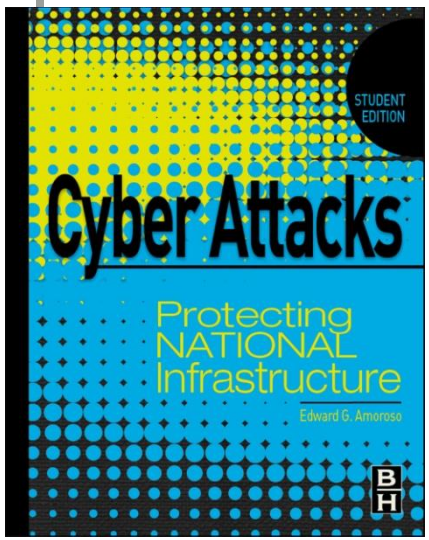


Chapter 1

Introduction

Introduction

- National infrastructure
  - Refers to the complex, underlying delivery and support systems for all large-scale services considered absolutely essential to a nation
- Conventional approach to cyber security not enough
- New approach needed
  - Combining best elements of existing security techniques with challenges that face complex, large-scale national services

Fig. 1.1 – National infrastructure cyber and physical attacks

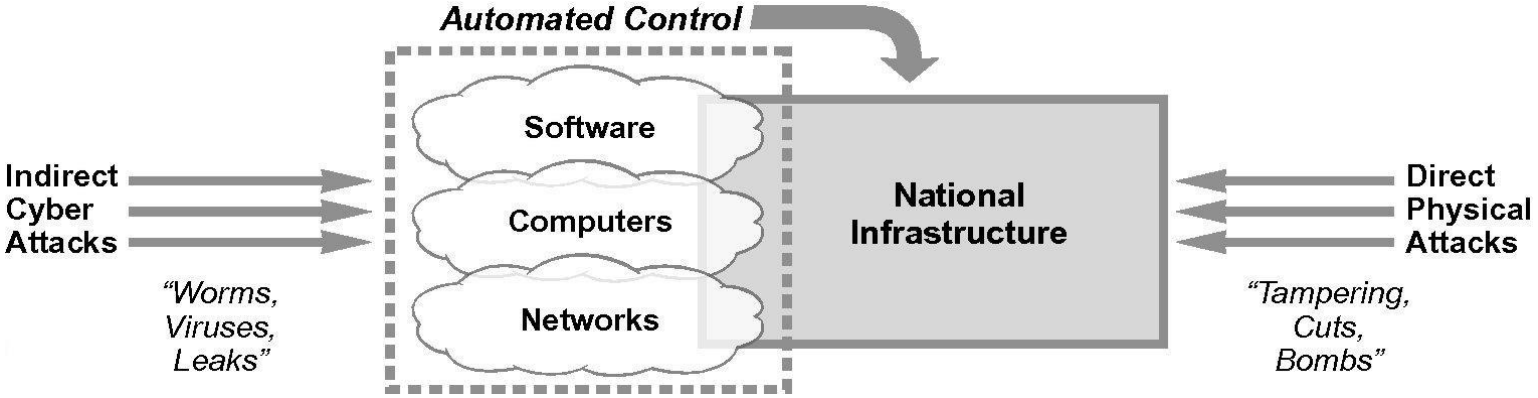
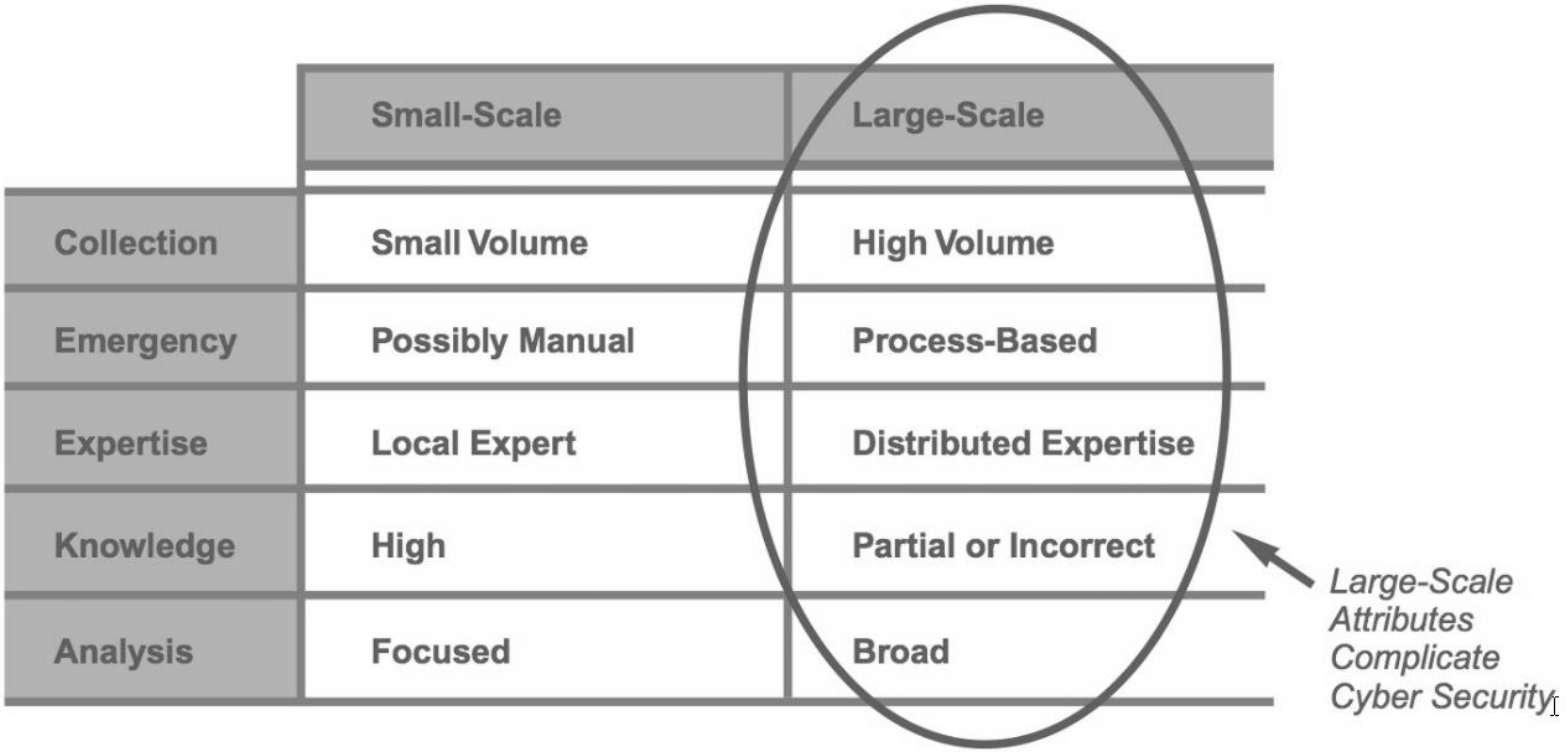


