Chapter XXVIII
Cyber Security Models

Norman F. Schneidewind
Naval Postgraduate School, USA

ABSTRACT

Predictive models for estimating the occurrence of cyber attacks are desperately needed to counteract the growing threat of cyber terrorism. Unfortunately, except to a limited degree, there is no genuine database of attacks, vulnerabilities, consequences, and risks to employ for model development and validation. However, it is still useful to provide definitions, equations, plots, and analyses to answer the "what if" questions concerning potentials attacks. We do this by reasoning about the elements of predictive models and their relationships, which are needed to mirror objects and events in the real world of cyberspace. The application of these models is to provide the user with a vehicle for testing hypotheses about how to respond to a cyber attack before it occurs, using risk, vulnerabilities, time between attacks, and intrusion (number and duration) concepts.

INTRODUCTION

Motivation

We are interested in developing *cyber security prediction models* to serve as a frame work for researchers to develop models of cyber threats and for practitioners to use for input in their decision-making process when responding to cyber terror. We are motivated to develop the models because of the severity of the cyber security problem and the havoc that cyber attacks are wreaking on the world's information infrastructure. The criticality of the cyber threat problem is expressed in excerpts from the following report:

> *The Nation's information technology (IT) infrastructure, still evolving from U.S. technological innovations such as the personal computer and the Internet, today is a vast fabric of computers—from supercomputers to handheld devices—and interconnected networks enabling high-speed communications, information access, advanced computation, transactions, and automated processes relied upon in every sector of society. Because much of this infrastructure connects to the Internet, it embodies the Internet's original attributes of openness, inventiveness, and the assumption of good will.* ("Cyber Security," 2005)

These attributes have made the United States information technology (IT) infrastructure an irresistible target for vandals and criminals worldwide. Members of the President's Information Technology Advisory Committee (PITAC) believe that terrorists will inevitably follow suit, taking advantage of vulnerabilities, including some that the nation has not yet clearly recognized or addressed. The computers that manage critical U.S. facilities, infrastructures, and essential services can be targeted to set off system-wide failures, and these computers frequently are accessible from virtually anywhere in the world via the Internet ("Cyber Security," 2005).

Computing systems control the management of power plants, dams, the North American power grid, air traffic control systems, food and energy distribution, and the financial system, to name only some. The reliance of these sensitive physical installations and processes on the IT infrastructure makes that infrastructure itself critical and in the national interest to safeguard ("Cyber Security," 2005).

Evidence of this problem is contained in the following excerpt from an article in *The Washington Post* (Graham, 2005):

Web sites in China are being used heavily to target computer networks in the Defense Department and other U.S. agencies, successfully breaching hundreds of unclassified networks, according to several U.S. officials. Classified systems have not been compromised, the officials added. But U.S. authorities remain concerned because, as one official said, even seemingly innocuous information, when pulled together from various sources, can yield useful intelligence to an adversary.

It's not just the Defense Department but a wide variety of networks that have been hit,' including the departments of State, Energy and Homeland Security as well as defense contractors, the official said. 'This is an ongoing, organized attempt to siphon off information from our unclassified systems.'

'With the threat of computer intrusions on the rise generally among Internet users, U.S. government officials have made no secret that their systems, like commercial and household ones, are subject to attack. Because the Pentagon has more computers than any other agency—about 5 million worldwide—it is the most exposed to foreign as well as domestic hackers,' the officials said. (p. A1)

It is evident that the potential for cyber attacks is not limited to sources in the United States. For example, Yurcik and Doss (2001) report in their paper *Internet Attacks: A Policy Framework for Rules of Engagement* that there also is concern about foreign sources as well, as articulated in the following testimony:

We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyberwarfare programs in other countries. We have identified several (countries), based on all-source intelligence information that are pursuing government-sponsored offensive cyberprograms. Information Warfare is becoming a strategic alternative for countries that realize that, in conventional military confrontation with the United States, they will not prevail. These countries perceive that cyberattacks launched within or outside of the U.S. represent the kind of asymmetric option they will need to level the playing field during an armed crisis against the U.S. The very same means that the cybervandals used a few weeks ago could also be used on a much more massive scale at the nation-state level to generate truly damaging interruptions to the national economy and infrastructure. (John Serabian, the CIA's information operations issue manager, in testimony before the Joint Economic Committee of Congress 3/4/00)

In the commercial arena, Microsoft, heretofore not noted for the security of its systems, has done an about face and has instituted the following policy: "With the implementation of Trustworthy Computing, security has become the number one priority. Default installations aimed at ease of use are now not always sufficiently secure, but, going forward, security in Microsoft's products will take precedence over ease