Cyberwar: You’re Doing it Wrong!
The relationship between four threats in the 21st Century

Marcus J. Ranum
CSO, Tenable Network Security, Inc
Who am I?

- Author of “The Myth of Homeland Security”
- Industry “insider” with 20+ years work in security
  - System designer
  - Teacher
  - Manager of coders
  - CTO, CSO, CEO
What is this talk about?

- Some questions:
  - Does putting “cyber-” in front of something automatically mean it’s new, different, or interesting?
  - What are the different “battlefield doctrines” of attack and defense in each of these focus areas:
    - Cyberwar / Cybercrime
    - Cyberterror / Cyberespionage
How we will proceed

- First, we will analyze our focus areas
- Secondly, we will examine the properties of attack and defense in each of those areas
- Thirdly, we will consider positive/negative overlaps or synergies between attack and defense
- Finally, we will conclude with some recommendations
Cybercriminal

- Agenda:
  - Diffuse and profit-driven
  - Tactical: short-term

- The threat:
  - Profitably “hit and run”
  - Cannot eradicate: more will take their place
  - Creative
  - Rapidly shift to where the money is
Cyber Spy

- Agenda:
  - Surreptitiously get secrets from target
  - Suborn and manage trusted agents in critical positions
  - Strategic: long-term

- The threat:
  - The cyber-era simplifies some technical aspects of espionage a bit while complicating others a bit
Cyberterrorist

- Agenda:
  - Ideological maximum-damage maximum-profile highly visible attacks with no restraint
  - Tactical: “Hit and run” to Cause Fear

- The threat:
  - Targets will be critical infrastructure that results in explosions, destruction and death
    - Power, water, oil, shipping, vehicle control
Cyberwarrior

- Agenda:
  - Be prepared to attack/degrade/penetrate enemy command and control systems as an adjunct to physical military operations
  - Strategic: Long-term covert warfare

- The threat:
  - Targets will be high-value, high-cost, and will have varying “hardness” against attack
Agenda Alignment

- Cybercriminal: Tactical Profit
- Cyberspy: Strategic Surreptitious
- Cyberterrorist: Tactical Maximum-profile
- Cyberwarrior: Strategic Destructive
# Agenda Mis-Alignment

<table>
<thead>
<tr>
<th></th>
<th>Cybercriminal</th>
<th>Cyberspy</th>
<th>Cyberterrorist</th>
<th>Cyberwarrior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercriminal</td>
<td>Compete</td>
<td>Provide cover</td>
<td>Provide cover</td>
<td>Provide cover</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interfere with ops</td>
<td>May provide tech</td>
<td>Interfere with ops</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyberspy</td>
<td>No effect</td>
<td>No effect Counterintelligence</td>
<td>May detect</td>
<td>May compromise ops</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyberterrorist</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyberwarrior</td>
<td>No effect</td>
<td>May interfere with ops during a conflict</td>
<td>No effect</td>
<td>Direct engagement during a conflict</td>
</tr>
</tbody>
</table>

Cybercriminal

Cyberspy

Cyberterrorist

Cyberwarrior
Some Things

- Some things jump out at us immediately, namely:
  - Cybercriminals and Cyberterrorists operational needs are isolated; therefore they will tend to be very robust.
  - Cyberspies and cyberwarriors operational needs are overlapped; therefore they need to coordinate carefully to prevent “cyber friendly fire incidents.”
A Mis-Alignment Scenario

- It’s cyber-attack day, H hour, and we’re in the war-room
  - The order to attack is given
  - The cyberattack teams take down the enemy’s command and control systems
  - Out cyberspy force is now blinded and unable to communicate
- This can be avoided; but: cyberwarriors must coordinate with cyberspies
Another Mis-Alignment Scenario

- It’s cyber-attack day, H minus 10 hours
  - Because of cybercriminal activity the target performs a crucial security update
  - The update also happens to disable, expose, or compromise the impending cyberattack
- This can be avoided, also, but with increased logistical costs for the attacker at no additional cost to the defender
  - Balance of opportunity favors defender
## Defense Strategies

<table>
<thead>
<tr>
<th></th>
<th>Response, by target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Government</td>
</tr>
<tr>
<td><strong>Cybercriminal</strong></td>
<td>“typical computer security” (firewalls, antivirus, patch management, IDS, system log analysis)</td>
</tr>
</tbody>
</table>
| **Cyberspy**      | **Counterintelligence +**
                     | “typical computer security” | Expect the government to deal with it |
| **Cyberterrorist**| “typical computer security” | “typical computer security” |
| **Cyberwarrior**  | **Counterintelligence +**
                     | “typical computer security” | Expect the government to deal with it for anything beyond “typical computer security” |
Some Things

Some things jump out at us immediately, namely:

- Defensive approaches almost entirely overlap; what helps protect the target from cybercrime is likely to help protect the target.
- The only other thing that can usefully be thrown at the problem is counterintelligence:
  - There aren’t any super cool government-specific defensive technologies for cybersecurity; they’d already be part of “normal internet security”.
Overlap of Attack and Defense

- By definition:
  - cyberespionage and cyberwar tools will need to be different from the “run of the mill” attack tools being used by cybercriminals and hackers
    - Because, otherwise, a security fix (and there is a constant stream of them!) designed to fix one of the “run of the mill” problems could disable an entire cyberespionage or cyberwar effort
    - Realistically that is not the case; but it raises the question of logistics and life-span of cyberweapons
Overlap of Attack and Defense - II

Therefore:

- It stands to reason that counterintelligence would be one of the most valuable tools for mooting an enemy’s specialized cyberweapons.
- Additionally, since the weapons almost certainly have to be pre-fielded against the target, they are subject to identification, analysis, and dissection.
Conclusions I

- There is insufficient intellectual gap between cyberwarfare and cyberespionage
  - They are nearly the same thing, just fulfilling two different purposes, tactical versus strategic
- Treat them as the same thing!
  - Counterintelligence is the defense in both cases
  - Effective counterintelligence can render the enemy’s weapons inert
Conclusions II

- Due to the logistical problem of maintaining secured, fielded, cyberweapons in place, or up-to-date, I seriously question the utility of rapid deployment offensive cyberwarfare

- The utility of strategic intelligence and counter-intelligence is disproportionately increased

- Targeted cyberwarfare (like Stuxnet) may be practical but will take as long or longer to field against a given target than “boots on the ground”
Summary

- Spies are the key maneuver element of 4th generation warfare - not warriors
  - They are how you get into your enemy’s decision process
- Maintain vigilance using “typical internet security” techniques
  - Counterintelligence should include cyberespionage as a critical hit-point
- Not much has changed, really, that is not a consequence of shift to new technologies