Fig. 1.2 – Differences between small- and large-scale cyber security



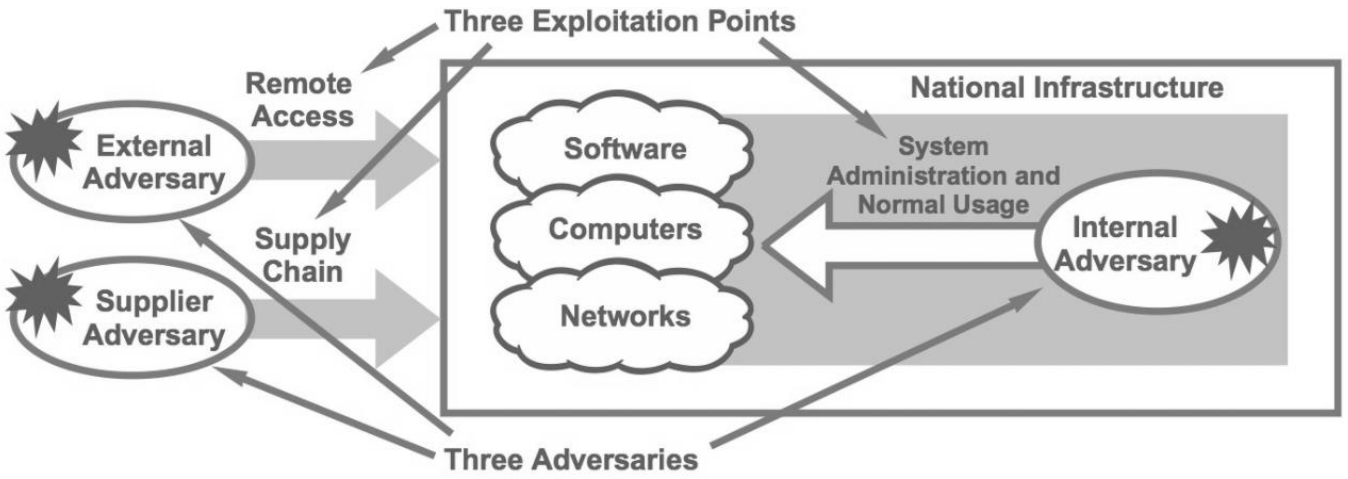
	Small-Scale	Large-Scale
Collection	Small Volume	High Volume
Emergency	Possibly Manual	Process-Based
Expertise	Local Expert	Distributed Expertise
Knowledge	High	Partial or Incorrect
Analysis	Focused	Broad

