service attacks, The World Bank's online conference was not disrupted[20]. However, significant coverage of the cyber attacks helped to promote the causes of the activists. The World Bank, in an effort to manage the negative public relations, invited several protest speakers to the conference, thereby meeting the activist's goal of changing (in a small way) the World Bank's actions.

The Future of Politically Motivated Computer Crime

Politically motivated computer crime has been around since the mid-1980's and will continue to grow as connectivity and access increase. The use of the Internet for communication, organizing and public relations will increase dramatically.

Online protest will increase and diminish with political activity in the real world, but will probably always remain disorganized – relying on the collective activities of disparate individuals and groups.

Activity that catches the attention of the press today will become old news tomorrow thereby requiring larger and more impressive attacks to capture interest.

What Should You Be Doing?

Because of the myriad motives behind politically motivated computer crime and the level of media hype, it is often difficult for executives and security professionals to understand and manage the threat. This confusion makes it easy to either over or under react.

Several trends are clear and should be considered when assessing the risk from politically motivated computer crime:

- Over time, disruption will increase in both volume and impact. The techniques and tools enabling individuals and groups to carry out attacks will become more sophisticated, effective and available. This trend is seen in all forms of computer crime.
- Public relations are a major weapon of hacktivist groups and will continue to create significant exposure. Organizations must likewise prepare for and effectively manage media attacks.
- Nationalist based attacks will shift in conjunction with the level of conflict between antagonists. U.S. and Western European organizations will continue to be at highest risk and exposure. Executives and security professions need to understand that they become the target of politically motivated attacks based on the perception of the attacker, not necessarily the reality of the organization's business. Therefore, major U.S. companies are likely targets simply because of their international brand recognition, not because of any action on the part of the company.
- Increasingly, third parties will become the target of attacks. Activist groups supporting animal rights and anti-globalization movements often target the customers or investors of the intended victim in order to produce greater pressure. When attacks are aimed at websites, other, unrelated websites hosted by the same provider can be affected. In other cases, attackers may not have the sophistication to identify accurately the ownership of particular IP addresses and may affect suppliers, outsourcers or vendors connected to the target's network.
- As wireless and hand-held technologies are developed and become more widely implemented, politically motivated attackers will see these mobile infrastructures as rich targets to spread their messages and agendas.

[20] "ABCDE Online Conference Draws Broad Participation in Global Dialogue", Press Release, World Bank, June 26, 2001.

As with all computer crime, there is no "silver bullet" solution to prevent politically motivated attacks. However, basic security precautions and preparedness can significantly mitigate potential impact.

Specifically, Security Officers should:

1. Develop intelligence to determine if your organization is a potential target. This should include an analysis of your relationship with other third parties that may place your organization at risk. This is not a "one off" assessment, but should be carried out on an ongoing or periodic basis.
2. Perform regular formal risk assessments. A thorough understanding of risk is crucial to making informed decisions on where controls should be implemented. The consequences of not properly assessing risk can be profound – not only are some threats overlooked, but resources and budgets are misapplied to threats that do not exist or have minimal impact.
3. Develop comprehensive incident response plans and test them regularly to ensure they are effective.
4. Include public relations and crisis communication in response plans.
5. Analyze network architectures to understand the potential for disruption from common threats such as denial-of-service attacks. Review firewall configurations and your IT organization's ability to detect quickly unusual patterns of activity.
6. Perform regular vulnerability scans of systems and applications, ensure software patch levels are up-to-date and monitor websites for unauthorized changes.

These recommendations are a good first step in managing the risk associated with politically motivated crime.

Incident planning during a crisis is a recipe for disaster. If an organization's leaders have not proactively planned how they will manage a problem, they will inevitably suffer greater business disruption, exposure to negative PR and higher recovery costs.

Forethought and planning make a significant difference in the outcome of any crisis.

Other Papers by Kent Anderson, CISM, Managing Director, Encurve, LLC

"A Business Model for Information Security", published in *Information Systems Control Journal,* Vol. 3, May, 2008.
One of the greatest challenges in information security is aligning with business objectives. The disconnect between information security operations and strategic business objectives results in pressure to increase security spending while risks, incidents and losses continue escalating to unsustainable levels. A framework enabling information security professionals to align their activities with their organization's business is needed.

"Convergence: A Holistic Approach to Risk Management" published in *Network Security*, Elsevier Ltd., Volume 2007, Issue 5, May, 2007.
Every year IT security managers develop new budgets requesting more funds and resources to stem the tide of endless security issues – patching, virus management, provisioning, installation of new appliances, the list goes on. Every year business leaders listen to these requests and usually provide a fraction of the requested increases. This cycle has become a ritual in the IT security profession and fits Albert Einstein's definition of insanity: Doing the same thing over and over again expecting different results.

"IT Security Professionals Must Evolve for Changing Market" published in *SC Magazine*, October 12, 2006.
IT security awareness is at an all-time high, and organizations are spending and hiring in record numbers. Legislation and regulations are proliferating. Yet, for all this effort, nearly every statistical measure of IT security performance – from the number of incidents and vulnerabilities to the cost and impact of a security breach – is bad news. In what other endeavour would so much investment be permitted with such poor results?

