Security Informatics
a SpringerOpen Journal

REVIEW Open Access

Biologically-inspired analysis in the real world: computing, informatics, and ecologies of use

Laura A McNamara*

Abstract

Biological metaphors abound in computational modeling and simulation, inspiring creative and novel approaches to conceptualizing, representing, simulating and analyzing a wide range of phenomena. Proponents of this research suggest that biologically-inspired informatics have practical national security importance, because they represent a new way to analyze sociopolitical dynamics and trends, from terrorist recruitment to cyber warfare. However, translating innovative basic research into useful, usable, adoptable, and trustworthy tools that benefit the daily work of national security experts is challenging. Drawing on several years' worth of ethnographic fieldwork among national security experts, this paper suggests that information ecology, activity theory, and participatory modeling provide theoretical frameworks and practical suggestions to support design and development of useful, usable, and adoptable modeling and simulation approaches for complex national security challenges.

Background

Making analytic software useful, usable, and adoptable in the context of the United States' national security community is a difficult challenge. Not only is the "national security community" a massive, complicated, and heterogeneous set of institutions, but its members are responsible for providing timely and trustworthy assessments of significant trends. Analysts are taught to think critically about the data and information they are examining, as well as the cognitive biases they bring to its interpretation. Critical thinking and skepticism often extend to innovative and exotic technologies, such as new informatics tools, particularly those developed outside the analytic workplace. As Philip Huxtable, a researcher at the United States Joint Forces Command, has observed, national security analysts are not likely to adopt a technology if they do not "...trust the tool or method's validity and usefulness for their tasks" [1].

Biologically-inspired algorithms and frameworks are certainly innovative and exotic. Although biological metaphors have long influenced computer science (for example, in the form of neural nets), innovations in biology have more recently inspired creative, interdisciplinary approaches to conceptualizing, representing, simulating and analyzing social, economic and cultural trends. In relation to the national security community, proponents of biologically-inspired informatics believe these approaches might shed light on trends and threats that are not well-addressed by traditional social science theory and methods. However, before biologically-inspired informatics can be usefully applied in national security settings, proponents must pay attention to the challenge of translating innovative science into working tools. This is a complicated process [2]; innovation and novelty alone will not guarantee that biologically-inspired informatics will find a productive niche in national security analysis and decision-making.

In keeping with the biologically-inspired theme of this special issue, this essay draws on Nardi and O'Day's metaphor of information ecologies as a holistic framework for understanding the relationships among tools, people, and information in potential contexts of use [3]. Approaching contexts of use from an ecological perspective can help developers appreciate the design challenges associated with introducing new technologies into existing organizational cultures. Two complementary methodological frameworks, activity theory and participatory modeling, provide practical guidance for translating ecological perspectives into usable and useful design knowledge, while building productive working relationships with the people responsible for making sense of complex national security challenges. Hopefully, this essay will

Correspondence: lamcnam@sandia.gov
Sandia National Laboratories, PO Box 5800, MS 0519, Albuquerque, NM 87185-0519, USA

inspire proponents of biologically-inspired informatics to seek new ways of engaging national security analysts and decision-makers as informed and committed stakeholders in informatics research and development.

New problems, new methods

The 9/11 attacks highlighted significant problems with information collection, sharing, and analysis in the United States' national security community. Since 9/11, the United States has taken many steps to improve the analysis and communication of intelligence assessments. Significant investments in analytic practices have led to new paradigms for evaluating intelligence information and communicating assessments to decision-makers; i.e., the Analysis of Competing Hypotheses (ACH) and Words of Estimative Probabilities (WEP) [4,5]. As part of this reform, government agencies have sought out computer software and hardware that will improve the processes and products of intelligence analysis: not just new search engines and databases, but information visualization and visual analytics platforms, computer-supported collaborative environments, even classified versions of social media such as Twitter and Facebook [6]. These days, both military and civilian agencies are awash in new software, from 'grass-roots' analyst-driven initiatives such as the collaborative platforms of Intellipedia and A-Space [7] to vendor-provided visual analytics software, such as Analysts' Notebook and Palantir [8,9].

Informatics research and development is also playing a role in the evolution of analytic practice and technology. Of particular importance is the recent emergence of the interdisciplinary field of computational social science, which is a trading zone [10] that brings framings from other disciplines, such as biological metaphors, to bear on the analysis of social, political, and cultural trends. The new methods and theories have emerged from these intersections have researchers extolling the potential for interdisciplinary computational science to "...[extend] our cognitive range [and provide] a new means of knowing the world, which is fundamentally different from that of experimental control" [11].