Large-Scale Attributes Complicate Cyber Security

National Cyber Threats, Vulnerabilities, and Attacks

- Three types of malicious adversaries
  - External adversary
  - Internal adversary
  - Supplier adversary

Fig. 1.3 – Adversaries and exploitation points in national infrastructure



National Cyber Threats, Vulnerabilities, and Attacks

- Three exploitation points
  - Remote access
  - System administration and normal usage
  - Supply chain

National Cyber Threats, Vulnerabilities, and Attacks

- Infrastructure threatened by most common security concerns:
  - Confidentiality
  - Integrity
  - Availability
  - Theft

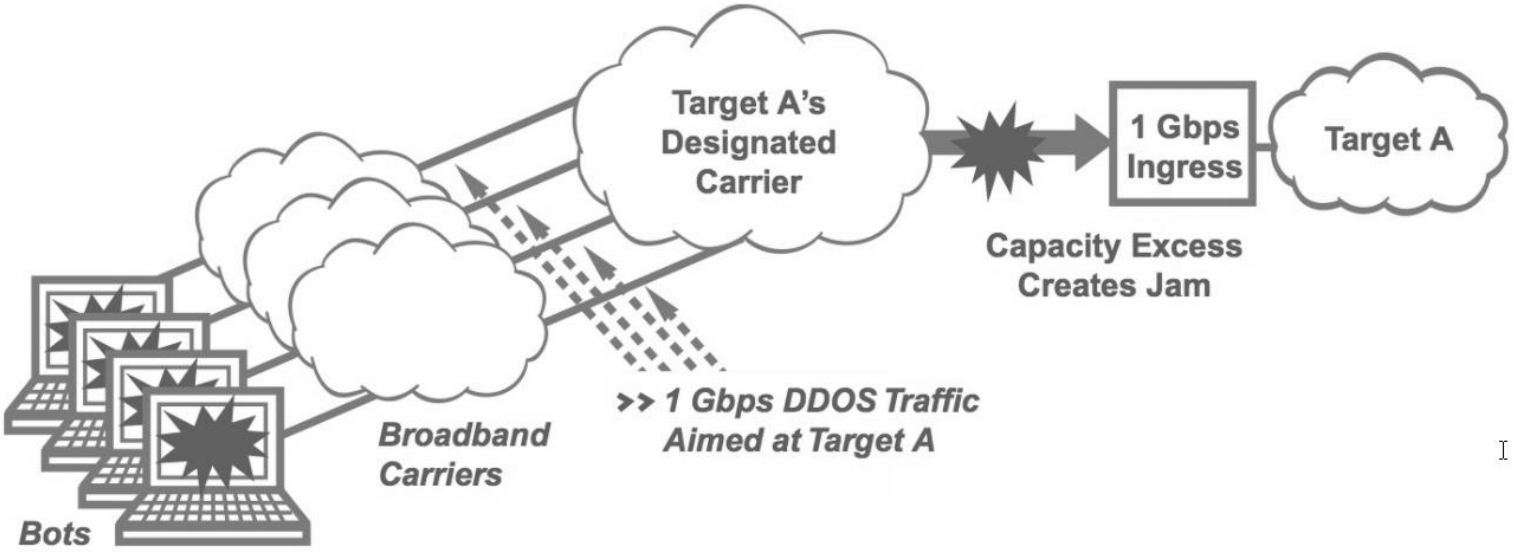
Botnet Threat

- What is a *botnet attack?*
  - The remote collection of compromised end-user machines (usually broadband-connected PCs) is used to attack a target.
  - Sources of attack are scattered and difficult to identify
  - Five entities that comprise botnet attack: *botnet operator, botnet controller, collection of bots, botnot software drop, botnet target*

Botnet Threat

- Five entities that comprise botnet attack:
  - Botnet operator
  - Botnet controller
  - Collection of bots
  - Botnot software drop
  - Botnet target
- Distributed denial of service (DDOS) attack: bots create “cyber traffic jam”

