

RAID 2000
October 2-4, Toulouse France

Early Warning & Threat Assessment for Information Assurance

Topic Category: 3. Vulnerabilities and Attacks

Authors

Dr. Andrew Rathmell,
Mr Jim Dorschner, Mr Michael Knights & Mr Leon Watkins

Speaker

Dr. Andrew Rathmell

Institution

International Centre for Security Analysis (ICSA)
Department of War Studies
King's College London
Strandbridge House
Strand, London WC2R 2LS
United Kingdom

http: www.icsa.ac.uk

Biography

Dr. Andrew Rathmell

Dr. Andrew Rathmell is Executive Director of the International Centre for Security Analysis (ICSA) and Senior Lecturer in the Department of War Studies, King's College London. He joined the Department in July 1996 as ICSA Deputy Director and organized the ICSA's launch in October that same year. Previous to King's, Dr. Rathmell was a Research Fellow in the Centre for Arab Gulf Studies, University of Exeter. He was educated at Balliol College Oxford, George Washington University, and King's College London. He teaches courses on War & Peace in the Middle East and Intelligence & International Security in the Department of War Studies and at the Joint Services Command & Staff College. Research interests include Information Operations, Middle East security, and intelligence and low-intensity conflict/terrorism. Dr. Rathmell currently holds a NATO Research Fellowship, is a specialist advisor to the House of Commons Select Committee on Defense, and a member of the DTI's Foresight Threat & Security Task Force.

Abstract

Current reliance on *Attack Detection and Reaction* in Information Assurance is problematic because it accepts limited or no warning, and thereby accepts greater risks from successful attacks. This on-going, two year study involves devising and testing a basic methodology for *predicting cyber-attacks* based on understanding, and thereby anticipating hostile activity *by sub-state actors*.

Underlying the study is the concept that deeper understanding of potential threat actors – combining *technical and psycho/social aspects* to further refine estimates of *capabilities, intent and motive* – may increase the probability of developing *effective attack indicators*, thereby improving prospects for *substantive warning*.

The analytical method involves compiling a *multi-source data base* and establishing a *monitoring regime* limited to certain *hacktivists, single issue pressure groups and cyber-terrorists*. These, in turn, are exploited to develop reliable *indicators* for use in *predicting cyber-attacks*.

Data collection, methodology development and testing will be complete by December 2000, for publication in the spring/summer of 2001.