

**Managing Risks, Countering
Threats:
Protecting Critical National
Infrastructure Against Terrorism**

Martin Rudner

Canadian Centre of Intelligence and Security Studies
The Norman Paterson School of International Affairs
Carleton University

CRITICAL NATIONAL INFRASTRUCTURE

- **PUBLIC GOODS & SERVICES**
- **PRIVATE OWNERSHIP/OPERATORS**
- **INTERDEPENDENCY**
- **INTERNATIONAL LINKAGES /GLOBALIZATION**

CIP SECTORS

- **ENERGY**
- **TRANSPORTATION**
- **TELECOMMUNICATIONS**
- **DEFENCE & CHEMICAL INDUSTRY**
- **FINANCE**
- **WATER SUPPLY**
- **PUBLIC HEALTH**
- **FOOD**
- **GOVERNMENT**

THREAT ASSESSMENTS

- **AL-QAEDA TARGETING OF CRITICAL NATIONAL INFRASTRUCTURE**
 - STRATEGY
 - EVOLUTION
 - OBJECTIVES
- **AL-QAEDA OPERATIONS IN IRAQ AGAINST CRITICAL NATIONAL INFRASTRUCTURE**
 - REDEPLOYMENT/RETURN OF MUJAHIDEEN
- **AL-QAEDA OPERATIONS ELSEWHERE AGAINST CRITICAL NATIONAL INFRASTRUCTURE**
 - LONDON, MADRID, TURKEY
 - SAUDI ARABIA
 - JORDAN
 - BAB EL-MANDEB
- **OTHER TERROR TARGETING OF CRITICAL NATIONAL INFRASTRUCTURE**
 - COLOMBIA
 - NIGER DELTA
 - SRI LANKA
 - ISRAEL

A DEFENSIVE APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

- **FOCUS AT MICRO-LEVEL,
SINGULARITIES**
- **REACTIVE, PASSIVE PROTECTION**
 - **GUARDS, GATES (AND GUNS?)**
 - **PROTECTIVE SECURITY**
 - **HARDENING**
 - **ROBUST DESIGN/TECHNOLOGIES**
 - **REDUNDANCY**
- **EMERGENCY PREPAREDNESS**
- **ASSURANCE**
- **MITIGATION MANAGEMENT**

A RISK MANAGEMENT APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

- **PUBLIC/PRIVATE LIABILITIES**
- **PARADIGMS OF RISK**
 - **ACTUARIAL RISK**
 - **PROBABILITY ASSESSMENT**
 - **WICKED PROBLEMS**
- **CONSEQUENCE MANAGEMENT**
- **CRITICALITY AND INTERDEPENDENCE**
 - **PRIORITIZATION/RESOURCE ALLOCATION**
 - **LOW RISK, CATASTROPHIC CONSEQUENCES**

A STRATEGIC APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

- **PROACTIVE INTELLIGENCE-LED CIP**
 - IDENTIFY THREATS
 - EARLY WARNING
 - PREVENT ATTACKS
- **INTEGRATED, ALL-SOURCE ASSESSEMENT OF THREATS**
 - DATA-MINING
 - NETWORK ANALYSIS
- **OPERATIONAL PARTNERSHIPS: SECURITY MANAGERS - INTELLIGENCE – LAW ENFORCEMENT**
- **CULTURAL SHIFT: FROM “NEED TO KNOW” TO “NEED TO SHARE”**
 - THREAT BASED, DESIGNED PROTECTION

A STRATEGIC APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

(CONT.)

- **PUBLIC-PRIVATE SECTOR**
 - PRIVATE SECTOR LIABILITY
 - INFORMATION SHARING
 - INFORMATION PROTECTION
 - STANDARDS FOR PROTECTIVE SECURITY
- **COUNTER-PENETRATION ALERTNESS**
- **RESILIENCE PLANNING**
- **INTERNATIONAL COOPERATION**
- **TRAINING REQUIREMENT**

LESSONS THAT NEED TO BE LEARNED

- **Gaps in protection represent vulnerabilities to determined terrorists**
- **Terrorists will exploit any chink in our armor**
- **There will always be chinks in the armor of an open society**
- **National Security Policy for CIP to ensure:**
 - **that cost to adversaries of trying to exploit these chinks is high**
 - **their prospects of success minimal**
 - **potential consequential damages are mitigated, and that our Critical National Infrastructure has a pre-planned capacity for resilience.**

THE ETHIC OF WARNING

- “On issues of life and death the intelligence officer must always err on the side of the threat and not on the side of the optimist. Even if the threat is classified as being of low probability, it must be perceived as real and immediate. This is especially so if the penalty of a mistake would result in the deaths of thousands, major economic catastrophes, and ... social upheaval...”

-Efrain Halevy