



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



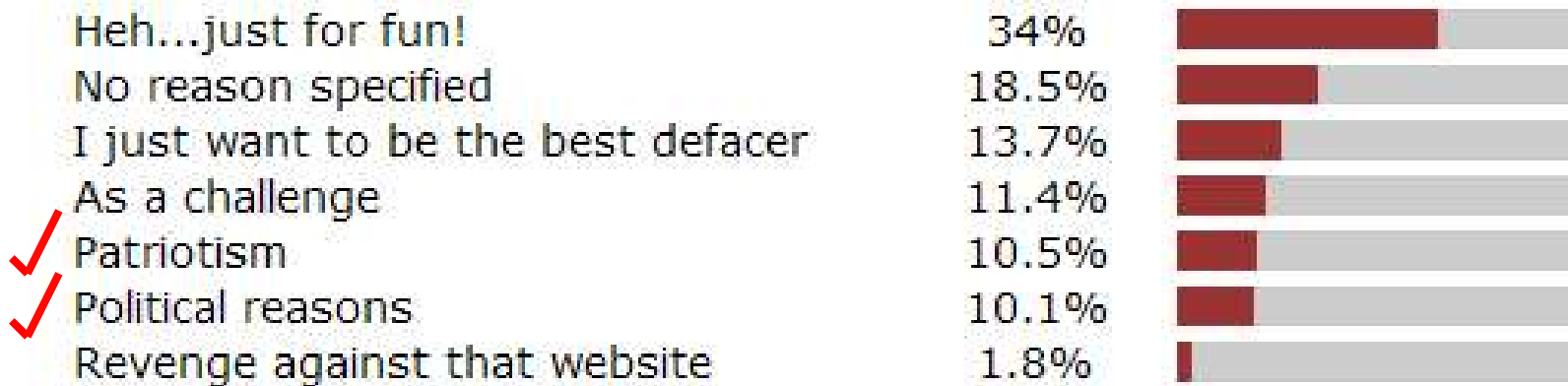
Cyber targets

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

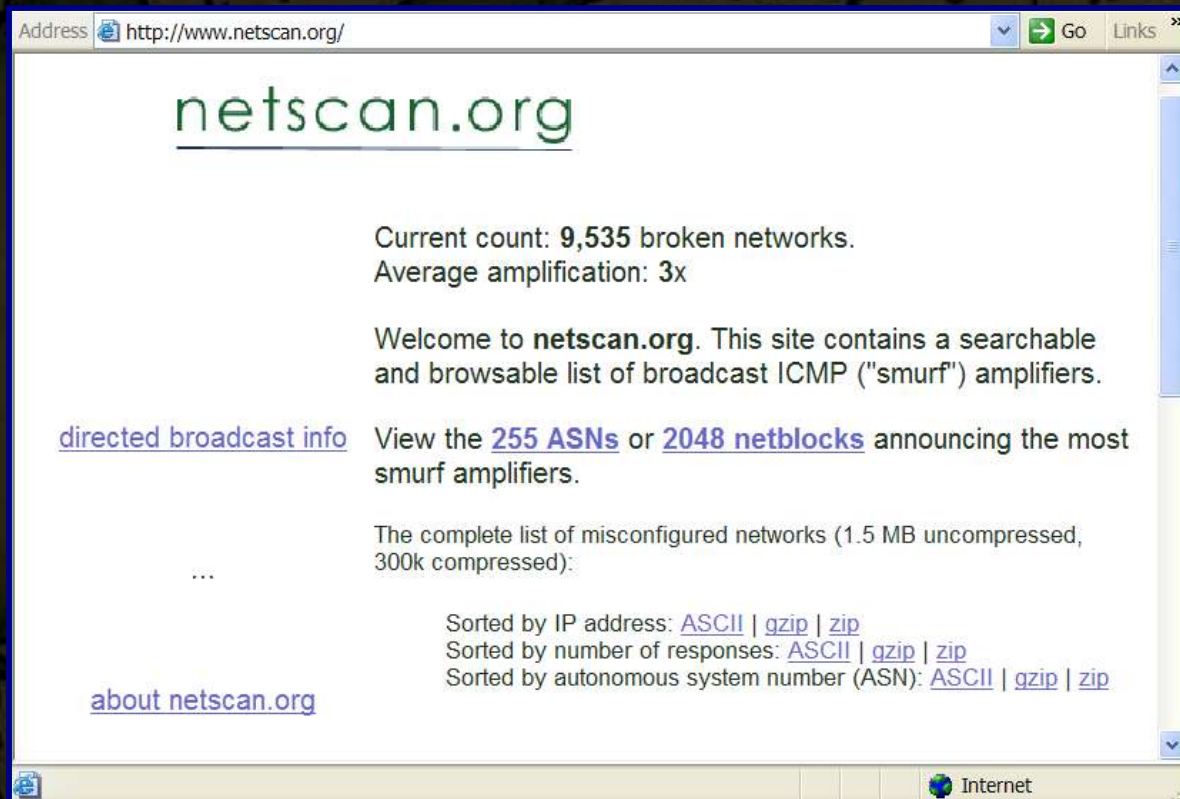
Zone-H statistics

- Why did you deface this website?