Fig. 1.4 – Sample DDOS attack from a botnet



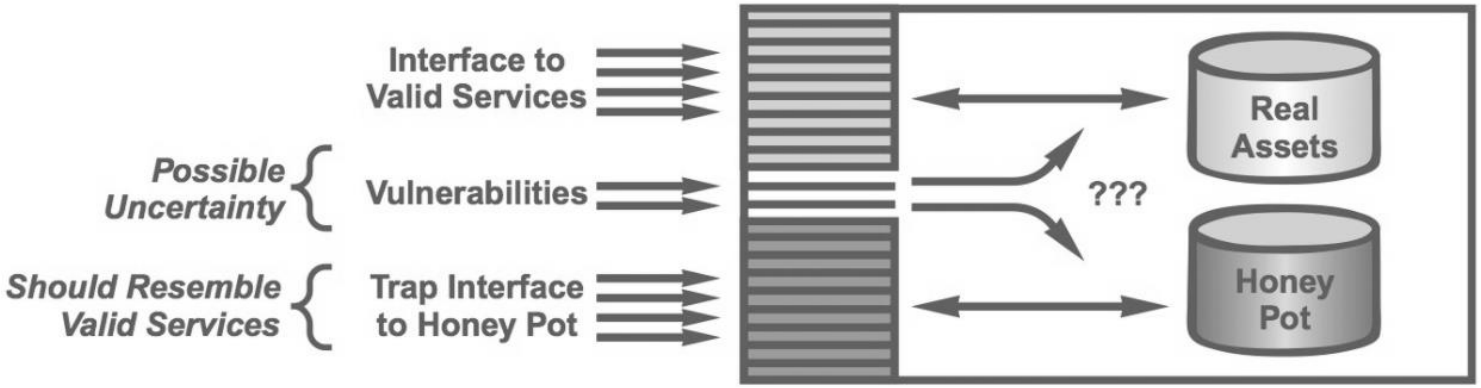
National Cyber Security Methodology Components

- Ten basic design and operation principles:
  - Deception
  - Separation
  - Diversity
  - Commonality
  - Depth
  - Discretion
  - Collection
  - Correlation
  - Awareness
  - Response

Deception

- Deliberately introducing misleading functionality or misinformation for the purpose of tricking an adversary
  - Computer scientists call this functionality a *honey pot*
- Deception enables forensic analysis of intruder activity
- The acknowledged use of deception may be a deterrent to intruders (every vulnerability may actually be a trap)

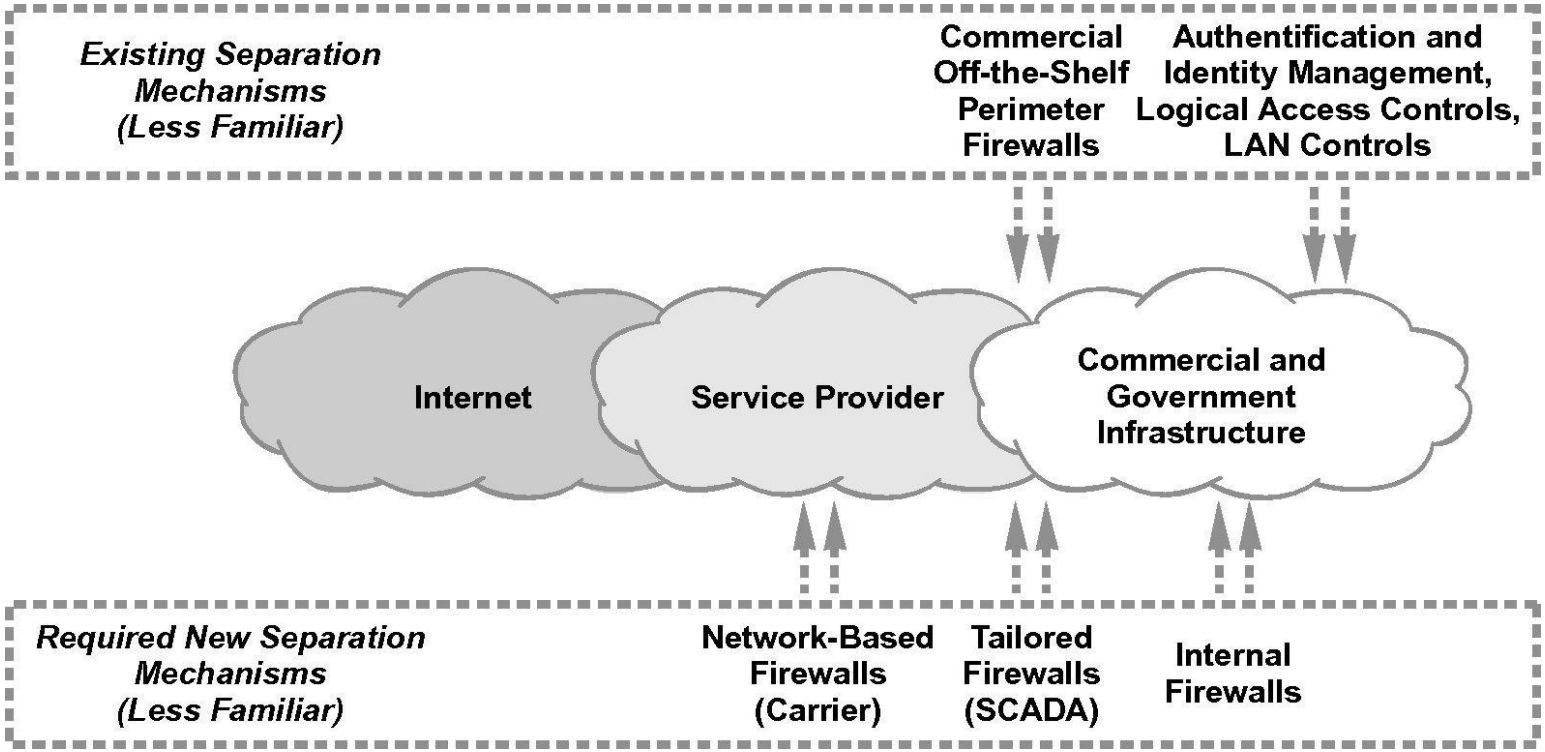
Fig. 1.5 – Components of an interface with deception



