Cyber Jihad and the Globalization of Warfare

Computer Networks as a Battle Ground in the Middle East and Beyond

Kenneth Geers, NCIS
Dr. Peter Feaver, Duke University
Asymmetric warfare

- Unconventional weapons
- Innovative strategy
- Leveraging inferior strength to tactical advantage
- Aimed at attacking the will of your target
- Leads to fighting chances for the weaker opponent
- Used by terrorists
- Used by the media
- Used by computer hackers
Asymmetry and hacking

- Anonymity
- Deniability
- Affordability
- Myriad avenues of attack
- Non-state actors can join the fight
- Subcultures can mobilize
The globalization of warfare

- Private and state interests sometimes indistinguishable
- Citizens of country X might fight for country Y
- Anyone, anywhere, can volunteer at any time
- Corporations are active participants both as targets and possibly as combatants
Let’s Go Fight!

- No traditional chain of command
- Coalitions of the willing
- Opportunistic participants
  - Spanish civil war
  - Hacktivism gives **everyone** a chance to impact the course of history
- Outsourcing warfare
Cyber targets

- Two predominant attacks: DoS and defacements
- Business loses revenue, government face
- Is target significant or merely vulnerable to attack?
- Nation-state involvement
Zone-H statistics

- Why did you deface this website?

<table>
<thead>
<tr>
<th>By attack reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heh... just for fun!</td>
<td>34%</td>
</tr>
<tr>
<td>No reason specified</td>
<td>18.5%</td>
</tr>
<tr>
<td>I just want to be the best defacer</td>
<td>13.7%</td>
</tr>
<tr>
<td>As a challenge</td>
<td>11.4%</td>
</tr>
<tr>
<td>Patriotism</td>
<td>10.5%</td>
</tr>
<tr>
<td>Political reasons</td>
<td>10.1%</td>
</tr>
<tr>
<td>Revenge against that website</td>
<td>1.8%</td>
</tr>
</tbody>
</table>
• Lists broadcast sites, average amplification 5x
The Challenges of Privatized War: Retaliation

• Who really hacked me, or the problem of the last hop
• What if the hack was state-sponsored?
• Sue, hack back, or bomb the hell out of them?
• What do the lawyers say?
Challenges of Privatized War: Legal

- Hacking is illegal, but state-sponsored hacking occurs every day
- The question of “patriotic” hackers
- FBI sting operation in Russia
- The U.S. may have more legal liabilities than some of its adversaries
Case in Point: The Middle East cyberwar

- Core hackers: less than 100
  - provide the ideas, the tools
- Volunteers and conscripts: a few thousand
  - From all over the world
  - Provide brute force scanning and DoS power
- Cyber attack intensity has mirrored the intensity of fighting on the ground
Hacktivist volunteers

• Middle East conflict stirs emotions
  – Emotional
  – Ideological
  – Patriotic
  – Religious

• Everyone, everywhere, has a strong opinion about something!
Cyber tools used by both sides

- Ping-flood
- Ping of Death
- EvilPing
- Winsmurf
- QuickFire
- Defend
- HTTP Bomber 1.001b
- FakeMail
- MailBomber
- Attack 2.5.1
- PutDown
The Defend attack tool

• FloodNet-type
• New attack method
  – Requests non-existent webpages
  – Specifies the current date / time
  – Defeats Web-caching security mechanisms
• Many versions developed during war
• Mirrored on many partisan websites
• Dozens of targets successfully attacked
• Effectiveness relies on number of attackers
The victims

• Pro-Israeli attacks
  – Official/organizational in nature
  – Terrorist/extremist websites first
  – ME government sites second

• Pro-Palestinian attacks
  – Israeli official government
  – Commercial/corporate: technology, telecommunications, media, financial
Types of targets

- Web sites
- E-commerce servers
- E-mail servers
- Internet relay chat (IRC) channels
- WWW chat rooms
- Domain name servers (DNS)
- Internet service providers (ISPs)
- File transfer protocol (FTP) sites
Government websites attacked

- Israel
- Palestine
- Iran
- Lebanon
- Malaysia
- Qatar
- United Arab Emirates
- United States
Israeli hackers

- Deri Schriebman
- Mossad
- Nir M
- Polo0
- Wizel
- Israel Hackers Unite
- Mike Buzaglo
- Israeli Internet Underground
- a.israforce.com
- SmallMistake
- Hizballa – No More
- Lion&type_o ha k’eil
- ViRii
- The Analyzer
www.magaf.org
June, 2004

For nomadic (javascript-based) crypto tools, see Ubik CipherSaber (UbikLite, UbikChat, etc.)