By attack reason:



Netscan.org



- Lists broadcast sites, average amplification 5x



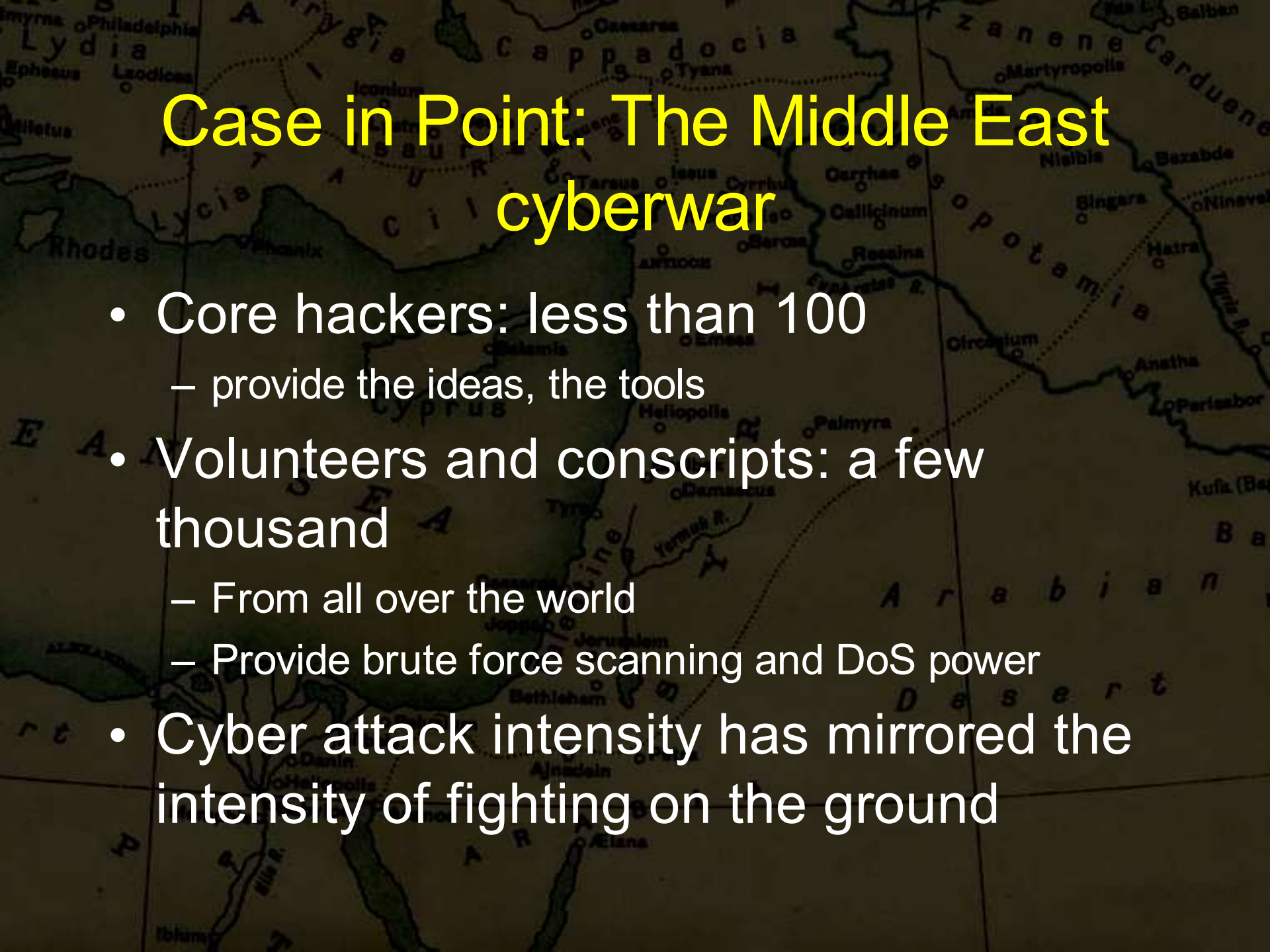
The Challenges of Privatized War: Retaliation

- 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



Hactivist 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.a.israforce.net

Nov. 9, 2000

חיזבאללה - לא עוד!