Separation

- Separation involves enforced access policy restrictions on users and resources in a computing environment
- Most companies use enterprise firewalls, which are complemented by the following:
  - Authentication and identity management
  - Logical access controls
  - LAN controls
  - Firewalls

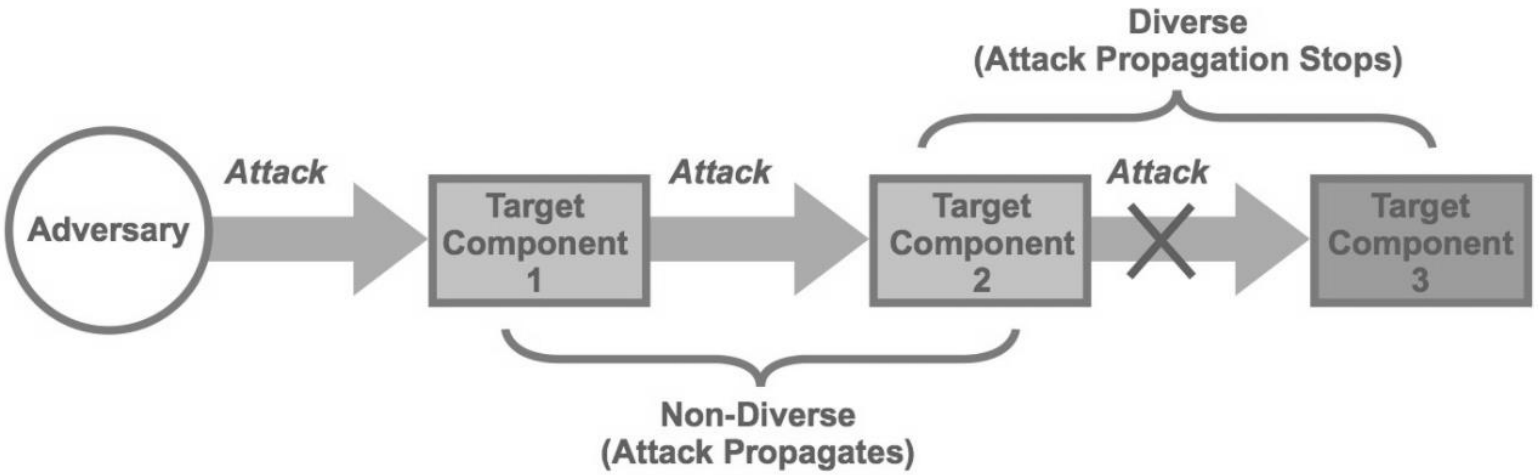
Fig. 1.6 – Firewall enhancements for national infrastructure



Diversity

- Diversity is the principle of using technology and systems that are intentionally different in substantive ways.
- Diversity hard to implement
  - A single software vendor tends to dominate the PC operating system business landscape
  - Diversity conflicts with organizational goals of simplifying supplier and vendor relationships

