Information Security’s Third Wave

Eli Jellenc
International Intelligence Director

ejellenc@idifense.com
Overview

+ Cyber security will never be the same…

+ Theories of Cyber War and its Problems

+ Cyberwarfare in Practice: Russia, Estonia, and Georgia

+ Regional Trends

+ Conclusions
“Little changes can have big effects; when small numbers of people start behaving differently, that behavior can ripple outward until a critical mass or ‘tipping point’ is reached, changing the world.”

Malcom Gladwell’s “Tipping Point”
Strategic Hacking: A New Era

+ Cyber security is now in the top 5 national security priorities of most great powers and many middle powers

+ Defense is not enough; major players are developing the offense

+ Private sector defense contractors are going on the offensive; underground elements are often employed as well

+ Everyone is attacking everyone else, even allies vs. allies

+ 2 likely scenarios: chaos or severe restriction
Everyone Attacks Everyone Else

+ UK Army Intelligence Report (Daily Telegraph; February 8, 2009)
  - “Security sources have revealed that the list of foreign agencies operating within the UK includes Iran, Syria, North Korea and Serbia…”
  - “…and some members of the European Union, such as France and Germany”

+ Germany: penetrated over 30 nations’ government systems by 2009
  - Source: Der Spiegel, March, 2009

+ Israel vs. Most of the Middle East

+ Fatah vs. Hamas

+ China
  - NOT just the official level
  - Chinese amateur crackers attack official systems and defense contractors
  - Foreign governments and private contractors fight back

+ Russia attacks everyone…no surprise

+ Myanmar (seriously, MYANMAR!!)
  - 2007 attacks against Irrawaddy.com
  - Using Russian criminal malware
Offense Becomes More Attractive

+ All of the major US Defense Contractors are developing defensive and offensive “cyber solutions” offerings

+ "One of the reasons we're looking at a Cyber Command is to unify all aspects of cyber defense, so that you don't separate out offense, defense, intelligence, so that all of the various aspects work together," (Dep. Secretary of Defense William Lynn, VoA News, June 15, 2009)

+ The UK’s GCHQ is looking for “naughty boys” to conduct offensive (and defensive) operations (Lord West, in The Register, June 29, 2009)
Emerging Models of Cyber Conflict

+ Centralized Model:
  - Authorized institutions
  - Working in secret
  - Big budgets

+ Decentralized Model
  - Uses Underground
  - Working with “open secrets”
  - Lower budgets

+ Internally Focused
  - Highly Defensive
  - Highly Restrictive

+ In Reality: most are hybrids
Regional Trends - Russia

- Justified Self Assertion
- New Nationalism
- Cyber War / Hactivism is a Reality
- Cyber Crime
2008: Cyber War Becomes Reality

Increasing Nationalism

Cyber Criminals = Strategic Asset

The state wields cyber attack expertise for domestic and international advantage

Political Dispute with Russia? – Expect Cyber Harassment
Regional Trends - China

- Cyber Espionage
- Cyber Crime
- Cyber Sabotage
- Cyber Militias
China: Net Militias
China’s Net Militias
China’s Dirty Secrets

+ They are just as vulnerable as everyone else... in some ways, more so.

+ Chinese vs. Chinese attacks are rampant, almost as common as external attacks
  - Rival data centers
  - Rival departments within the same company

+ Corruption makes many organizations more vulnerable...

