

## **SPECIAL ISSUE on**

### **Big Data Applications and Techniques in Cyber Intelligence**

#### **GUEST EDITORS**

Zheng Xu, Shanghai Polytechnic University, China (Lead GE)

Neil Y. Yen, University of Aizu, Japan

Vijayan Sugumaran, Oakland University, USA

#### **DESCRIPTION**

This special issue in [Open Computer Science](#) focuses on the Big Data Applications and Techniques in Cyber Intelligence

The development of big data needs to rely on cyber intelligence technology, because it uses many theories and methods of cyber intelligence. Furthermore, it has achieved certain results. The value of big data as an infrastructure of cyber intelligence is about to usher in a long-term development opportunity. On the other hand, solve the problem of scalability and growth of cyber intelligence cannot be done without big data technology. The development of cyber intelligence also needs to rely on the environment and technology support of big data. It is necessary for cyber intelligence, just like human beings, to have a lot of knowledge and rich experience; behind these knowledge and experience is the need for a large number of data support. The development of cyber intelligence and big data will push each other to form an effective mutual promotion effect. Therefore, the development of cyber intelligence relies on big data, at the meanwhile; big data also open a new chapter for cyber intelligence. Humans will develop intelligent technology under a new perspective of mechanism, thinking and environment of big data.

This special issue focuses on the theory, methods and creative solutions of cyber intelligence and big data. Topics of interest include but are not limited to the following:

- Data acquisition and preprocessing technology
- Intelligent computing, data mining methods and algorithms
- Big data system solutions and tools platform
- Cyber intelligence theory and application
- Intelligent control and intelligent management
- Knowledge science and knowledge engineering
- Cyber intelligence technology for big data
- Tracing real Internet attackers through information correlation
- Intrusion detection
- Malware detection
- Anomaly behaviour analytics
- Blockchain
- Blockchain and Big Data
- forecasting utilizing big data
- threat indicators in massive data sets
- threatcasting using bag data
- operational situation awareness utilizing big data-driven intelligence

Authors are requested to submit their full revised papers complying the general scope of the journal. The submitted papers will undergo the standard peer-review process before they can be accepted. Notification of acceptance will be communicated as we progress with the review process.

## HOW TO SUBMIT

Before submission authors should carefully read the [Instruction for Authors](#), available online at:

[https://www.degruyter.com/publication/journal\\_key/COMP/downloadAsset/COMP\\_Instruction%20for%20Authors.pdf](https://www.degruyter.com/publication/journal_key/COMP/downloadAsset/COMP_Instruction%20for%20Authors.pdf)

Manuscripts can be written in TeX, LaTeX (strongly recommended) - the journal's [LATEX template](#). Please note that we do not accept papers in Plain TEX format. Text files can be also submitted as standard DOCUMENT (.DOC) which is acceptable if the submission in LATEX is not possible. **For an initial submission, the authors are strongly advised to upload their entire manuscript, including tables and figures, as a single PDF file.**

All submissions to the Special Issue must be made electronically via online submission system Editorial Manager: <http://www.editorialmanager.com/opencs/>

All manuscripts will undergo the standard peer-review process (single blind, at least two independent reviewers). **When entering your submission via online submission system please choose the option “Special Issue on Big Data Applications and Techniques in Cyber Intelligence”.**

Submission of a manuscript implies that the work described has not been published before and it is not under consideration for publication anywhere else.

**The deadline for submissions is January 30, 2023**, but individual papers will be reviewed and published online on an ongoing basis.

Contributors to the Special Issue will benefit from:

- Critical peer-review
- no space constraints
- quick online publication upon completing the publishing process (**continuous publication model**)
- better visibility due to **Open Access** – free, unrestricted and permanent access to all the content
- **liberal policies on copyrights** (authors retain copyrights) and on self-archiving (no embargo periods)
- promotion of published papers to readers and citers
- **long-term preservation** – content archiving with Portico

We are looking forward to your submission!

In case of any questions please contact [Editorial Office](#) ([opencomputerscience@degruyter.com](mailto:opencomputerscience@degruyter.com))