"Managing the Cyber Threat"
Technology is not the only source of risk to information infrastructures. Political, physical, environmental, legal and regulatory issues are all factors contributing to the creation of a multi-dimensional problem. While prevention is the preferred course of action, no security measures are perfect. Organizations must be prepared to quickly detect and effectively respond to the threats they face in the ever-changing e-business environment.

"Intelligence-Based Threat Assessments"
Few organizations invest in proper risk assessment before implementing controls. Even fewer have the capability to understand and qualify specific threats to their information assets in order to assess risks accurately. The consequences can be profound. Not only are some threats overlooked leaving inadequate controls, but also scarce resources and budgets may be misapplied to threats that do not exist or have minimal impact. This paper will discuss threat assessments, risk assessments and information infrastructures in general and provide an overview of an intelligence-base threat assessment model.

"Criminal Threats to Business on the Internet: A White Paper"
This paper looks at the increasing trend of criminal activity against information systems, from the low-level, amateur intruder to organized crime, industrial and international espionage. In addition, the author looks how this activity is likely to evolve in the near future.

"International Intrusions: Patterns and Motives"
A summary of the author's investigations of international intrusions. This paper presents a classification model of the attributes and motives displayed by intruders and explains common patterns of activities. The author argues that common methods of investigating computer intrusions are limited in scope; therefore, security solutions and tools have limited effectiveness.

ABOUT KENT ANDERSON

Mr. Anderson is considered a leading authority on security with more than 23 years of experience in the field. He is the founder and Managing Director of Encurve, LLC located in Portland, Oregon.

Mr. Anderson's international experience includes managing the security organization for a Fortune 50 company, developing professional security businesses and advising security and business executives on risks and threats, establishing proactive security programs and implementing effective response capabilities.

Mr. Anderson's expertise is founded on real-world understanding of threats and business requirements. He has led or coordinated numerous international investigations including espionage, industrial espionage, computer misuse (hacking), sexual harassment, threats of violence, extortion, fraud, intellectual property thefts, copyright infringement and product counterfeiting. These investigations have resulted in the successful prosecution of 10 individuals including Kevin Mitnick and numerous civil cases.

Mr. Anderson has been quoted by numerous publications including the Washington Post, CNN, Associated Press, Reuters, USA Today, Los Angeles Business Daily, Singapore Business Times, Danish National Radio (DR), the BBC and numerous trade publications. He is a spokesperson on security matters for ISACA.

He has provided training and assistance to various law enforcement and government agencies including the FBI, U.S. Secret Service, Department of Defense, Department of Justice, FLETC, Scotland Yard, the German BKA, the Russian MVD and Norwegian, Danish and Swiss police. Additionally, he provided consulting to the Organization for Economic Cooperation and Development (OECD) on international harmonization of computer crime laws and the British Houses of Parliament on the development of the U.K.'s Computer Misuse Act.

He has held positions as Senior Vice President of IT Security and Investigations with an international business risk consultancy, as Director in the Dispute Analysis & Investigations group of PricewaterhouseCoopers, LLP and as the European Information Security Manager for Digital Equipment Corporation.

Mr. Anderson is a Certified Information Security Manager and serves on Motorola's Research Visionary Board and on ISACA's Security Management Advisory Committee.

ABOUT ENCURVE, LLC

Encurve, LLC is a Portland, Oregon based, independent risk consulting firm providing *informed risk strategies*™ to its clients worldwide. Encurve has provided consulting and advisory services to companies in a wide range of industries such as high tech and heavy manufacturing, food services, mining, banking and finance, biotech and telecommunications.

We believe in *building intentional security*™. Intentional security is *purposeful, deliberate* and *planned*. It takes the guesswork and fire-fighting out of security to develop efficient and proactive security organizations and operations. Encurve never sells pre-packaged services delivered by inexperienced consultants using checklists and canned reports. We listen to and understand our clients and solve *their* problems. All of our offerings are based on four guiding principles:

1. Alignment of security with business objectives to enable and support the organization;
2. Convergence of security strategies to maximize return on investment – traditional models of separate security functions can be wasteful and hinder management of cross-functional risk;
3. Risk-based decision making founded on understanding the unique threats and risks to each organization; and,
4. Strategic focus to transform the security organization from tactical and fire-fighting to strategic and pro-active.

From surveillance systems to Internet investigations, Encurve is one of few risk consultancies that can provide truly converged security solutions. We also specialize in understanding how to align security organizations and operations with the business – something many companies talk about but few can deliver.

Encurve, LLC offers services in three broad practice areas:

1. **IT& Physical Security Management Services –** Employing real-world experience and proprietary methodologies to help security organizations become more focused and efficient.
2. **Executive Support Services –** Providing the strategic and business focused analysis executives require to make investment and risk decisions without getting lost in the technology. We understand that security is a business investment and should return value to the organization.
3. **Security Business Development –** Enabling companies to provide professional or managed security services through the development of core and differentiated capabilities.

Encurve, along with its pre-qualified and certified partners, provides world-class security and investigative capabilities to address the needs of both executives and operational staff.

Contact us today to learn how you can create *intentional security*™ in your organization:

www.EncurveLLC.com
+1.503.203.8295
kea@EncurveLLC.com