Security Informatics
a SpringerOpen Journal

EDITORIAL Open Access

Introduction to a special issue on biologically inspired analysis of social systems: a security informatics perspective

Victor Asal[1], Kristin Glass[2*] and Richard Colbaugh[3]

Many national security challenges have at their core the problem of understanding and predicting the behavior of social systems, for instance in order to discover groups of individuals of interest, characterize their current activities and motivations, and anticipate the way they are likely to behave in the future. However, despite the allocation of vast resources to the task of analyzing and forecasting social behavior, the utility of such analysis remains limited. *Biologically inspired* (BI) approaches to analyzing complex systems appear to offer significant potential for this problem domain. For example, rapid progress is being made in the application of BI algorithms to challenging questions in the fields of financial market analysis, cyber security, and large-scale optimization. The current special issue brings together experts from a variety of fields to try and build on the potential of gaining traction on complex security problems by drawing on BI approaches. The genesis of the special issue was a series of workshops sponsored by the Department of Homeland Security on this theme. The special issue brings together an extraordinarily diverse group of researchers from fields across the social and hard science in areas such as biology, computer science, ecology, economics, engineering, psychology, and security studies.

As one might expect the papers in this issue often take very different approaches to examining the issue of how BI approaches can help us in analyzing complex systems to understand why and how individuals might behave in certain ways within the context of a social system and specifically within a security perspective. The papers examine issues as diverse as information analysis for intelligence purposes, how to respond to, or predict the growing threat of cyber warfare how to understand the lethality of different terrorist organization and how leaders can help individuals in their organization deal more effectively with the increased stress that a more diffuse and dangerous security environment has engendered. The authors use a wide array of approaches from computational experiments, to agent based modeling and ethnographic studies. Despite the diversity we believe that the papers hold together very well as a broader and multi-disciplinary effort to increase our understanding of how *Biologically inspired* can better help us understand the changing security environment the United States currently faces.

Rafe Sagarin and Terence Taylor provide a broad theoretical overview to how our understanding of biological evolutionary systems and the frameworks that have been developed to think about them can be applied to the security challenges that societies face. Saragin and Taylor are particularly interested in how our understanding of natural adaptability can be applied to the social problems of security. They provide a very useful discussion of adaptability that clarifies why the theoretical meaning of adaptability which is often used in security contexts is unclear and counterproductive. By clarifying the concept of adaptability and drawing directly from existing biological knowledge about the concept Sagarin and Taylor are able to outline four useful lessons which so far have not been applied in a security context but which they make a compelling argument would be much to our advantage if they were.

Also drawing on a broad BI inspired perspective, Paul Ormerod's paper leverages evolutionary theory to create an agent based modeling (ABM) approach to help better understand the distribution of fatalities in terrorist attacks. Basing his analysis on data of such attacks Ormerod focuses on dealing with the problem that such attacks are, like many human phenomena, heavily right skewed. From a cultural evolutionary theory perspective Ormerod argues that "copying" is a better explanation of human behavior as it relates to the lethal question at

* Correspondence: klglass@sandia.gov
[2]Sandia National Laboratories, New Mexico, USA
Full list of author information is available at the end of the article

hand then the often used economic perspective of rationality. Testing this argument with 1,000 separate solutions of the ABM model he has created, Ormerod finds evidence that the evolutionary theory argument is substantive and suggests the utility of applying this approach to a wider array of security challenges.

Several of the papers in the issue address the growing challenge of cyber-attacks. Laura McNamara argues that this growing threat is one that demands creative thinking and the exploitation of theoretical frameworks that will allow the security community to analyze this challenge creatively. McNamara points out that computational science has been drawn to BI inspired perspectives for a long time and has served to inspire important creative thinking about a wide array of computational problems. McNamara follows this established tradition in computational modeling and simulation and also applies it to the realm of cyber-warfare. Using ethnographic evidence from years of fieldwork with experts in national security McNamara argues that frameworks that help experts structure their thinking about the threats of cyber-warfare provide a useful and important tool to better think about the threats they are trying to deal with in their work. Specifically McNamara suggests that the theoretical frameworks of *information ecology*, *activity theory,* and *participatory modeling are important tools for helping the security community to model the problem of cyber-warfare.*