Jabber instant messaging - (Launch java client...)

The Disorder of Johnny RandomSeed

You can exchange keys here (powered by Tag-Board):

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/05, 13:24</td>
<td>MuShKila</td>
<td>hi all</td>
</tr>
<tr>
<td>02/04, 15:38</td>
<td>CitizenX</td>
<td><a href="http://docs.indymedia.org/view/Local/TmcIsrael">http://docs.indymedia.org/view/Local/TmcIsrael</a></td>
</tr>
<tr>
<td>01/04, 21:23</td>
<td>skidz</td>
<td>shut?</td>
</tr>
<tr>
<td>06/03, 13:05</td>
<td>Goat boy</td>
<td>QuickCAT is not open source, QuickCAT is baaaaaahaaad.</td>
</tr>
<tr>
<td>26/02, 5:04</td>
<td>Nimrod</td>
<td>psssst. want a web-based rss aggregator for a price of 10 minutes work?</td>
</tr>
<tr>
<td>14/02, 16:16</td>
<td>Nimrod</td>
<td>Dazz? As in Daz23? How's it going, mate?</td>
</tr>
<tr>
<td>1/02, 14:15</td>
<td>Dazz</td>
<td><a href="http://www.haaretz.co.il/hasite/spages/394019.html">http://www.haaretz.co.il/hasite/spages/394019.html</a></td>
</tr>
<tr>
<td>10/03, 11:10</td>
<td>polynomial</td>
<td>UbikCAT (<a href="http://www.ubikcat.com">http://www.ubikcat.com</a>) has novel software that year</td>
</tr>
</tbody>
</table>
Targets of Israeli hackers

- Palestinian National Authority
- HAMAS
- Hizballah
- U.S. Pentagon
- VISA
- Iranian government
- Israeli sites, including Knesset
m0sad defacements

Attacked by m0sad: 67 of which 54 are single IP and 13 mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement

<table>
<thead>
<tr>
<th>Time</th>
<th>Attacker</th>
<th>Domain</th>
<th>OS</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001/01/03</td>
<td>m0sad</td>
<td>sys.edu.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>saaa.org</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>mustafadaas.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>spicers.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/01</td>
<td>m0sad</td>
<td>modelli.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/31</td>
<td>m0sad</td>
<td>dpi.net.ir</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/31</td>
<td>m0sad</td>
<td>sysnet.com.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/29</td>
<td>m0sad</td>
<td>hsrep.com.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/20</td>
<td>m0sad</td>
<td>isna.net</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/19</td>
<td>m0sad</td>
<td>iugaza.edu</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/15</td>
<td>m0sad</td>
<td>talkislam.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/12</td>
<td>m0sad</td>
<td>★ mfa.gov.ir</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/10</td>
<td>m0sad</td>
<td>★ dcaauh.gov.ae</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/03</td>
<td>m0sad</td>
<td>★ islam.gov.qa</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/01</td>
<td>m0sad</td>
<td>webhosting.ajeeb.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/11/29</td>
<td>m0sad</td>
<td>islamweb.net</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/11/27</td>
<td>m0sad</td>
<td>khaleej.com</td>
<td>Windows</td>
<td>view</td>
</tr>
</tbody>
</table>
Shot across the bow

www.hizbulla.org website

October 25, 2000
Poisoned pen tactics

- Disinformation campaign
- Israeli tactic
- Used against Hizballah websites
- Israelis registered and configured websites using misspellings of “Hizballah”
- Hizballa.org, hizballa.com, etc
- Great opportunity for free propaganda!
• FloodNet-style DoS attack tools
• Tools targeted six different Hizballah sites
• Activates a file to target the site every second
• Oct 6, 2000, Ali Ayoub, Hezbollah site webmaster: “The Web site will automatically do the attacking for them"
אוקיי חרב

عصתי אנחתי סבכי ללבך מה הולך הלויות כآن!!!

הולכת ליהוה כآن مديرונתי מישכיתו!!!!

אנתים חפש נאלא או חרבם!!!!

נישרו זה בתיהו!!!

נידקר כל ציור שועבר ברוחו!!!!

אנתים שמים זה על.metroן!!!

וזו על כל ה損害ו!!!!

ינדך!!!!

ולמי שרואים חורב?!

למי שלא ראינו! שופטו! ישראלתלחת חיות!AMED!!!