אתר עם מטרה אחת - לא לתת לארגוני טרור אכזריים להשריץ אתרי טרור, הפצת מאמרים, סרטים ותמונות חולניות ברשת האינטרנט הכלל-עולמית

ברוכים הבאים

טפסים היוניים

שבת, 5/6/2004

Israforce
Net

מבזקי חדשות

ליבנו איתם!



חיילנו החטופים

עד מתי?

מימין לשמאל:

סמ"ר בני אברהם, רס"מ עומר סוועד וסמל עדי אביטן



israforce.net



"חיזבאללה - לא עוד" שולח את תנחומיו אל משפחת זאבי האבלה שאיתה איבדנו אדם שהיה חלק מליבה הגדול של מדינת ישראל.

ספר אורחים

פורום

Ynet news

הוסף אותנו לוואלה

טבלת מצב

ציאת - חדש

בדוק איי-מייל

תמונות

כתבות/ראיונות

חמאס - לא עוד

קישורים

צור קשר

פרסום

ריכוז אופציות להפלת החיזבאללה:

תוכנה:

הורידו עכשיו את התוכנה המיוחדת נגד החיזבאללה. (יש להוריד עידכון מיד לאחר הורדת התוכנה והתקנתה)

www.magaf.org

June, 2004



כניסה

(צריך SSL)

New design by Mushroom of Doom
Got a better design for this page? Post it as an attached zip
(or forever hold your peace :-)

"אף אחד לא בא לפה בשביל הגרפיקה" -- Hackerina

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

Jabber instant messaging - דיבור צפוף

חדש: שפיפון > ^, ~ ~ ~ ^ (ושפיפ > ^, ~ ~ ~ ^ (

The Disorder of Johnny RandomSeed

Become an indicsiple

Prove that you are one

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

```
02/05, 13:24 MuShKiLa: hi all ☺
26/04, 23:51 raad: hi please try to look in
http://italy.indymedia.org/news/2004/04/533588.php
02/04, 15:38 Citizen X: http://docs.indymedia.org/view/Local/ImcIsrael
01/04, 21:23 skidz: 🤪 shu???
08/03, 13:05 Goat boy: QuickCAT is not open source. QuickCAT is baaaaaaahhaaaad.
26/02, 5:04 Nimrod: psssst. want a web-based rss aggregator for a price of 10 minutes work?
http://rawfish7.tripod.com
14/02, 16:16 Nimrod: Dazz? As in Daz23? How's it going, mate?
13/02, 14:15 Dazz: http://www.haaretz.co.il/hasite/spages/394019.html
10/02, 11:19 polynomial: QuickCAT (http://www.quickcat.com) has novel software that uses
```

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

Time	Attacker		Domain	OS	View
2001/01/03	m0sad	H	sys.edu.pk	Windows	view mirror
2001/01/02	m0sad	H	saaa.org	Windows	view mirror
2001/01/02	m0sad	H	mustafadaas.com	Windows	view mirror
2001/01/02	m0sad	H	spicers.com	Windows	view mirror
2001/01/01	m0sad	H M	modelli.com	Windows	view mirror
2000/12/31	m0sad	H	dpi.net.ir	Windows	view mirror
2000/12/31	m0sad	H	sysnet.com.pk	Windows	view mirror
2000/12/29	m0sad	H	hrep.com.pk	Windows	view mirror
2000/12/20	m0sad	H	isna.net	Windows	view mirror
2000/12/19	m0sad	H	iugaza.edu	Windows	view mirror
2000/12/15	m0sad	H	talkislam.com	Windows	view mirror
2000/12/12	m0sad	H	★ mfa.gov.ir	Windows	view mirror
2000/12/10	m0sad	H	★ dcaauh.gov.ae	Windows	view mirror
2000/12/03	m0sad	H	★ islam.gov.qa	Windows	view mirror
2000/12/01	m0sad	H	webhosting.ajeel.com	Windows	view mirror
2000/11/29	m0sad	H	islamweb.net	Windows	view mirror
2000/11/27	m0sad	H	khaleej.com	Windows	view mirror

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!



www.wizel.com

- 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"

