Cyber Systems and Analytics Minitrack Introduction

Chad A. Bollmann
Naval Postgraduate School
cabollma@nps,edu

John D. Roth
Naval Postgraduate School
jdroth@nps.edu

James W. Scrofani
Naval Postgraduate School
jwscrofa@nps,edu

Abstract

Cyber Systems and associated analytics will enable a future where secure, cognitive technologies anticipate long- and short-term information needs, perceptively coordinate and adapt distributed sensors, and deliver timely and accurate information and recommendations to humans and machines. Effective designs will require machine-to-human, human-to-machine, and machine-to-machine collaboration. This minitrack invites original, technical research in the subject area.

1. Introduction

The issues associated with the intersection of data, devices, and implementation are the focus of the Cyber Systems and Analytics minitrack. Exploding numbers of devices generate exponentially-growing data; security, design, and handling of these systems and their data are often afterthoughts.

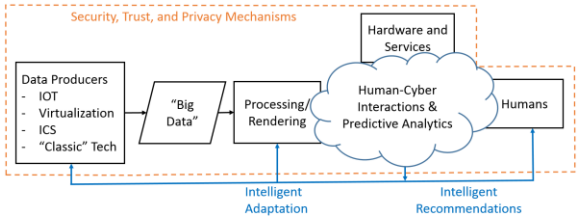

Figure 1. The confluence of data, devices, and implementation

These systems will enable a future where secure, cognitive technologies anticipate long- and short-term information needs, perceptively coordinate and adapt distributed sensors, and deliver timely and accurate information and recommendations to humans and machines. Effective designs will require machine-to-human, human-to-machine, and machine-to-machine collaboration.

This minitrack invites original, technical research in the subject area as well as theoretical work containing a rigorous evaluation of its proposals. We welcome papers containing evaluations of proposed tools and techniques. We are also interested in thorough survey papers that establish the state of the practice or directions for exploration. We are particularly interested in alternative approaches that challenge dominant implementations or status quo methodologies.

Specific areas of interest include, but are not limited to:

1. Intelligent Design, Organization, and Securing of "Big Data" including Industrial Control Systems, Cloud Systems, and IOT
   a. Secure cyber physical system design
   b. Design and implementation of trust and privacy in large distributed sensing environments
   c. Automation and optimization of data collection and analysis
   d. Command, control, and adaptation of collectors
   e. Alternative modeling, analysis, and representation methodologies
   f. Scalable network, data, and system intrusion detection and trust/privacy assurance methodologies
2. Human-Cyber Systems Interactions
   a. Orchestrated resource management to coordinate and adapt large sets of dynamic sensing methods in order to perceive complex systems and adversarial action
   b. Information valuation and decision search space methods for the large-scale problem of many targets and sensors
   c. Cognitive sensemaking architectures that assimilate, model, interpret, anticipate, and represent in complex, high-dimensional environments
   d. Human-computer symbiosis to support collaborative analysis and problem solving

e. Representation of and adaptation to adverse and emergent behavior through complex adaptive systems (CAS) theory
f. Innovations in machine-to-human, human-to-machine, and machine-to-machine collaboration, partnership, symbiosis.

2. HICSS-52 Submissions

For HICSS-52, three submissions were accepted to this minitrack. These papers were entitled: 1) Big Data SAVE: Secure Anonymous Vault Environment; 2) SiMoNa: A Proof-of-concept Domain-Specific Modeling Language for IoT Infographics; and 3) Trends in Detection and Characterization of Propaganda Bots.

These papers are exciting and enable cognitive cyber systems because they challenge existing practices by proposing new methods to address persistent concerns including scalable privacy and security; machine-human interaction and usability; and malicious cyber systems.

a. The volume, velocity, and heterogeneity of the data that will be generated by future cognitive systems demands new approaches to data storage and data handling. However, as with many emerging fields, security is often an afterthought. In *Big Data SAVE: Secure Anonymous Vault Environment*, the author addresses both the need for increased storage space and improved data handling and secure storage

   The author proposes an innovative storage system that can provide large-scale, low-overhead data security, which allows for anonymously-shared storage space, discrete levels of access, plausible deniability, and customizable degrees of overall protection (including warrant-proof). A promising factor of this new model is the use of a simple encryption algorithm (proven faster than industry-standard ciphers), that provides inherent attack resiliency and strong backward secrecy.

b. The Internet of Things (IoT) is generating unprecedented volumes of heterogeneous data at rates that, in many cases, have surpassed the ability of real-time human interpretation. Making sense of such data and taking appropriate subsequent actions are significant challenges. In *SiMoNa: A Proof-of-concept Domain-Specific Modeling Language for IoT Infographics*, the authors present a novel domain-specific modeling language (DSML) that enables the ability to create, connect, interact, and build interactive infographic presentations for IoT systems.

   Infographics are visual representations that provide a visual space for end-users to compare and analyze data, information, and knowledge in a more efficient form than traditional methods. Conceptualizing and implementing infographics in an IoT system can require significant planning and development for data scientists, graphic designers, and developers. The efficiency of the modeling language suggested is discussed and the infographics approach is validated using real-world use cases.

c. As cyber systems evolve, inherent vulnerabilities will be exposed and exploited. In, *Trends in Detection and Characterization of Propaganda Bots*, the authors survey the current state of research in propaganda botnet exploitation detection and characterization. Recent algorithms for detection of propaganda botnets and metrics by which their impact can be measured are discussed.

   Research in this area is particularly relevant considering the revelations of interference by malicious online actors and propaganda bots in the 2016 US Presidential elections, the UK's Brexit referendum, the Catalan independence vote in 2017, and numerous other major political events. These events have resulted in increased interest in understanding how to detect and characterize such threats.