אנתים ביאס מתשובה מה שאנתים יוכלים בדריס בזענו!!! בוא ונפל את האזרחים של החווראה!!!

שלום ימה להם אצק להתייבא במעשיו הנגביהו בходим צייקו!!!

וזו על כל הugeotים!!! זוז!!!

 besar

THE_MAN & ZeroCool
The search for more targets

• There were not enough Palestinian sites to attack
• Israelis began attacking sites indirectly involved in conflict
• Iranian Min Foreign Affairs, Agriculture
• Lebanese television
• www.almanar.org attack
Interfada: Counterattack

- Pro-Palestinian hackers began to work methodically through .il sites
- At height of ME Cywar, defaced 5x number of websites as pro-Israeli side
- Paralyzed half of Israel’s e-mail system for several days
- Took aim at Israeli e-commerce sites
Israel: cyber target

- Unlike Palestinian side, extensive target list
- Thus, Israel potentially had more to lose
- Most of population, nation wired
- Millions of Internet connections
- More than all Arab countries combined
- More targets = more vulnerable boxes
- Pro-Palestinian hackers successfully attacked many more sites during the conflict
Pro-Palestinian Hackers

- UNITY
- G-Force Pakistan
- Doctor Nuker
- Pakistani Hackerz Club
- ReALiST
- PROJECTGAMMA
- World’s Fantabulous Defacers (WFD)
- Arabhackers.org

- dodi
- Xegypt
- Hezbollah
- Ummah.net
- Arab Hax0rs
- al-Muhajiroun
- m0r0n
- nightman
العوائد الجديد

إحتفال المسلمين في مصر وحدهم وحدهم في بيوتنا نشاط أعمال وآلاف الفقهاء في فلسطين ونرى أننا
أبقوا يحتفلون وطريق مختلف وكان الهيكل يحتفل طرق جيدة للفصل؟ فإنها هولاوا بangen؟؟ الأسما
 المسلمين الذين مع تلك أثر في عملنا هو المرجع، فإن به من تاريخنا إلى نحن عن الرحمة رضوان
الله عليهم؟؟ أن نحن عن صفر الحسابهم وهم لم يتجاوزوا السامسا والسبدسة عشر ويجادون في سبيل
الله؟؟

لماذا لا نجاهد في سبيل الله تنصر لإخواننا في فلسطين وإخلاء للكتلة الله تعالى فيما الفصص أو الشهادة ورضوان
الله والنور والغيوم وما تريوا
أما ما يحدث الآن فهو قمة الأذل للعرب والملحنين في شتى بلاد العالم، إن كان لا تستطيع الناس في فلسطين ففيكك الفقاه والتبعية
وعلل عن طريق تغير المواقع الإسرائيلية

والتى على شبه العمل للملحنين الكبار إ oldu دعوتنا تتح ولا مرة

لمشاركة في مجموعة الجهود الإلكترونية

عدد المشاركة في مجموعة جهود وبث النشر بموجب الضرورة للمواقع

شارك في جمعية رحلة الفقه وأโปรด رائد، وأيضاً إن كنت ترى أن يوجد برنامج تدريب متغير عن ما ذكر أو برنامج تري في الله علم لنا
GROUP(I):
Click HERE and Help the Resistance(I).

You will attack:

IP: 212.143.256.4

IP: 212.143.256.4

IP:63.194.226.226

IP: 194.90.202.20

GROUP(II):
Click HERE and Help the Resistance(II).

You Will Attack:

www.bankisrael.gov.il
IP:161.58.232.244

Tel Aviv Stock Exchange(www.tasc.co.il)
IP:192.116.46.129

www.pmo.gov.il(Prime Ministry Office)
IP:147.237.72.93

www.wizel.com
Pro-Palestinian attack portals

- www.ummah.com/unity
- Pro-Palestinian attack portal
- Due to complaints, moved and renamed:
  - http://defend.unity-news.com
  - http://members.tripod.com/irsa2003
  - http://members.tripod.com/irsa2004
We have been forced to remove this site

The bandwidth providers to our ISP, after receiving many complaints from Zionists and their supporters in the UK, have threatened to cut off our internet connection if this site was not removed. We have therefore removed this site in order to keep the rest of ummah.com online.

Most sincere apologies,

The ummah.com team
Israeli victims

- Official gov’t portal
- Israeli Foreign Ministry
- Israeli Knesset
- Israeli Army
- Israeli Central Bank
- Haaretz, Jpost
- Netvision
- TA Stock Exchange
- Bank of Israel
- www.wizel.com
- AIPAC
- Prime Minister
- Likud party
- Israeli universities
- AT&T
USA: caught in the crossfire

- The friend of my enemy is my enemy
- Israeli hackers had been hacking U.S. sites for years
- Pro-Palestinian hackers (including the anti-American Brazilians) found a natural target in Israel’s ally, the U.S.A.
Hacking the U.S.A.

