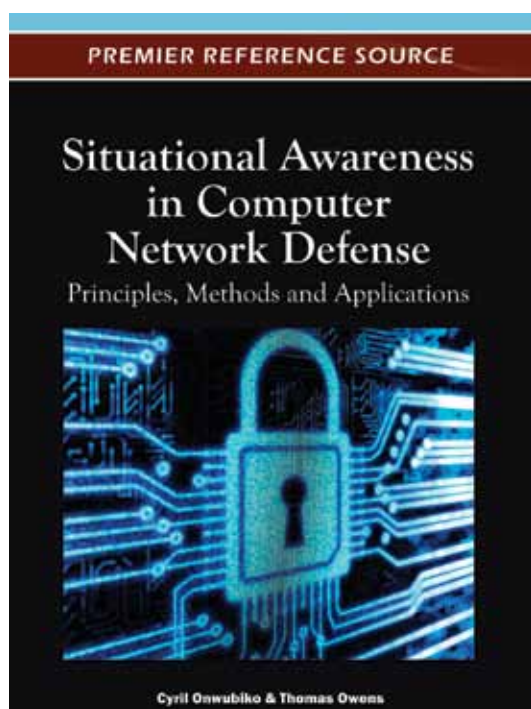


# An Excellent Addition to Your Library!

Released: January 2012

## Situational Awareness in Computer Network Defense: Principles, Methods and Applications



Cyril Onwubiko (Research Series Ltd, UK)  
and Thomas Owens (Brunel University, UK)

Worldwide computer crimes cost organizations and governments billions of dollars each year. In response, organizations use a plethora of heterogeneous security devices and software such as firewalls, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM) to monitor networks in conjunction with Computer Security Incident Response Teams (CSIRT) that are responsible for ensuring availability, integrity, and confidentiality of network services.

**Situational Awareness in Computer Network Defense: Principles, Methods and Applications** provides academia and organizations insights into practical and applied solutions, frameworks, technologies, and implementations for situational awareness in computer networks. This book presents situational awareness solutions in Computer Network Defense (CND) currently being researched or deployed. The key objective is to fill a gap that exists in the way CND and security are being approached by formalizing the use of situational awareness in computer network security and defense.

### Topics Covered:

- Computer Network Security
- Cyber Attacks
- Cyber Command and Control
- False Data in Wireless Sensor Networks
- Forensic Investigative Procedures
- Global Collaborative Defense
- Information Security for Situational Awareness
- Modeling Situational Awareness
- Optimization of Enterprise Network Defense Systems
- Security Incident Analysis

ISBN: 9781466601048; © 2012; 414 pp.

Print: US \$195.00 | Perpetual: US \$295.00 | Print + Perpetual: US \$390.00

**Market:** This premier publication is essential for all academic and research library reference collections. It is a crucial tool for academicians, researchers, and practitioners and is ideal for classroom use.

**Cyril Onwubiko** is a leading information security expert and founder of Research Series in London, UK where he leads on intelligence and security assurance, Cyber security, and situational awareness in computer network defense. Prior to Research Series, he was an information security consultant at British Telecommunications, CLAS consultant at Cable & Wireless Worldwide, and a security analyst at COLT Telecommunications. He holds a PhD degree in Computer Network Security from Kingston University, London, UK. Dr. Onwubiko has authored several books, including "Security Frameworks for Attack Detection in Computer Networks," and has published over 30 academic articles in reputable journals, conference proceedings, and edited books. He is a member of the IEEE, Institute of Information Security Professionals (IISP), and CESG Listed Advisor Scheme (CLAS).



www.igi-global.com

Publishing Academic Excellence  
at the Pace of Technology Since 1988

## Section 1: Principles of SA CND

### Chapter 1

*Review of Situational Awareness for Computer Network Defense*

Onwubiko Cyril (Research Series Limited, UK)

Owens Thomas John (Brunel University, UK)

### Chapter 2

*The Contributions of Information Security Culture and Human Relations to the Improvement of Situational Awareness*

Hagen Janne Merete (Norwegian Defence Research Establishment, Norway)

### Chapter 3

*Cyber Command and Control:*

Ruiz Michael E. (Deloitte Consulting, USA)

Redmond Richard (Virginia Commonwealth University, USA)

### Chapter 4

*A Proactive Defense Strategy to Enhance Situational Awareness in Computer Network Security*

Luo Yi (The University of Arizona, USA)