<p>עם ישראל!!! עזרו לכולם להפיל את האתר של החיזבלה לפנכים המדריך בישביל לדעת איך להפיל את האתר נכנסים לתפריט, התחל,שבצדל מטה של המסך, אחר כך נכנסים להפעלה,ואז כותבים את הפקודה הבאה ping 192.116.19.4 -t -w 2600 ולוחצים אישור ואז ייפתח חלון שחור כזה פשוט לעשות לחלון מזער והוא יירד למטה ולהשאיר אותו פתוח, אם יעשו ככה הרבה אנשים האתר ייפול חזק,תודה לכולם על שיתוף הפעולה זה כתובת האתר http://www.pna.net בבקשה העבירו לכולם</p>	<p>לכל מי שיש ניוקים ופצצות לאימייל !שיפוצץ את האימייל של החיזבלה !זה האימייל webmaster@hezbollah.org <u>אם אין לכם תוכנה אז תורידו כאן</u></p>
<p>כולם להמשיך אתר נוסף של החיזבלה</p>	<p><u>הורידו את התוכנה שמפילה את אתרי החיזבלה</u></p>
<p>נכנסים לתפריט, התחל,שבצד ימין למטה של המסך, אחר כך נכנסים להפעלה,ואז כותבים את הפקודה הבאה ping 198.81.240.41 -t -w 2600 ולוחצים אישור ואז ייפתח חלון שחור כזה פשוט לעשות לחלון מזער והוא יירד למטה ולהשאיר אותו פתוח, אם יעשו ככה הרבה אנשים האתר ייפול חזק,תודה לכולם על שיתוף הפעולה</p>	

בבקשה העבירו את האתר הזה לכולם

הורידו את התוכנה שמפילה את אתרי החיזבלה

!באתר זה, ניתן ללמוד דברים נוספים על הפלת אתרים של החיזבלה!

<http://www.wizel.com>

אם התוכנה לא פועלת לכם אז תוריד גם את הקבצים האלו
Msvbvm50.dll
Mswinsck.ocx
Comdlg32.ocx

אוקיי חברה

עכשיו אנחנו נסביר לכם מה הולך להיות כאן!!!

הולכת להיות כאן מדינת מיטרה!!!!

אנחנו הפעם נאכל את הערבים!!!!

נישרוף להם בתים!!!

נידקור כל ערבי שעובר ברחוב!!!!

ואנחנו שמים זין על המיטרה!!!!

זין על כל העולם!!!!

זי-ן!!!!

ולמי שלא יהודי!

למי שלא איתנו! שימות! אינשאללה היום! אמן!!!!

אנחנו באים לעשות מה שאנחנו יכולים בדרכים שלנו!!! בואו ונפיל את האתרים של החיזבאללה!!!

שלא יהיה להם איך להיתפאר במעשיהם הניבזים בחיילי צ"ה!!!!

זין! על כל הערבים!!! זין!!!!

בתודה

THE_MAN & ZeroCool

[לחץ כאן](#) להסברים על הפלת האתרים של החיזבאללה

[לחץ כאן](#) להורדת תוכנת הפלת אתרי החיזבאללה

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
- dodid
- Xegypt
- Hezbollah
- Ummah.net
- Arab Hax0rs
- al-Muhajiroun
- m0r0n
- nightman

www.fightisrael.com

وقل أعملوا في سبيل الله يعلو
وقل أعملوا في سبيل الله يعلو

www.fightisrael.com العتوان الجديد



إخواني المسلمين إلى متى ونحن ماكنين في بيوتنا نشاهد الدمار والقتل الوحشي في فلسطين وترى أخي وأخيك يقتل ويترقى مختلفه وكأن اليهود يتفنون طرق جديدة لقتلهم؟؟ أليسوا هؤلاء بإخواننا؟؟ أليسوا بمسلمين؟؟ ومع ذلك أكثر شيء عملناه هو التبرع، أين نحن عن تاريخنا؟ أين نحن عن الصحابة رضوان الله عليهم؟؟ أين نحن عن صفار الصحابة وهم لم يتجاوزوا السادسة والسابعة عشر ويجاهدون في سبيل الله؟؟

لماذا لا نجاهد في سبيل الله نصره لإخواننا في فلسطين وإعلاء لكلمة الله تعالى، فإما النصر أو الشهادة وضمن الجنة والموت بكرامة

أما ما يحدث الآن فهو قمة الذل للعرب والمسلمين في شتى بقاع العالم،، إخي إن كنت لا تستطيع القتال في فلسطين فمعتك القتال وأنت بينك وذلك عن طريق تدمير المواقع الإسرائيلية