Fig. 1.7 – Introducing diversity to national infrastructure



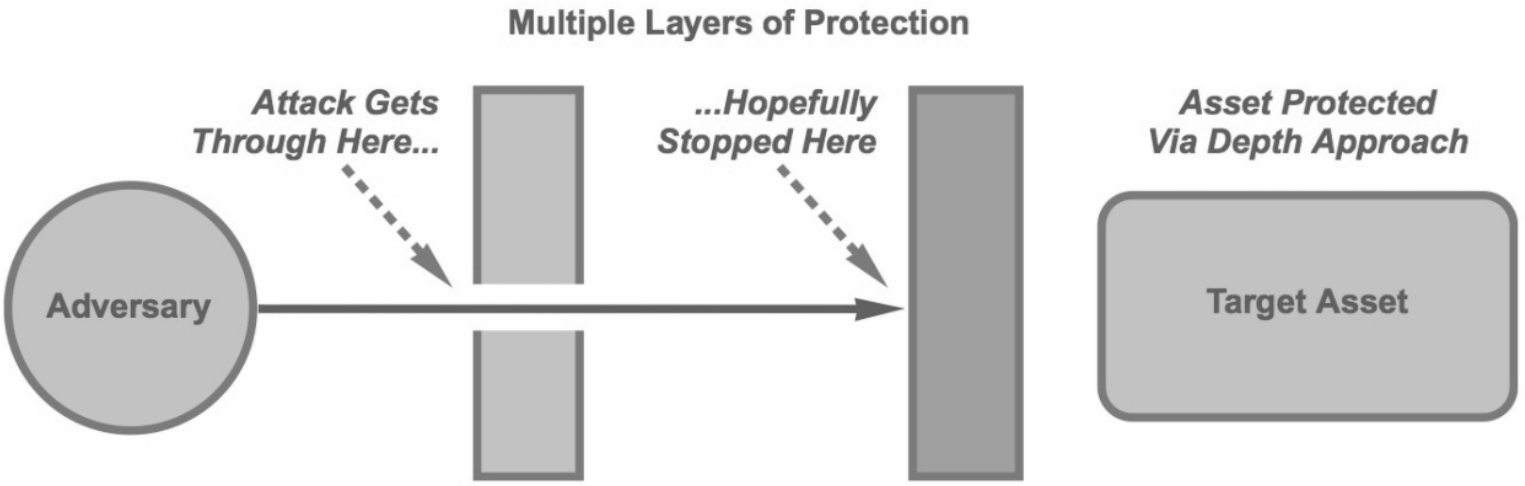
Commonality

- Consistency involves uniform attention to security best practices across national infrastructure components
- Greatest challenge involves auditing
- A national standard is needed

Depth

- Depth involves using multiple security layers to protect national infrastructure assets
- Defense layers are maximized by using a combination of functional and procedural controls

Fig. 1.8 – National infrastructure security through defense in depth



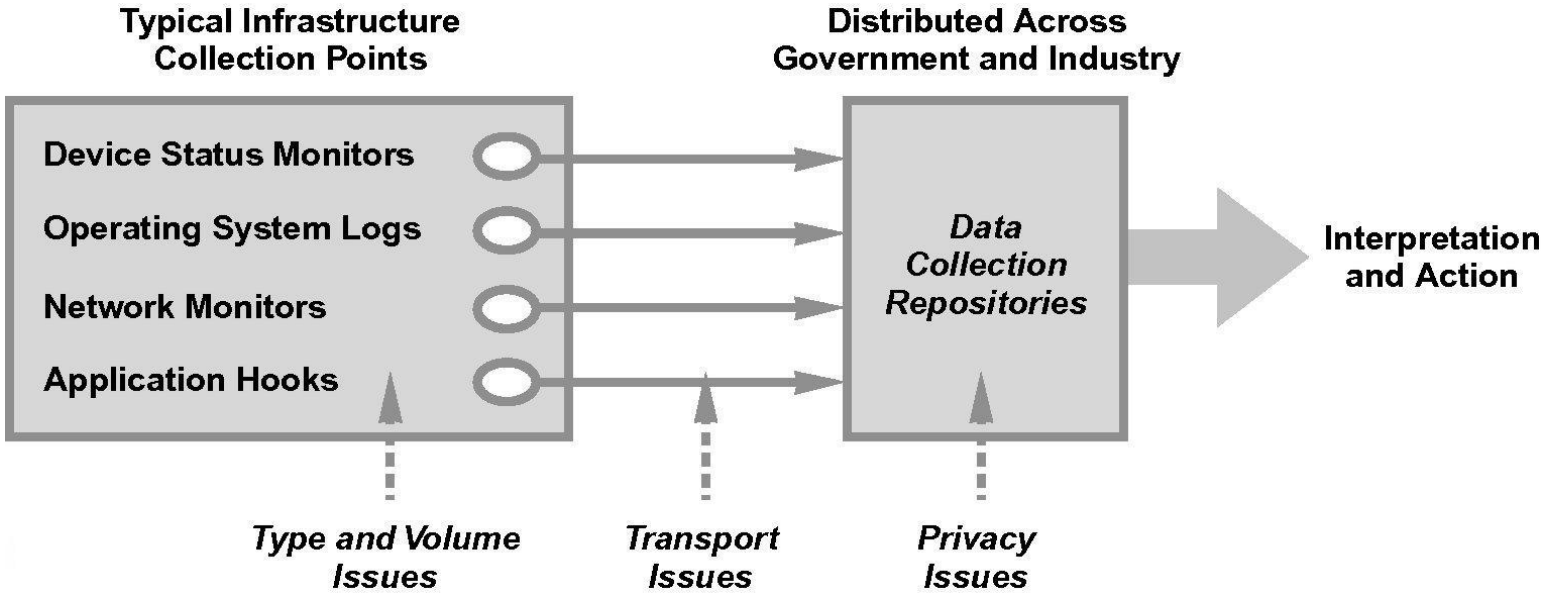
Discretion

- Discretion involves individuals and groups making good decisions to obscure sensitive information about national infrastructure
- This is not the same as “security through obscurity”