As computational social science has grown, researchers have sought funding and application areas in the national security community [12,13]. Computational modeling and simulation have long track record of informing government decision-making, and decision-makers are hungry for better forecasting capabilities, even rudimentary ones, to support resource allocation decisions and timely policy, operational, and tactical responses in an uncertain and rapidly changing world [14-18]. As a result, a number of national security thought leaders have suggested that new computational science techniques, including a wide range of modeling, simulation, and informatics approaches, might give decision-makers a jump on complex, seemingly intractable sociopolitical trends. Perhaps the best-known funding vehicle for this intersection is the Human Social, Cultural, and Behavior (HSCB) program, under the Director of Defense Research and Engineering (DDR&E) in the Office of the Secretary of Defense (OSD). Since its inception, HSCB has itself funded over fifty research projects in government, industry and academia [16,17]. Overall, the DoD's publicly available research portfolio indicates at least thirty different interdisciplinary sociocultural research and development projects [17], many of which involve computational modeling, simulation, and informatics [17-21].

Such research investments have led to tremendous innovation in algorithms, data, and technology. Yet the long-term viability of any application depends less on its scientific novelty than whether it is presented in a way that people can use it.[a] Unfortunately, very little attention been paid to the problem of translating the innovations of biologically-inspired informatics into useful, usable, and adoptable tool for the analysts who ostensibly comprise the intended user communities [20,22,23].

Usability, utility, and adoptability

Usability, utility, and adoptability each describe distinct but interrelated qualities associated with the potential impact of a new technology; i.e., the degree to which humans can employ an artifact to achieve a desired goal, end, or effect on the world around them. Usability refers to such qualities as learnability, efficiency, and whether important operations are easily performed and remembered. Utility or usefulness describes the degree to which people can use the technology to perform tasks that matter to them, and a rich literature provides guidance and techniques for assessing these qualities [22-27]. Lastly, adoptability addresses the goodness-of-fit between a tool or technology and the sociocultural characteristics of an intended user community [28].

The relationships among usability, utility, and adoptability are complicated: although they can be mutually reinforcing, none is sufficient (nor perhaps even necessary) to achieve the other two. This is because all are context- and user-dependent. For example, a software application that has a highly learnable and efficient interface may not provide capabilities that align well with a user community's core tasks. Similarly, high utility can overcome mediocre usability, as when technically proficient users are comfortable employing unfinished software. A prototype optimization toolkit that incorporates a new solver may be useful enough that engineers are willing to overlook a nonexistent interface or annoying bugs, at least temporarily. Lastly, both usability and

utility tend to emphasize the relationship between a human user and a particular technology; neither quite addresses whether or not tools can be adopted into existing work environments. Adoptability brings additional consideration to higher-order social and organizational factors that may enable and constrain tool adoption, such as norms for technology acquisition and organizational modes of communication [28].

A vignette may help explain how usability, utility, and adoptability play out in the development and deployment of new software tools. Several years ago, the author became acquainted with a computer science research group embedded in a large government agency. Seeking to have a positive impact on analytic approaches in the agency, a few of the computer scientists decided to redesign a search engine that analysts commonly used with the agency's largest database. The researchers selected the project after hearing analysts complain about the non-intuitive nature of the current search engine. They elicited suggestions from experienced personnel to ensure that the new search engine would provide smoother navigation experience than the existing one. When the prototype was ready, the team invited analysts to test it and provide feedback. The testers praised the simplicity and learnability of the interface and the efficiency with which they could review records in the database.

Surprisingly, however, the new search engine was not widely adopted; in fact, only a handful of analysts expressed interest in getting the interface installed on their desktop machines. In discussing this mystery with the research and development team and with some of the agency's analysts, it became apparent that the older, clunkier search engine had considerable inertia in the work environment. For one thing, it was well-integrated into the suite of commercial tools that most analysts were already using. Not only would switching to the new search engine require additional steps to export and import data, but searching the database was only one of many tasks analysts did in a day, and time spent retrieving information was relatively low compared to other work tasks. In addition, because of cyber security concerns, the agency's software acquisition policies required extensive review of new code, even when developed internally. Lastly, as one analyst explained, she had "grown up" using the older search engine and felt comfortable with it. She believed her peers felt similarly; after all, it did not appear that using the existing search engine was hurting her group's overall performance. Such factors made it difficult for the research group's innovation to gain the momentum necessary for successful adoption.