- Largest player in international politics
- Largest IT infrastructure
- Corporate Internet security still inadequate
- Vulnerable to same tactics used in ME
- FBI's NIPC warned early that ME Cywar could spread to US-based sites
- Should expect shots in future cyber conflicts
The USA versus China

- May 2001: PRC hackers attempted a national, coordinated cyber attack on U.S.
- EP-3 triggered a major conflagration
- Chinese, U.S. hacking portals built: “USA Kill”, “China Killer”
- U.S. retaliation: Poizonbox
- NIPC warning: 26 April 2001
Impact: perception and reality

- Cyber war is a new avenue through which to take part in global conflicts
- Computer exploits can be good PR
- ME Cyber War may serve as a test bed for cyber weapons and strategies
- DoS and defacements worth guarding against, but they are not WMD!
- The question of defacements and free speech
National defense strategies

- Still in flux, like early nuclear era
- Europe: squashing all hacking activities
- United States: laissez-faire attitude
- International agreements not likely
- Widespread scanning for zombies
- Incentives to security, law enforcement
- Encourage the White Hats?
- Fine those with poor security practices?
Can hacking affect military operations?

- **Before the fighting**
  - Intelligence collection
  - Indications and warning

- **During the fighting**
  - Denial and deception
  - Negative e-mail campaigns
  - Poisoning military blogs
Could populist cyber attacks spark a real war?

- Cyber attacks usually follow, and react to international events, not vice versa
- If governments are not in control, hackers could affect level, timing of tension
- In Middle East, not enough pro-Palestinians are yet wired
- U.S.-China case: American hackers have more independence, thus more power
The most powerful cyber attack: propaganda

- Old fashioned
- Some *faked* in English papers
- The Internet dissemination of the Abu Ghraib photos did more to damage the political interests of the U.S. than all of the cyber attacks since the beginning of the Internet age!
Who is most at risk from hackers?

- Corporations have the most to lose
- Loss of trust
- Public ridicule
- Money lost from downed e-commerce
- Time and effort needed to fix the problem costs even more money
The Future

- Populist cyber attacks will be part and parcel of highly-charged, emotional conflicts
- So far not very effective at accomplishing political goals
- They are best for targeting corporations
- Sophistication of attacks is increasing over time
- Will anti-globalization forces launch the next cyber war?
- Will traditional extremist groups begin to work with these hacker groups?
Cyber Jihad and the Globalization of Warfare

Computer Networks as a Battle Ground in the Middle East and Beyond

Kenneth Geers, NCIS

Dr. Peter Feaver, Duke University
References

Bit666 Wise (bit666wise@hotmail.com). “FBI Chases Analyzer (Hacker),” Original Format Newsgroups: alt.2600.hackerz, 1998/03/11.
Gentile, Carmen J. “Israeli Hackers Vow to Defend,” wired.com, Nov. 15, 2000 02:00 AM PT. http://www.wired.com/news/politics/0,1283,40187,00.html
Allen, Patrick D.; Demchak, Chris C., U.S. Army CGSC Military Review March 1, 2003 SECTION: No. 2, Vol. 83; Pg. 52; ISSN: 0026-4148 IAC-ACC-NO: 106732244
Hershman, Tania. “Israel Discusses the ‘Inter-fada’,” wired.com, Jan. 12, 2001 06:00 AM PT. http://www.wired.com/news/politics/0,1283,41154,00.html

"Israeli-Palestinian Cyber Conflict," iDEFENSE Intelligence Services Report, Version 2.0PR, PUBLIC RELEASE, Jan. 3, 2001
Leibold, Dave (djcl@bnw.debe.fl.us). “Subject: Israeli Hacker Caught View,” Newsgroups: comp.dcom.telecom, 1991-09-17, 10:24:12 PST.
References, cont’d


masakim (masakim@kun.ne.jp). “Re: asymmetrical warfare,” Newsgroups: alt.usage.english, 2001-09-12 00:07:25 PST.


Neo202 (bachafrancois@my-deja.com). “cyber war 2 leb vs israel,” Newsgroups: soc.culture.lebanon, 2000-10-30, 06:10:11 PST.


Zone-h.org, http://www.zone-h.org/en/index