Collection

- Collection involves automated gathering of system-related information about national infrastructure to enable security analysis
- Data is processed by a *security information management system.*
- Operational challenges
  - What type of information should be collected?
  - How much information should be collected?

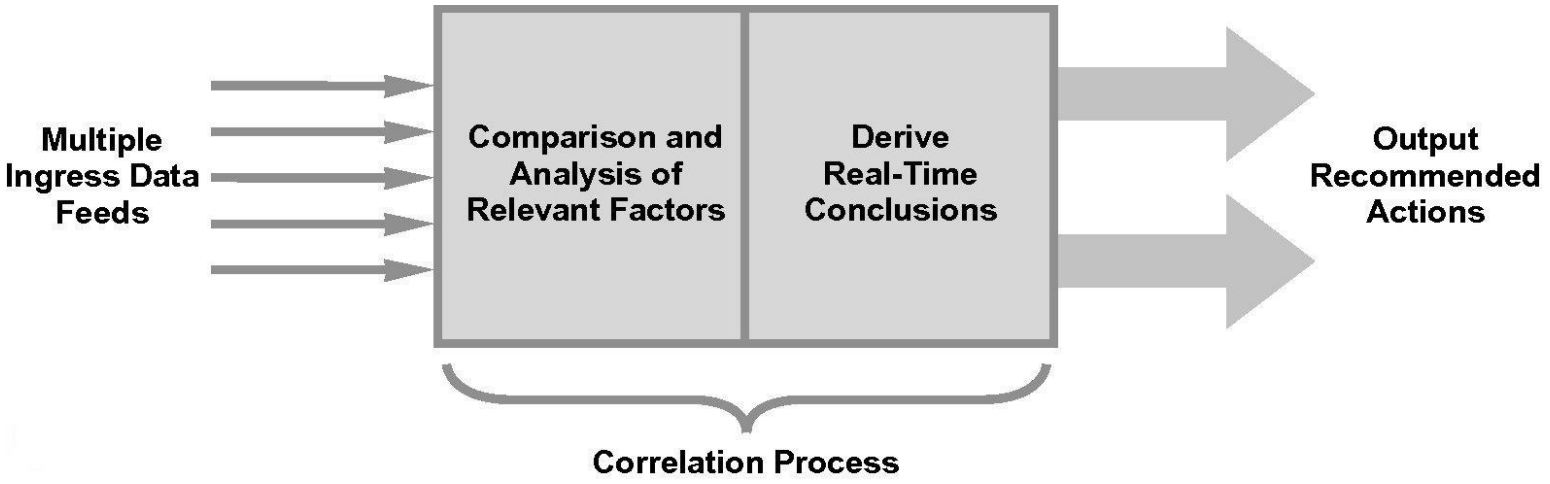
Fig. 1.9 – Collecting national infrastructure-related security information



Correlation

- Correlation involves a specific type of analysis that can be performed on factors related to national infrastructure protection
  - This type of comparison-oriented analysis is indispensable
- Past initiatives included real-time correlation of data at fusion center
  - Difficult to implement

