IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB9161

Chapter III

Integrating Cooperative Engagement Capability into Network-Centric Information System Security

Alexander D. Korzyk, Sr.
University of Idaho, USA

ABSTRACT

The U.S. military's concept of a Cooperative Engagement Capability should serve as a useful referent for those attempting to design/develop large scale, organization-wide information security systems. This concept involves centralizing command over the entire suite of defensive assets (naval, air, ground) available in some region or locale; whenever a threat is directed against any US force element (a ship, an infantry unit, etc.), this central authority would then be expected to direct the deployment of whatever appears to be the most efficient countermeasure…in light of prospective as well as actual threats. This is a dramatic departure from the traditional decentralized approach, whereby each force element was expected to draw on its own defensive measures to counter any threat directed at it from any source.

Industrial/commercial organizations might draw on the logic of the Cooperative Engagement Capability *logic in devising a system to secure its informational assets.*

INTRODUCTION TO NETWORK-CENTRIC INFORMATION SYSTEM SECURITY

Network-Centric Security

The end of the "Forty Years War," as historians of the 23rd century may note, marked the end of the 20th century Cold War. For 40 years the world lived in the specter of nuclear holocaust or an apocalyptic catastrophe of the magnitude of the Great Flood. The two superpowers waged a nuclear arms race for nearly a quarter-century based on a doctrine of deterrence. Industrial nations silently conducted espionage of governments and corporations with thousands of intelligence and counter-intelligence agents. President Nixon even claimed that World War III had begun with the ratification of the first Strategic Arms Limitation Treaty. However this war would be a global economic war based on information assets. The foundation of today's society has moved to the accessibility and availability of valuable information. It is important to note the great economic differences in the value of information. Much information is literally worthless and is called garbage information. Many citizens of today's society have not been able to sift through the garbage information because of the glut of worthless information. Those individuals who have found the crown jewels of information (i.e., Bill Gates, Larry Ellison, Paul Allen, etc.) have accumulated great wealth at an astonishing rate (almost beyond comprehension). They have replaced the Sheiks of Arabia and the Sultan of Brunei, once the wealthiest individuals in the world because of a physical asset called oil. Thus, in the shift from an industrial to an information-centered economy, information and economic value are nearly synonymous. The way in which a nation-state wages war is similar to how it accumulates wealth (Toffler, 1980). Information warfare is fought on digital battlespace in which information assets are considered the strategic assets worthy of conquest or destruction. Information systems and critical infrastructure assets supporting those information systems become the new first-strike strategic targets of the post-Cold War era (Jones, 2000, p. 39). The new strategic defense weapons can be based on the Cooperative Engagement Capability Doctrine.

Evolution of Network-Centric Information Systems

Before discussing how Cooperative Engagement Capability may become an information security strategic defense weapon, let me first recall the concept of network-centric warfare from an information warfare perspective and how Cooperative Engagement Capability is part of network-centric warfare. Early computing