Szidarovszky Ferenc (The University of Arizona, USA)

### Chapter 5

*An Alternative Framework for Research on Situational Awareness in Computer Network Defense*

McMillan Eric (The Pennsylvania State University, USA)

Tyworth Michael (The Pennsylvania State University, USA)

### Chapter 6

*Information Security for Situational Awareness in Computer Network Defense*

Blumenthal Uri (MIT Lincoln Laboratory, USA)

Haines Joshua (MIT Lincoln Laboratory, USA)

Streilein William (MIT Lincoln Laboratory, USA)

O'Leary Gerald (MIT Lincoln Laboratory, USA)

### Chapter 7

*Designing Information Systems and Network Components for Situational Awareness*

Onwubiko Cyril (Research Series Limited, UK)

## Section 2: Methods in SA CND

### Chapter 8

*Cyber Situation Awareness through Instance-Based Learning:*

Dutt Varun (Carnegie Mellon University, USA)

Gonzalez Cleotilde (Carnegie Mellon University, USA)

### Chapter 9

*Information Data Fusion and Computer Network Defense*

Ballora Mark (The Pennsylvania State University, USA)

Giacobe Nicklaus A. (The Pennsylvania State University, USA)

McNeese Michael (The Pennsylvania State University, USA)

Hall David L. (The Pennsylvania State University, USA)

### Chapter 10

*Usefulness of Sensor Fusion for Security Incident Analysis*

Thomas Ciza (College of Engineering, India)

Balakrishnan N. (Indian Institute of Science, India)

### Chapter 11

*GCD:*

Acharya Subrata (Towson University, USA)

### Chapter 12

*DNSSEC vs. DNSCurve:*

Anagnostopoulos Marios (University of the Aegean, Greece)

Kambourakis Georgios (University of the Aegean, Greece)

Konstantinou Elisavet (University of the Aegean, Greece)

Gritzalis Stefanos (University of the Aegean, Greece)

### Chapter 13

*IEEE802.21 Assisted Fast Re-Authentication Scheme over GS-ABA*

Mussabbir Qazi Bouland (Brunel University, UK)

Owens Thomas John (Brunel University, UK)

## Section 3: SA CND Applications

### Chapter 14

*Modelling Situation Awareness Information and System Requirements for the Mission using*

*Goal-Oriented Task Analysis Approach*

Onwubiko Cyril (Research Series Limited, UK)

### Chapter 15

*On Situational Aware En-Route Filtering against Injected False Data in Cyber Physical Systems*

Yang Xinyu (Xi'an Jiaotong University, P. R. China)

Lin Jie (Xi'an Jiaotong University, P. R. China)

Yu Wei (Towson University, USA)

Fu Xinwen (University of Massachusetts Lowell, USA)

Chen Genshe (Independent Consultant Professional, USA)

Blasch Erik P. (Air Force Research Laboratory, USA)

### Chapter 16

*Attack Graphs and Scenario Driven Wireless Computer Network Defense*

Hawrylak Peter J. (The University of Tulsa, USA)

Louthan George (The University of Tulsa, USA)

Daily Jeremy (The University of Tulsa, USA)

Hal John (The University of Tulsa, USA)

Papa Mauricio (The University of Tulsa, USA)

### Chapter 17

*Advanced Security Incident Analysis with Sensor Correlation*

Thomas Ciza (College of Engineering, India)

Balakrishnan N. (Indian Institute of Science, India)

### Chapter 18

*PITWALL:*

Acharya Subrata (Towson University, USA)

### Chapter 19

*Forensic Investigative Process for Situational Awareness in Information Security*

Ali Khidir Mohamed (Jubail University College, Saudi Arabia)

Owens Thomas John (Brunel University, UK)

## Order Your Copy Today!

Name: \_\_\_\_\_

Organization: \_\_\_\_\_

Address: \_\_\_\_\_

City, State, Zip: \_\_\_\_\_

Country: \_\_\_\_\_

Tel: \_\_\_\_\_

Fax: \_\_\_\_\_

E-mail: \_\_\_\_\_

☐ Enclosed is check payable to IGI Global in  
US Dollars, drawn on a US-based bank

☐ Credit Card ☐ Mastercard ☐ Visa ☐ Am. Express

3 or 4 Digit Security Code: \_\_\_\_\_

Name on Card: \_\_\_\_\_

Account #: \_\_\_\_\_

Expiration Date: \_\_\_\_\_