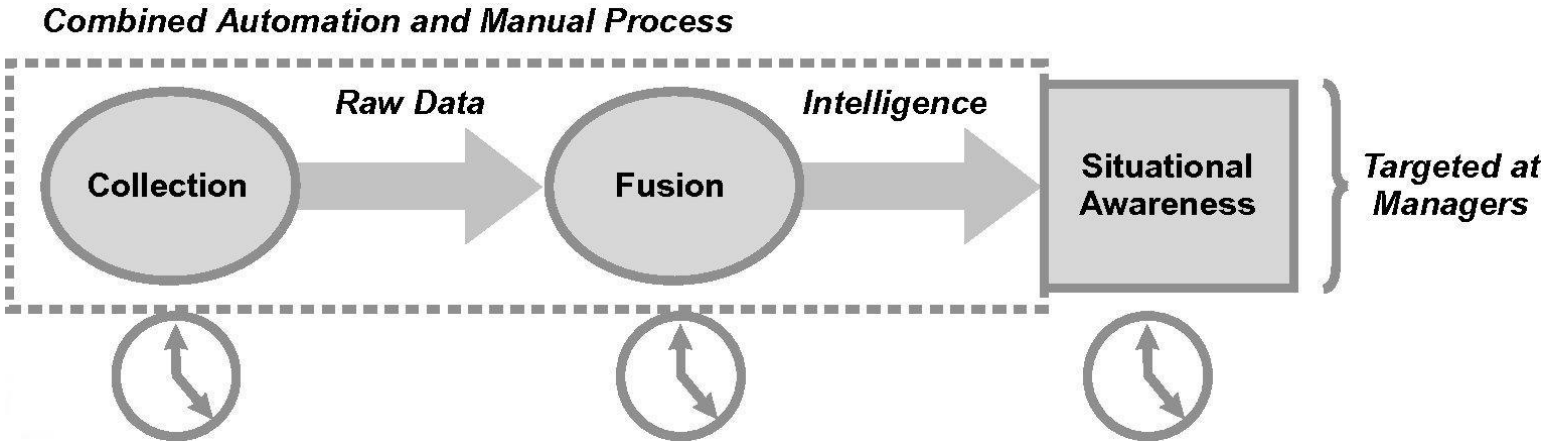
Fig. 1.10 – National infrastructure high-level correlation approach



Awareness

- Awareness involves an organization understanding the differences between observed and normal status in national infrastructure
- Most agree on the need for awareness, but how can awareness be achieved?

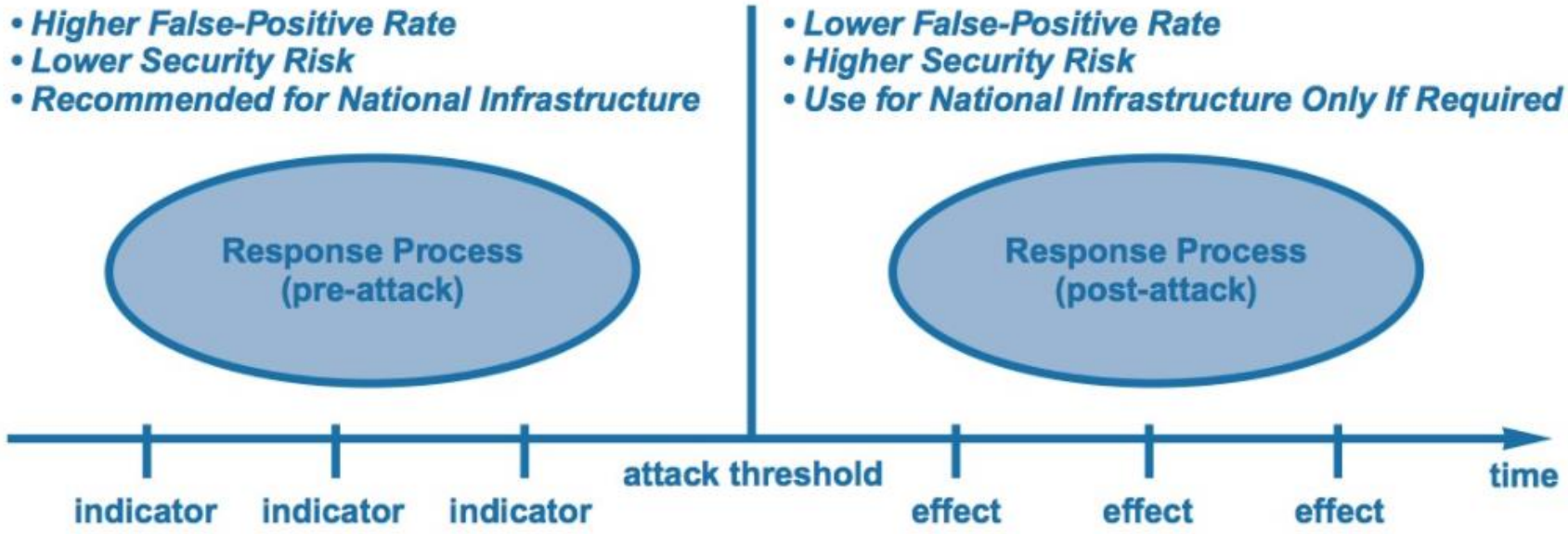
Fig. 1.11 – Real-time situation awareness process flow



Response

- Response involves the assurance that processes are in place to react to any security-related indicator
  - Indicators should flow from the awareness layer
- Current practice in smaller corporate environments of reducing "false positives" by waiting to confirm disaster is not acceptable for national infrastructure

Fig. 1.12 – National infrastructure security response approach



Implementing the Principles Nationally

- Commissions and groups
- Information sharing
- International cooperation
- Technical and operational costs