+ “The state” is not a monolith... there are rivalries within
Regional Trends – Greater Middle East

Secular Hacking

Ideological Hacking

Religiously Motivated Hacking

Fatwa Justification

Contracted Hacking
2008 Headlines: Middle East Fatwas Justify Cyber Fraud

Defend Islam against Internet based defamations

Cyber fraud is legitimate fund raising

Prediction: Middle East - Threat Region - Cyber Fraud

Sheikh Al-Tantawi

Al-Azhar University
Fatwa Committee
Jihadists and Cyber Cartels: Moving Closer?
Cyber Revolution in Iran: Ongoing

+ Government uses service deactivation and monitoring to disrupt opposition communications

+ Opposition uses DDoS attacks and twitter to spread dissident messages

+ Pro-opposition Hacker Group “209,” Organizing and Coordinating its Hacking Campaigns through Twitter (Right)
Regional Trends – Brazil

2008 Proof of Concept: Hacks Change Data of Brazilian Ministry of Natural Resources Management

Result: millions of Reais in illegal logging
Catalyst: Bullet Proof Hosting

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Madet Ltd.</td>
<td>Russia</td>
</tr>
<tr>
<td>STARLINE_EE</td>
<td>Estonia</td>
</tr>
<tr>
<td>UATELECOM</td>
<td>Ukraine</td>
</tr>
<tr>
<td>UrkTeleGroup</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Colocall Ltd.</td>
<td>Ukraine</td>
</tr>
<tr>
<td>HopOne</td>
<td>USA</td>
</tr>
<tr>
<td>Net Access</td>
<td>USA</td>
</tr>
<tr>
<td>ABDAllah</td>
<td>Turkey</td>
</tr>
<tr>
<td>Hostfresh</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>TIMETELECOM</td>
<td>Malaysia</td>
</tr>
<tr>
<td>TMNET-BORNEO</td>
<td>Malaysia</td>
</tr>
<tr>
<td>MALAYSIA BERHAD</td>
<td>Malaysia</td>
</tr>
<tr>
<td>PRIADIUS NET</td>
<td>Malaysia</td>
</tr>
<tr>
<td>Applied Info Mgt</td>
<td>Malaysia</td>
</tr>
<tr>
<td>Starhub Internet</td>
<td>Singapore</td>
</tr>
</tbody>
</table>

Published in 2002

Press Exposure Kills: RBN, McColo, Intercage
Disruptor/Catalyst: Splintered Internet

Top Level Domains

International Domains
Catalyst: Evolving FastFlux, DoubleFlux, MetaFlux

Manipulates DNS

Distributed Botnets

Practically Untraceable

Permanent Malicious Infrastructure

Better than Bullet Proof Hosting

Asprox – OlateSuite - Storm
Why is Progress Elusive?

+ Conflicting Interests…turf wars…

+ Lack of conceptual clarity…almost no consensus among the expert communities

+ Foundational Theories are absent or poorly formed
Theories of Cyber Warfare

+ Until 2007, there was no empirical evidence of cyber conflict…only secretive examples of cyber espionage

+ Now, we have examples, and everything is much different than most theorists supposed

+ 2 biggest conceptual (and empirical) problems:
  - Deterrence
  - The Security Dilemma
Theories of Cyber Warfare: Deterrence

+ Basic premise: if you can’t defend, threaten to attack in response
+ Model of nuclear deterrence in the Cold War

+ Many theorists think that this concept is useful for cyber warfare:

+ IT IS NOT!
Theories of Cyber Warfare: Deterrence

+ Deterrence requires:
  - Capacity to impose pain on adversary
  - Credible threat to be able to impose pain
  - Ability to absorb first attack and respond
  - Ability to respond in variable way
  - Ability to identify attacker

+ With cyber attacks, many of these are not present
  - Difficult to identify attacker
  - Others can pose as attacker
  - Damage assessment is unclear
  - No guarantee that attack will not also hurt others
Theories of Cyber Warfare: The Security Dilemma

+ Basic premise: Efforts to increase your own security makes other insecure

+ With Cyber Warfare:
  - Everyone can attack easier than they can defend
  - Sometimes, defense and attack are difficult to distinguish
  - Most countries are talking more about offense
  - Private sector and underground are doing offense

+ Results:
  - Spiral of Mistrust
  - Incentives to go on the offense
## The Security Dilemma: Game Theory Foundation