Richard Colbaugh and Kristin Glass also try to contribute to a better understanding of the cyber threat that McNamara discusses with a paper that forwards our understanding of human social activity by combining a biologically inspired modeling perspective with sophisticated computational analytics to deal with the challenges of the current security environment. Specifically, Colbaugh and Glass describe an ongoing effort to predict the outcomes of social diffusion processes using a dynamic network approach. Their approach is grounded in findings in biology that stochastic hybrid dynamical systems are a productive way to understand a network's community and core periphery structure and the impact of this structure on network dynamics. They build on this foundation to develop an effective approach to predicting the extent of the spread of political "memes" in social media, and extend the approach to provide predictive capabilities for the growing security threats of large-scale protests and politically motivated cyber attacks.

Like Colbaugh and Glass, Neal Holtschulte and Melanie Moses also look to a BI approach to examine the issue of cyber attacks. Using an experimental approach Holtschulte and Moses draw on the biological thinking about pathogens and immune systems to create an effective immune system design they call the Robust Adaptive Decentralized Search and Automated Response (RADAR) to better respond to the growing cyber threat. Their experimental approach allows them to investigate how connected computers are able to repair and respond to attacks and to deal with vulnerabilities in the system. Holtschulte and Moses find that connectivity has interesting and not necessarily intuitive impacts on the degree of diversity in the system and that this diversity in complexity can vary by the type of node.

The paper by Craig Vineyard, Stephen Verzi , Michael Bernard, Shawn Taylor, Irene Dubicka, and Thomas Caudell identifies one of the most important and challenging problems facing the security community in the new environment created with the rise of potentially devastating threats now posed by violent non-state actors (VNSA). Given the diffuse nature of these new threats, intelligence analysts need to process very large amounts of data and strive to detect potentially threatening connections between different bits of diverse data. Drawing from biological investigations of the brain in neuroscience the authors lay out a multi-model information approach to store information and to automate an association mechanism. Their paper provides a fascinating simple example that illustrates the model's functionality and promise.

While Paul Bartone's paper comes from a completely different direction then many of the other papers in this special issue, it actually deals with a different facet of the same larger complex information challenge. Bartone's paper focuses on how leaders should work to increase individual and group stress resilience. The stress is created by and because of the very challenges the other special issue papers address. Since September 11^{th} the level of complexity and uncertainty in trying to deal with different and changing security threats has led to an increased level of stress amongst security forces who need to keep one step ahead of a wide spectrum of diverse threats. For some security personnel this increase in stress has led to serious health issues and a highly problematic decline in performance while other individuals facing similar challenges are not affected. Bartone provides a very useful review of the evidence for impact of psychological hardiness on how people deal with increased stress and then pulls together theory and findings from the literature to argue that strategies based on social influence theory offer a way forward to help security organizations increase the psychological hardiness of members of their organizations.

Overall we believe these papers help advance our understanding not only of how BI efforts can help us better deal with the new security challenges that societies face but also help our understanding of these threats in general. The papers underline the need to think creatively about the threat that comes from a

variety of entities and from a variety of strategies and tactics. The papers highlight the creative advantage of bringing together diverse disciplines to think outside the box and to meld approaches as diverse as computational modeling and ethnographic studies to create syntheses that are potentially greater than the sum of their parts. We hope you will agree. We would also like to take this opportunity to thank the authors, working with them and putting together this special issue has not only been a pleasure but has stimulated our brains to think in new directions.

Author details
[1]University at Albany, New York, USA. [2]Sandia National Laboratories, New Mexico, USA. [3]Sandia National Laboratories, New Mexico, USA.

Received: 14 September 2012 Accepted: 14 September 2012
Published: 6 November 2012

doi:10.1186/2190-8532-1-22
Cite this article as: Asal *et al.*: Introduction to a special issue on biologically inspired analysis of social systems: a security informatics perspective. *Security Informatics* 2012 **1**:22.