Discussion 2: Cyberwarfare

I think the big question of cyberwarfare is when does it amount to war? There is need to determine whether cyber attacks should be considered acts of war, or whether they are better understood as criminality, espionage, or sabotage etc., are hampered by our loose understanding of what war itself amounts to. More specifically the means of war, whether construed as force or violence, remain under-explored and under-specified by strategic theorists. As a result, these terms are typically used both loosely and interchangeably, undermining their value as conceptual tools in the process. Computer network attacks with direct political and/or military objectives … distinct from cyber espionage, hacking, and crime”.

Security plan consists of security policies. Security policies give specific guidelines for areas of responsibility, and consist of plans that provide steps to take and rules to follow to implement the policies. If well follow aim to help juxtapose and harm to the organization but many time we see that this are not always the case as some security policy become organizational challenges. In some cases when they cause delay or have effect to human right of their victims. See policy limitations. According to Jeffrey Carr, author of "Inside Cyber Warfare," any country can wage cyberwar on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure. For the same reason, non-governmental groups and individuals could also launch cyberwarfare attacks. Carr likens the Internet's enabling potential to that of the handgun, which became known as "the great equalizer." (Danchev, 2012). Therefore Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and criple financial systems -- among many other possibilities. (Rouse, 2010). Risks of this nature are typically excluded from traditional commercial general liability policies. Policies should define what you consider valuable, and should specify what steps should be taken to safeguard those assets. Policies can be drafted in many ways. One example is a general policy of only a few pages that covers most possibilities. Another example is a draft policy for different sets of assets, including e-mail policies, password policies, Internet access policies, and remote access. The policy is a platitude rather than a decision or direction (Benson, 2013).

The rise is subjected to the global demand of software vulnerabilities because it aids attackers to take advantages of the loop holes within the software to create backdoors, therefore, grants them the upper-hand in this cyberwarfare. Government agencies become potential losers in this battle because they are oblivious of the software vulnerabilities inhabited in their network infrastructure. Also, government agencies are not regulated by a law that prohibits this black market, despite the fact that there is a law which prohibits dissemination of software products granting users the power to attack, deny, and disrupt computer infrastructure or networks. Also the policy should not really used by the organization. Instead it is a piece of paper to show to auditors, lawyers, other organizational components, or customers, but it does not affect behavior.

Now must of the national influence on computer protection are enforced as a policy through regulatory bodies to vendors or manufactures of hardware or software. A cyberattack intended to harm the U.S. economy would likely target computers that operate the civilian critical infrastructure and government agencies. However, there is disagreement among some observers about whether a coordinated cyberattack against the U.S. critical infrastructure could be extremely harmful, or even whether computers operating the civilian critical infrastructure actually offer an effective target for furthering terrorists' goals.

Examples of cyberwarfare:

* In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
* In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
* Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
* In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility. (Rouse, 2010).

Another way in which it could this influences an organization’s security offshore outsourcing may give a programmer in a foreign country the chance to secretly insert a Trojan horse or other malicious code into a new commercial software product. GAO reportedly has begun a review of DOD reliance on foreign software development to determine the adequacy of measures intended to reduce these related security risks in commercial software products purchased for military systems. Many major software companies now outsource code development to subcontractors who design and build large portions of COTS products outside the United States (Kaplan, 2003).

One good thing you should know that influences this action is that First and foremost, insurers are afraid of a "cyber-hurricane‟ which is a major disaster resulting in great number of claims. Cyber-hurricanes represent an uncertain risk of very large losses, and as such are very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability. A lack of data also makes cyber- insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance. .

Reference

Benson, Christopher. (2013). Security Planning. http://technet.microsoft.com/en-us/library/cc723503.aspx

Danchev, D. (2012). The current state of the cyber warfare threat' featuring Jeffrey Carr. http://www.zdnet.com/blog/security/q-and-ampa-of-the-week-the-current-state-of-the-cyber-warfare-threat-featuring-jeffrey-carr/12066

Kaplan, D. (2003). Playing Offense: The Inside Story of How U.S. Terrorist Hunters Are Going after Al Qaeda," U.S. News & World Report

Rouse, M. (2010). Cyberwarfare. http://searchsecurity.techtarget.com/definition/cyberwarfare