Cyberwarfare: Characteristics and challenges

By Tom Olzak
June 25, 2013, 5:45 AM PDT

Takeaway: The specter of cyberwarfare isn’t just a problem for governments — many types of organizations could be in the line of fire. Knowing the types of attacks and their probability will help you prepare.

Journalists, business executives, and government bureaucrats like to use the term “cyberwarfare” when it suits their needs: especially when an organization loses intellectual property through an advanced persistent threat. A warfare claim is often accompanied by the victim organization’s claims that it was helpless in the face of state- or crime organization-sponsored espionage, theft, or denial of service. Many managers believe the government should do more. While there are things the federal government can do, each organization is responsible for implementing basic prevention, detection, and response controls to deal with inevitable breach attempts.

In this first installment of a two-part series, we’ll examine the characteristics of cyberspace that enable the growing number of cyberwarfare events. In addition, we’ll explore the various types of warfare-related attacks as well as underlying motives, tools, and techniques. Part two develops a cyberwarfare defense using existing standards of best practice.

Cyberspace

Unlike physical space, cyberspace is a manmade landscape of interconnected devices and networks. Organizations must connect, and remain connected, to this Internet in order to compete in today’s markets. However, consistent governance does not apply across all geographic Internet presences. Lior Tabansky, a Neubauer research associate working on the Cyber Warfare Program at INSS, writes,

“Much of cyberspace is organized and managed by private and cooperative organizations without state or geographical overlap. The internet [sic], which is a central and growing component in this space, is built in a decentralized manner. The ideology of the internet’s creators and its leading thinkers is opposed to any type of state management” (p. 78).

Lack of governance is only one challenge facing connected businesses and government agencies. For years, relatively inexpensive tools have enabled almost anyone with a little computer knowledge to circumvent prevention controls, given enough time. Many tools, used by both white hat and black hat hackers, are free (e.g., Live Hacking). Others, like Metasploit, are intended for the professional cybercriminal and penetration tester. Finally, nation-sponsored intrusions often make use of proprietary tools and techniques designed specifically for a planned or ongoing attack.

Cyberspace itself lacks governance and control. This exposes the perimeters and internal systems (especially end-user) to a wide variety of threats. Table A, based on Tabansky’s work, lists cyberspace characteristics and associated vulnerabilities.

Table A
Cyberwarfare

The emergence of cyberspace adds an additional dimension to warfare: with and without clashes of traditional troops and machines of war. Cyberwarfare is often defined as major disruptions to critical infrastructure. However, this is the least likely outcome. Attacking a nation via the Internet will have extreme consequences to the attacker as well as collateral global damage. No nation—including both public and private infrastructure—is immune from attack.

Cyberwarfare occurs continuously across cyberspace connections, resulting in minor disruptions, website defacement, theft of national defense information, and intellectual property theft. As Michael Riley and Ben Elgen write in *China’s Cyberspies Outwit Model for Bond’s Q*, China is one country that is actively invading U.S. infrastructure, stealing defense secrets, and walking away with industrial technology useful in narrowing industrial and military gaps. According to *The Economist*, “Some experts believe that such thefts have cost hundreds of billions of dollars in stolen R&D” (para. 2). While some of this is simply related to criminal activity, much of it is attributable to nation-sponsored espionage.

A country or group does not need a strong military or economy to wage warfare against industrial powers. Sreeram Chaulia writes in *Cyber warfare is the new threat to the global order*, “Cyber war capacities are not the domain of only big guns like China and the U.S. They are spreading horizontally to middle and even minor powers” (para. 5).

Anyone with the right tools and legal/political environment can launch attacks against large or small targets, regardless of how may guns and tanks the objective has. Table B lists several characteristics of current cyber threats.

**Table B**

<table>
<thead>
<tr>
<th><strong>Characteristic</strong></th>
<th><strong>Potential Vulnerabilities</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid pace of change</td>
<td>Management of controls requires continuous vigilance over the changing threat landscape.</td>
</tr>
<tr>
<td>Rapid reduction in price and wide scale use of commercial, off-the-shelf equipment</td>
<td>Low cost of attacks allows anyone or any state to initiate attacks.</td>
</tr>
<tr>
<td>Structure of TCP/IP protocol</td>
<td>Difficult to identify the source of an attack for law enforcement or counter attack purposes.</td>
</tr>
<tr>
<td>High level of complexity</td>
<td>Anomalous network or system activity often resembles a technology issue rather than attack behavior.</td>
</tr>
<tr>
<td>Asymmetry</td>
<td>Attacks can come from anywhere: and they do. Defence must take this into account, with prevention, detection, and response controls in place for all data/control channels on all attack surfaces</td>
</tr>
<tr>
<td>Vague laws</td>
<td>Cyberwarfare is not consistently defined across all national borders. Further, many countries have no laws against it, do not enforce them, or are themselves the sponsors of attack teams.</td>
</tr>
</tbody>
</table>
Government’s role in defense

The U.S. has been very slow to react to cyberwarfare threats. Although the military is taking steps to shore up its controls, private and public organizations are not moving to properly protect themselves. The Sarbanes-Oxley and the Gramm-Leach-Bliley Acts, for example, do little to protect publicly traded companies and financial institutions from cyber attack. While protecting data integrity and customer privacy, they fall short in providing mandates for preventing, detecting, and responding to known and future nation-sponsored advanced persistent threats. Congress doesn’t seem to be able to make this situation any better.

The Cyber Security Act of 2012 died as Congressional leaders waged their own internal ideological warfare regarding challenges like the fiscal destruction brought on by government policy (Experian). President Obama has made an attempt to shore up this gap with Presidential Policy Directive 20 (PPD 20).

PPD 20 instructs the military to take steps to identify attackers and take offensive or other relevant action against them: according to risk. However, it does little to require the government to review private and public infrastructure and assist organizations in their efforts to mount a cyber defense. This begs the question whether offense or defense is the best way to protect against attack.

Offense vs. defense

PPD 20 appears to favor offensive actions as a deterrent. This requires identification of attack sources and a willingness to attack infrastructure of countries like Russia and China. Emilio Iasiello writes in Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills, “No standard methodology exists today for establishing a degree of confidence in determining cyber-attribution. The defender must be able to identify the perpetrator for an appropriate response action” (Para. 5)

Even if a military identifies the attack source, will its government have the political will to take offensive action if the source is China, Russia, or North Korea? Will the public be willing...
to withstand the damaging effects of a response against a national infrastructure not ready to quickly react to a series of back-and-forth attacks in the name of deterrence? Not likely…

A strong defense must be the first step in dealing with cyberwarfare. This is the topic of Part 2.

Get IT Tips, news, and reviews delivered directly to your inbox by subscribing to TechRepublic’s free newsletters.