• About the Centers

• Objectives and Methodology for the Workshop

• Top Five Findings from the Workshop

• The Technical Papers that Comprise the Book

• Discussion
The Global Cyber Security Center (GCSEC) is a not-for-profit organization created to advance cyber security in Italy, Europe and around the world.

The Geneva Centre for Security Policy (GCSP) is an international foundation with 45 member states which was established in 1995 for the primary purpose of promoting peace, security and stability through training, research and dialogue.
• Discuss and share best practices on computer network defense

• Focus on incident detection and response

• Support NATO Cyber Defense Policy Implementation (Action Plan Item 12)
Workshop Objectives

- Assemble experts from some of the leading computer network defense organizations to understand the best practices for incident detection and response
- Identify the state-of-the art tools and processes being used
- Highlight the technology gaps
- Examine indicators and metrics to measure security of critical national infrastructures
- Investigate the emerging technology trends (e.g., cloud, mobility, IPv6, etc,) that may change the nature of computer network defense
What are the new threats and trends challenging operators and decision makers?

What is the role of national and international strategies, legislation, and regulation to

What are effective mechanisms for coordination and cooperation to prevent and respond to incidents?

What emerging technologies exist for advanced prevention, detection, containment, and remediation for computer network defense?

What metrics exist for measuring cyber security effectiveness?

What is the role of standards and which standards are proving most useful for CND?

The Workshop Methodology

- **Expert Presentations**
  - 7 Panels
- **Group Discussion**
  - Multi-disciplinary Team of Experts
- **Discovery and Findings**
  - Report
Twenty-one specific findings emerged from the workshop and pathways toward achieving a stronger cyber defense posture were illuminated.

1. **Identifying critical services is more important than identifying critical infrastructures.** Changing the focus from critical infrastructure to critical service may change the approach to protection, resilience, recovery and restoration of assets. It may also highlight the interdependencies among organizations and nations requiring different approaches to common defense.

2. **A Baseline assessment is essential to measure current and future effectiveness.** A baseline assessment enables an organization to identify the current state of the controls it has in place to protect infrastructures, assets, and services.

3. **Acquisition, purchasing, and security decisions are not mutually reinforcing.** Security considerations must become a core component of the purchasing and acquisition decisions, and not be negotiable.

4. **Advanced, effective techniques for defense are operating in industry and showing promising results.** The technologies are accessible and affordable and are showing promising results.

5. **Detection has replaced defense as a strategy.** No organization should accept the status quo. New tactics and countermeasures are available to strengthen security postures and become more resistant to cyber threats, rather than just detect their success.

In a domain where speed is essential, where advanced defense is required against advanced offense, and where collaboration and learning amongst defenders is essential, keeping pace and deploying advanced process or technology is only possible when you know what is available.
# Best Practices in Computer Network Defense: Incident Detection and Response

Edited by
Melissa E. Hathaway

## Author and Paper Title

<table>
<thead>
<tr>
<th>Author</th>
<th>Paper Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gijsbers</td>
<td>Foreword</td>
</tr>
<tr>
<td>Hathaway</td>
<td>Advanced Research Workshop Findings</td>
</tr>
<tr>
<td>Stewart</td>
<td>Advanced Technologies/Tactics, Techniques Procedures: Closing the Attack Window and Thresholds for Reporting and Containment</td>
</tr>
<tr>
<td>McMahon</td>
<td>Beyond Perimeter Defense: Defense-in-Depth Leveraging Upstream Security</td>
</tr>
<tr>
<td>Lindner and Gaycken</td>
<td>Back to Basics: Beyond Network Hygiene</td>
</tr>
<tr>
<td>Holt</td>
<td>Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities</td>
</tr>
<tr>
<td>Kruidhof</td>
<td>Evolution of National and Corporate CERTS - Trust, the Key Factor</td>
</tr>
<tr>
<td>Purser</td>
<td>Standards for Cyber Security</td>
</tr>
<tr>
<td>Pelgrin</td>
<td>A Model for Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership</td>
</tr>
<tr>
<td>van den Heuvel and Klein Baltink</td>
<td>Coordination and Cooperation in Cyber Network Defense: The Dutch Efforts to Prevent and Respond</td>
</tr>
</tbody>
</table>

• Chapter 1: Summary of the 21 findings from the Advanced Research Workshop

• Chapter 2 follows with an in-depth analysis of new threats and trends for computer network defense. It describes three ICT trends that present both economic opportunity and potential new vulnerabilities to society.

• Chapters 3, 4, and 5 identify advanced computer network defense techniques, including state-of-the art tools and processes being used for cyber defense. These three chapters also highlight technology gaps that should be addressed in order to better prepare for tomorrow’s challenges.

• Chapter 6 describes how national cyber security strategies play a key role in shaping a country’s approach to CND. It also discusses how overlapping or conflicting requirements imposed by international organizations and individual countries may make national cyber security programs less effective.

• Chapter 7 describes how Computer Emergency Response Teams (CERTs) are designed and implemented, and discusses the importance of trusted collaboration in effectively handling cyber incidents.

• Chapter 8 highlights how standards play a key role in improving cyber defense and cyber security across different geographical regions and communities.

• Chapter 9 discusses how qualitative and quantitative metrics can inform decisions and change behavior.

• Chapter 10 highlights a concrete example from The Netherlands of a successful private-public partnership aimed at improving overall cyber security. It shows the reader why effective CND requires close cooperation and collaboration between government and industry, science and education, and national and international efforts.