Special issue on **Cybersecurity, Cybercrime, Cyberwarfare**  
Guest editor: Sherali Zeadally, University of Kentucky, USA

**Journal of Homeland Security and Emergency Management**  
Editor-in-Chief: Dr. Renda-Tanali, Irmak; Managing Editor: Dr. McGee, Sibel

1. **Scope**

Over the recent decades, we have witnessed tremendous advances in computing, communications, and hardware and software technologies, all of which continue to fuel the development, growth, and importance of cyberspace. Today, governments and industry heavily depend on cyberspace for many of their daily operations. Critical infrastructures are increasingly characterized by cyber interdependencies through their growing reliance on computerized control systems that use and sustain electronic and informational linkages. Cyberspace is also playing an important role in the personal lives of citizens around the world. The social and economic well-being of all societies now depend on the safe, secure, and reliable functioning of cyberspace. Such increased connectedness, however, puts the security of cyberspace and critical personal, corporate, and national assets under the constant threat of criminal and terrorist activities. Ranging from corporate espionage to hacking into systems that contain nationally significant intelligence, cybercrimes and cyberwarfare are on the rise. The protection of cyberspace has become a national priority for many nations. As a result, cybersecurity research has been receiving a lot of attention from government, industry, and academia.

The goal of this special issue is to present state-of-the-art research results in the areas of cybersecurity, cybercrime, and cyberwarfare. We are particularly interested in innovative, scalable, cost-effective solutions that can improve the security and resiliency of cyberspace. Solutions that adopt a multidisciplinary approach are particularly encouraged. Research areas of relevance would therefore include (but not be limited to) the following topics:

- Cybersecurity incident response
- Cybersecurity economic modeling and metrics
- Cybersecurity standards, policy, law, and regulation
- Cyber risk and vulnerability assessment
- Cybercrime
- Cyber warfare
- Cybersecurity education
- Cyber forensic tools, techniques, and analysis
- Cyber threat modeling analysis
- Visual analytics for cybersecurity
- Cybersecurity testbeds, tools, methodologies
- Active and passive cyber defense techniques
- Insider threat detection and prevention
• Critical infrastructure protection
• Intrusion detection and prevention
• Botnet detection and mitigation

2. Important Dates

Deadline for paper submission: May 1, 2014
Notification of acceptance: July 1, 2014
Expected publication date: 2014

3. Submission

All submitted papers (limited to a maximum of 16 pages) must be written in English. We invite submission of original research articles—that is, articles that present research that has not been previously published nor is currently under review by other journals or conferences/symposia/workshops. Papers previously published as part of conference/workshop proceedings may be considered for publication in the special issue, provided that they are modified to contain at least 40 percent new/original content. Authors of such submissions must clearly indicate in a separate letter to the guest editor at the time of submission how their papers have been altered for this special issue. Moreover, authors must acknowledge their previous papers in the manuscript and resolve any potential copyright issues prior to submission.

All submissions will be reviewed by the guest editor, as well as by JHSEM senior editors and anonymous referees.

Formatting instructions and author guidelines for preparing the manuscript can be found at http://www.degruyter.com/jhsem. All manuscripts should be submitted through http://mc.manuscriptcentral.com/dgjhsen. The author(s) must clearly state in the cover letter that the paper is being submitted to the special issue.

4. Guest Editor

Sherali Zeadally
314 Little Library Building
College of Communication and Information
University of Kentucky
Lexington, KY 40506-0224
USA

Email: szeadally@uky.edu