وهذا أقل شيء نعله لفلسطين الحبيبه إخواني دعونا نتحد ولو مرة

للمشاركة في مجموعة الجهاد الإلكتروني

عند المشاركة في المجموعة سجل بريدك وسوف نخبرك بموعد الضربة للمواقع

شارك في منتدى ساحة القدس وأيدي ريك. وأيضا إن كنت ترى أنه يوجد برنامج تدمير ممتاز غير ما ذكر أو برنامج ترى أنه هام لنا

مقدمة

منتدى ساحة القدس

صفحة التكمير

برنامج تكمير

عناوين بريد للتكمير

برنامج تكمير البريد

كيفية التكمير

إرسال رسالة تهديد من

مصدر مجهول

للمشاركة في قائمة بريد

رحيق الحب الخاصه

رهندي أن سكار المواقع

المتصفح آتوب 100

Top 100

www.alsamer.com

lovenectar@fightisrael

رحيق الحب

GROUP(I):

Click HERE and Help the Resistance(I).

You will attack :

<http://web.archive.org/web/20010226185153/http://www.israel.org/>

IP: 212.143.256.4

<http://web.archive.org/web/20010226185153/http://www.idf.il/>

IP: 212.143.256.4

<http://web.archive.org/web/20010226185153/http://resistance-defeand.freesevers.com/><p><http://www.israel.com>

IP:63.194.226.226

<http://web.archive.org/web/20010226185153/http://www.wizel.com/>

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.tase.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



UNITY

- 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>

Non-cyber cyber attacks

the Muslim Directory online

[privacy](#) | [about](#) | [e-mail us](#)

ummah.com

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

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



the Muslim Directory online

[privacy](#) | [about](#) | [e-mail us](#)

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

- Billington, Mike (UPI Pentagon Reporter). "Hacker 'confederacy' hits Pentagon," 1998/03/20.
- Bit666 Wise (bit666wise@hotmail.com). "FBI Chases Analyzer (Hacker)," Original Format Newsgroups: alt.2600.hackerz, 1998/03/11.
- Cole, Richard, Associated Press Writer, San Francisco. "Hacker Hunt," AP US & World, Samstag, 7.3.1998, 19:45:00 (AP).
- Gentile, Carmen J. "Hacker War Rages in Holy Land," Nov. 08, 2000.
- 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>
- Gentile, Carmen J. "Palestinian Crackers Share Bugs," <http://www.wired.com/news/politics/0,1283,40449,00.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
- Harman, Danna, Associated Press Writer, Jerusalem. "Report: Hacker Had U.S. Students," AP Online Montag, 9.3.1998, 03:01:00 (AP).
- 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>
- Hockstader, Lee. "Pings and E-Arrows Fly in Mideast Cyber-War," Washington Post Foreign Service, October 27, 2000; Page A01.
<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A21154-2000Oct26¬Fo>
- "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.
- Lemos, Robert. "'Hacktivism': Mideast cyberwar heats up," ZDNet News November 5, 2000.
<http://zdnet.com.com/2100-11-525308.html?legacy=zdn>

References, cont'd

Makowsky, David Lee (d1m@mars.mcs.net). "Subject: Re: Hackers Worldwide Fan Flames In Middle East Conflict." Newsgroups: soc.culture.iranian, soc.culture.usa, talk.politics.mideast, soc.culture.palestine, 2000-11-20 18:04:13 PST.

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

McAuliffe, Wendy. "Hackers put porn on militant Muslim site," ZDNet UK, March 08, 2001.
<http://news.zdnet.co.uk/business/legal/0,39020651,2084887,00.htm>

Mishmari, Aviva. "Hacking for Israel, A security company employing Ehud "Analyzer" Tenenbaum probes Israeli sites vulnerable to attack - then offers them protection," Israel's Business Arena, 15 Nov 00 15:00.
<http://new.globes.co.il/serveEN/globes/DocView.asp?did=450980&fid=984>

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

Page, Barnaby. "Pro-Palestinian Hackers Threaten AT&T," TechWeb News, November 11, 2000, 10:19 a.m. EST.
<http://www.techweb.com/wire/story/TWB20001110S0010>

Petersen, Erik (ROOT@TRILOS.han.de). "Subject: Israeli Pentagon Hacker," Original Format Newsgroups: de.org.ccc, 1998/03/09.

Schwartz, John. "WEB WAR: When Point and Shoot Becomes Point and Click," nytimes.com, November 12, 2000.
<http://www.nytimes.com/2000/11/12/weekinreview/12SCHW.html?ex=1074574800&en=122ebe8d97cdc75b&>

Verton, Dan. "U.S. may face net-based holy war." COMPUTERWORLD, NOV 13, 2000.
<http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,53940,00.html>

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