The Technology of Cyber Operations

Herb Lin
Symposium on Cyber Operations and National Security
Dartmouth College
October 20, 2011
The one slide version of cyber (security) policy

• We depend on IT for military and civilian purposes.

• Important IT functionality and information must be protected.

• Defensive cybersecurity (highly publicized but inadequate)
  – Passive defenses
  – Law enforcement

• Offensive cybersecurity (rarely discussed in public by government officials)
  – Recent DOD “strategy for cyberspace” does not acknowledge role of offensive operations.

• Offensive cyber operations can also have non-defensive purposes
  – e.g., cyberattack to achieve military or political goal (Stuxnet?)

• Defensive cybersecurity focuses on countering offensive operations
Technology of offensive operations

• Elements of a offensive operation
  – Access: how to get at the network/system of interest (computers *must* interact with the outside world to be useful)
  – Vulnerability: weakness that attacker can take advantage of
  – Payload: what the attacker wants to do

• Aggressors use both technical and social means

• Access
  – Remote
    • Denial of service attack
    • Virus/worm over the internet
    • Malware on Web page
  – Close-access (e.g., through chip swap, USB key, supply chain)
## Vulnerabilities and access points

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Access points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Users and operators</td>
</tr>
<tr>
<td>Hardware</td>
<td>Manufacturers</td>
</tr>
<tr>
<td>Communications channels (e.g., unencrypted channel)</td>
<td>Communications channels (e.g., Web browser, undocumented Wifi, undocumented modem)</td>
</tr>
<tr>
<td>System configuration</td>
<td>Service providers</td>
</tr>
<tr>
<td></td>
<td>Moles inside a plant</td>
</tr>
</tbody>
</table>
Payloads for offensive cyber operations

• Cyberattack (degrade, disrupt, destroy, deny system/network or information therein)
  – Integrity (data/operations are altered)
    • Botnet, self-destruct, change data
  – Authenticity (data/operations are forged)
  – Availability (data/operations is inaccessible)

• Cyberexploitation (surreptitiously obtain confidential information)

• Both use same technical means—gain access, take advantage of vulnerability. To victim (and to news media), attack and exploitation look the same.
Key characteristics

• The indirect effects of cyberattacks are almost always more consequential than the direct effects of the attack – “indirect” does not mean “not primary”
  − Effects can span an enormous range; cyberattack is a methodology, not a specific weapon per se.
  − A cyberattack is NOT of lesser consequence because it targets “only” a computer.
  − Cyber operations can undermine confidence as well as technology and data.
  − Effects may be significantly delayed in time from moment of insertion.

• Offensive operations can be conducted with plausible deniability
  − But adversaries make mistakes too, and all-source intelligence helps

• Offensive technology is relatively inexpensive, easy to obtain;
  − Many nonstate actors (companies, patriotic hackers, criminals, terrorists) can have influence and may be able to cause some of the same kinds of effects as state actors.

• A poor attacker often has significant leverage, by
  − stealing computing and financial resources;
  − using automation to reduce personnel needed and increase tempo.
Key characteristics (continued)

• Cyber operations can be selective or broad in targeting.
  – Selectivity implies long lead time, complex intelligence requirements, specialized skills, higher cost

• Cyber operations (especially attacks) can be very complex to plan and execute.
  – Larger range of options than most traditional military operations
  – Time and spatial scales can span many orders of magnitude
  – Success depends heavily on good, detailed, timely intelligence
    – Small details of configuration matter a lot and can change easily
  – Cascading effects hard to predict.
  – Collateral damage hard to estimate
  – Damage assessment hard to perform
Some operational considerations

• A cyberattack may be
  – Usable only once or a few times
  – Limited temporally in effect
  – Limited in scope (e.g., if highly targeted)
  – Hard to execute on the fly
  – Technically fast but operationally slow; hence most suitable in non-time-urgent operational scenarios (e.g., early use); “speed of light” vs “speed of law/thought/analysis”
Using offensive operations for defensive purposes (illustrative)

• Before adversary attack
  – Early warning of attack means living inside adversary network
  – May need to pre-empt offensive cyber action about to be undertaken by adversary

• During adversary attack (the announced case for US policy)
  – Disrupt ongoing cyberattack by disabling attacking computers

• After adversary attack
  – Conduct forensic investigation that may require multiple intrusions into proximate and intermediate nodes.
  – Retaliation a possibility to discourage further attacks.
Using offensive operations for non-defensive purposes (illustrative)

• Traditional military operations
  – Suppression of adversary air defenses.
  – Degrade electrical power supporting adversary war-making capacity.

• Covert action
  – Influencing the outcome of a foreign election using electronic voting machines.
  – Disruption of adversary R&D or production of WMD

• Cyberexploitation
  – Exfiltration of negotiating positions, political plans, commercial information.
Some observations

• Many possible forms of offensive operations have not yet been seen ➔ future of conflict in cyberspace may be very different.

• Stuxnet is wake-up call for policy makers but not for technical community. Stuxnet approach is broadly applicable; Stuxnet code is not.

• The deterrence/defense paradox in cyberspace:
  • Defense is too hard, so we need to explore deterrence.
  • Deterrence is too hard, so we need to do better defense.

• Many forces driving towards offensive operations for non-defensive purposes:
  − Don’t know how to protect IT
  − Don’t know how to deter attacks on IT
  − Offensive operations not useful for defending your own IT assets
  − What’s left?

• Cyber conflict is not separate from other spheres of potential conflict—wide range of options for responding to cyberattack: changes in defensive postures, economic and/or law enforcement actions, diplomacy, cyberattacks, and kinetic attacks.

• Secrecy clouds necessary public discussion.
Macarthur foundation, cyberattack, policy

NRC, deterring cyberattacks
For more information…

Herb Lin
Chief Scientist, Computer Science and Telecommunications Board
National Research Council

202-334-3191
hlin@nas.edu
www.cstb.org