<table>
<thead>
<tr>
<th>Player 1</th>
<th>Player 2</th>
<th>Hold</th>
<th>Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold</td>
<td>Hold</td>
<td>(1) Low Threat ; (2) Low Threat</td>
<td>(1) Exploited ; (2) Dominant</td>
</tr>
<tr>
<td>Attack</td>
<td>Attack</td>
<td>(1) Dominant ; (2) Exploited</td>
<td>(1) Arms Race ; (2) Arms Race</td>
</tr>
</tbody>
</table>
The Realities of Cyber Conflict

+ Nothing like the theorists though it would be

+ Messy…not entirely controllable

+ No understanding of ultimate consequences…interconnected networks yield extensive feedback

+ Symbolic effects are often as important as direct effects
Russian Attacks Against Estonia: May 2007

“Web Watch: Estonian Disgrace!”

Hacked from RUSSIAN HACKERS (thx to ZyklonTeam, S-Teals, Web-Hack)

Our Honour  Our Freedom  Our Victory ...
Russian DDoS Coordination

+ Organized on Blogs (e.g. antichat.ru, Livejournal)
+ New Attack lists circulated among hundreds of blogs in minutes
+ Highly coordinated
+ Hundreds of attackers
+ Many identified as ordinary people
Russian DDoS Attack Tool: Sprut
Effects on Estonia

+ Major disruption to government websites and e-government services

+ Varying disruption to financial institutions
  ▪ Some banks shut down for 1 day or more
  ▪ Most banks have problems for several hours
  ▪ ATMs disrupted

+ No real response plan in Estonia, but with NATO assistance, they handled it well

+ Problem: nothing could have prevented the attacks completely
Russia vs. Georgia: August, 2008

+ Presaged by more robust equipment installation in Georgia

+ Unlike Estonia, Georgia fought back

+ Both sides attack the other’s media sites

+ Russia completely shuts off Georgian government’s web space

+ Georgia began hosting some sites on Blogger.com pages:
  ▪ Why?
  ▪ Because Russia can take down a country, but it can’t stop Google.
Russia Takes Down Georgian Government Sites

Ossetia.exe: Novice DDoS tool
+ Russian Underground Claims Responsibility:

+ Stopgeorgia.ru
Russia Also Deactivated Cables

 Courtesy of Arbor Networks
Kyrgyzstan: January, 2009

Border Gate Protocol Map of DDoS Attacks Against Kyrgyz Opposition Sites
Cyber Security Becomes a Public Affair

+ More offense:
  - Hints of a more offense-heavy strategy in new Administration’s proto-policy

+ Law Enforcement, Contractors and Consultants already doing so or are planning to
  - Definitely pragmatic, but offense is a dangerous default

+ What deterrence?
  - Attacker Origin?
  - Second-order effects?
  - Damage Assessment?

+ Increased Budgets = Dramatic Shift in Industry Priorities
What does this mean for Policy?

+ Is a cyberczar a good idea?
  ▪ In the US?
  ▪ The EU?

+ What is “the cyber infrastructure”?
  ▪ Is it even realistic to think we can secure it all?
  ▪ What international legal problems does this raise?
  ▪ Do the obligations it imposes outweigh the benefits?

+ Is more offense a good idea?
  ▪ Alternative— trapped defense
  ▪ Alternative— collective defense

+ Do we even know how to spend $6 billion? Who will do it?

+ Where are the diplomats and the treaties?
What does this all mean?

+ The late 1980s and early 1990s: the age of the pure hacker

+ Late 1990s and early 2000s: the age of the cyber criminal

+ Now...

+ The age of political and strategic information operations...up to and including war
What does this all mean?

+ If you thought the worms of the 1990s were bad…

+ If you thought RBN and Rockphish and Conficker were bad…

+ Just wait…

+ Wait until you see what political and strategic organizations with billions of dollars, and incentives for offensive strategies, will do…
Thank You