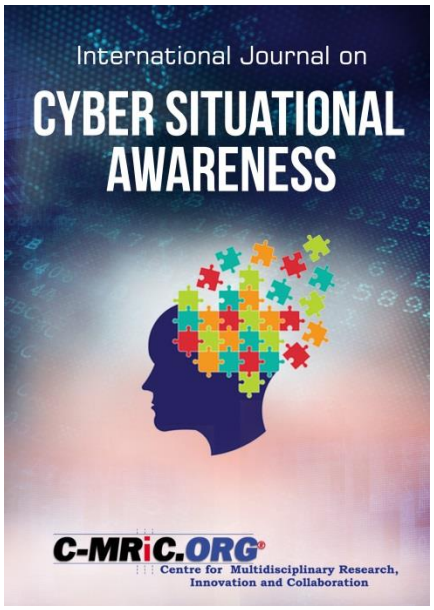
Guidelines for completing your manuscripts to the International Journal on Cyber Situational Awareness



ISSN: (Print) **2057-2182** ISSN: (Online) **2057-2182**

DOI: 10.22619/IJCSA

International Journal on Cyber Situational Awareness (IJCSA)

ISSN: (Print) **2057-2182** ISSN: (Online) **2057-2182**

DOI: 10.22619/IJCSA

Published Bi-annually. Est. 2014

Important Notes before submitting your manuscripts

1. Only original and previously unpublished manuscripts must be submitted to the IJCSA journal.
2. All accepted manuscripts will be checked against plagiarism using a number of sources including the IEEE PAL (Prohibited Authors List).
3. We only accept manuscripts dedicated and/or relating to **Situational Awareness**. We do NOT accept general purpose Cyber Security contributions. The IJCSA is solely dedicated to Cyber Situational Awareness; hence some excellent contributions relating to general purpose computing will be rejected.
4. All manuscripts must be prepared following the IJCSA paper template.
5. All manuscripts are subjected to multiple blind-peer reviews, and revisions may take longer than anticipated.
6. Please review our code of conducts policy - http://www.c-mric.com/code-of-conduct/
7. Please review our process map - http://www.c-mric.com/ijcsa-process-map/

Overall Mission

The **International Journal on Cyber Situational Awareness (IJCSA)** is a comprehensive reference journal, dedicated to disseminating the most innovative, systematic, topical and emerging theory, methods and applications of Situational Awareness (SA) across Cyber Systems, Cyber Security, Cyber Physical Systems, Computer Network Defence, Enterprise Internet of Things (EIoT), Security Analytics, Intelligence and Crypto systems to students, scholars, and academics, as well as industry practitioners, engineers and professionals.

Overall Scope

The **International Journal of Cyber Situational Awareness (IJCSA)** covers innovative research on theoretical and practical aspects of Situational Awareness on Cyber Systems. The journal focuses on the advancement of the principles, methods and applications of situational awareness to support, enable and facilitate advances in Cyber Systems, Business Information Systems (BIS), Computer Network Defence (CND), Computer Physical Systems (CPS), Enterprise Internet of Things (IoTs), Social Media, Cyber Incident Responses, Control, Containment and Countermeasures (CIRC3).

Coverage

Recommended topics include, but are not limited to, the following:

Situational Awareness for Computer Networks Defense
- Computer Network Defense
- Cyber Situation Awareness
- Correlation & Automation

Collaborative Situation Awareness for Decision Making
- Collaborative Defense Approach
- Situation Assessment & Decision Making

Defense Strategy for the Enhancement of Situational Awareness
- Risk Management, Governance and Compliance
- Trust, Privacy and Anonymity Issues
- Digital Forensic Information Analysis
- Enterprise Information Security Policies, Standards and Procedures
- Risks posed by Wireless Networks, including through the use of Mobile Computing, BYOD, Wearable in CND environment

Cyber Situational Awareness Tools & Techniques
- Fuzzy Logic
- Rough Set
- Artificial Neural Networks
- Artificial Intelligence
- Genetic Algorithm
- Evidence Theory (DST)
- Bayesian Networks & Set Theory
- Big Data Analytics
- Game Theory
- Graph Theory

Network Situational Awareness
- Cyber Attack Scenarios
- Situation-Aware and Context-Aware Network Applications
- CERTs and CSIRTs
- Security Event and Information Management
- Application Security, Audits and Penetration Testing

Human Factor Cognitive
- Workload
- Perception
- Stress

- Knowledge
- Training and Expertise
- Risk Assessment and Decision Making
- Forecasting and Prediction
- Operator SA & Team SA

National and Critical Infrastructure Security Issues

- Information Security
- Cyber Security
- Database Security
- Application Security
- Law Enforcement and Surveillance
- Border Protection and Controls
- Cyber Warfare and Counter Terrorism

Situation Awareness in Military Operations

- Military Doctrinal in Situation Awareness
- C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)
- Computer Network Operations
- Computer Network Defense
- Mission Awareness, Command and Control

Analysis of Large-Scale Internet Traffic

- Attack Graphs
- Advanced Security Incident Analysis
- Sensor Correlation and Cross-Correlation
- Implementing Situational Awareness Systems
- Information Security Metrics and Measurements

Web Traffic Characterisation

- Intrusion Detection Systems
- Traffic Characterisation Techniques
- Web Analytics
- Security Incident Response

Cyber Situational Awareness Frameworks

- Proactive Defense Strategies
- Instance-Based Learning
- Adaptive Neural Logic
- Human-Assisted Decision Control
- Human in the Loop
- Automated Self-Responder

Fusion Centres

- Tools for Metric Optimisation
- Visualisation and Digital Analytics
- Data Mining
- Filtration, Selection, and Risk-Based Prioritisation
- Metrics for Evaluation and Assessment

Situational Awareness Applications

- Situational Awareness in C4ISR
- Situational Awareness in Cyber Command and Control Centres
- Situational Awareness in Intrusion Defense
- Situational Awareness in Cyber Physical Systems (CPS)
- Situational Awareness for Internet of Things (IoTs), Enterprise Internet of Things (EIoTs)
- Open Source Applications

Designing Cyber Situational Awareness Solutions and Services

- Functional Requirements for Situation-aware services
- Non-Functional Requirements for Situation-aware Services and solutions
- Interface Design
- Interoperability
- Dynamism
- Complexity
- Performance
- Automation

- Realtime Processing

Usefulness of Multisensor Data Fusion

- Information Data Fusion
- Sensor Fusion for Security Incident Analysis
- Security Incident Analysis
- Data Association & Correlation
- Security Information Visualisation
- Data Analytics
- Security Monitoring

Situational Awareness Training

- Research and development in Situational Awareness
- Simulation and Testbeds in Cyber Situation Awareness
- Experimentation & Instrumentation
- Modelling
- Knowledge-base
- Theoretical Underpinnings in Situation Awareness

Possible Readership/Audience

The primary audience for this journal are industry professionals, scholars, researchers and academies working in this fast evolving and emerging discipline. Practitioners and managers working in information technology and cyber security across all industries would vastly improve their knowledge and understanding of critical human and social aspects of situational awareness and computer network defence, human computer interface (HCI) and information security in general. Air space controllers and defence agencies will also find this journal a very helpful and practical resource.

Competing Journals (list of current competition publication)

There are no competing journals in this unique and specialist area, especially those focusing on the application of situation awareness to Cyber Security (CS), Cyber Physical Systems (CPS), and Cyber Incident Responses, Control, Containment and Countermeasures (CIRC3).

Timetable

- Deadline for submission is 31st August 2019.
- The expected timeline for publishing **IJCSA Volume 4, No. 1, (2019)** is November 2019.
- Manuscripts can be submitted now using the Easychair link https://easychair.org/conferences/?conf=ijcsavol4