The search engine project described in the preceding vignette would probably have benefitted from more structured and careful elicitation, documentation, and management of basic technology and user requirements. The field of software engineering provides extensive guidance in this regard, including user-oriented design approaches that emphasize the importance of user priorities, tasks, and workflows in the development of new tools (e.g., [25,29]). Yet the intersection of "national security" and "biologically-inspired security informatics" introduces challenges to usability, utility, and adoptability that may not be adequately addressed by standard software engineering paradigms, even those that emphasize active user participation in the design, development, and testing of new technologies. Computer scientist Jean Scholtz has written that developing applications that take advantage of innovative computational science, such as the biologically-inspired research described in this issue, challenge mainstream software development paradigms [30]. These challenges are due to the organizational complexity and cognitive demands of national security analysis; cultural differences between researchers and national security analysts; and the interdisciplinary character of computational modeling and simulation itself. Each is briefly reviewed below.

First, the national security community is diverse, with workplaces that include trailers on forward operating bases in Afghanistan or (until recently) Iraq; buzzing cubicle farms in federal office buildings in Maryland or Virginia, and secure facilities located in bland industrial parks or university campuses around the country. Even analysts working on similar problems within the same agency may have very different customer sets, geographical focus areas, timelines, tools and technologies, and data sources. To make matters more complicated, multiple analytic groups in different agencies can be working on similar issues with quite different methodologies. Simply identifying the appropriate user community for a new software tool, analytic method or technique is a non-trivial problem, even for people within the national security community.

Related to this is the fact that informatics research and development tends to occur in industrial and/or academic domains that are organizationally, physically, and culturally distinct from the bureaucratic domains of the national security community. It is helpful to think of each domain as a distinct epistemic culture. These are cross-institutional communities whose members are engaged in shared activities, discussions, objectives, techniques, technologies, and practices, all of which have emerged over time as people pursue collectively-valued forms of knowledge [31].

The epistemic culture of computational social science tends to be grounded in academic, private nonprofit, and/or industrial research settings. It is intensely interdisciplinary, and emphasizes computational modeling and simulation as an empirical approach to the study of

social phenomena for which data can be difficult to acquire. In contrast, national security analysis and decision-making is located squarely in the realm of government and deals with real-world, high-consequence outcomes on a daily basis. National security analysts, civilian and military, are responsible for identifying, assessing, and ensuring that the United States can interdict potential tactical and strategic threats. Analysts identify important issues and respond to difficult questions, piecing together information sources that may be incomplete, uncertain, ambiguous, evolving, even conflicting or deceptive. Analytic assessments are routinely promulgated throughout the intelligence community, shared across multiple government agencies, and may find their way into policy discussions at very high levels of government, where they may be cited to support significantly risky courses of action. As most analysts can attest, errors in judgment or communication can disastrous for national security, which is one of the most politically charged and least forgiving areas of American public life. Rarely, if ever, do computer science researchers face the possibility of being held responsible for decision outcomes that may be literally existential.

Given explosive growth in information, analytical techniques, and computing power over the past two decades, it is not surprising that both the research and the policy- and decision-making communities are seeking practical benefit from computationally-driven analytical techniques. At the same time, the potential stakeholders may find biologically-inspired informatics opaque, particularly when projects leverage cross-disciplinary methods and frameworks in conceptually innovative and risky ways. Because of this gulf, ". . .it is frequently the case that policy-makers dismiss academic research as too theoretical, unrelated to the actual problems they are wrestling with, or in other ways irrelevant to their concerns" [32].

Last, the interdisciplinary novelty of biologically-inspired computational social modeling and simulation is itself problematic, because the rapid evolution and heterogeneity of these projects can make it difficult for non-practitioners to judge the quality of a model and/or its simulation outputs [33,34]. Anyone who has tried to rid their kitchen of sugar ants can appreciate the communicative talents and collective resilience of the ant colony. However, the assumptions and constraints associated with ant colony-inspired mathematical models of social networks or power markets are probably not intuitive to all-source intelligence analysts who lack familiarity with the mathematical formalisms of ant colony-inspired algorithms [35,36]. The ability to develop a good sense of how one's tools interact with data and information is a major factor that influences adoptability: national security work products can have significant existential consequences, and trust in one's work processes is perhaps the most important metric that attends technology design activities in this space.

Wanted: a new development model

Philip Huxtable and others who are familiar with efforts to bring modeling and simulation into national security analysis have emphasized the importance of breaking down organizational barriers between researchers and government analysts, so that analysts can develop "an understanding of [the tool's] strengths and weaknesses and thus develop confidence in using it for tasks on which significant decisions (and their professional reputations) will be based" [1,23,33,34]. Yet within the national security community, most modeling, simulation, and other informatics projects follow an "over the fence" development model: researchers develop and demonstrate working systems in a research setting; the resulting systems are then thrown "over the fence" to the users who are presumably waiting to receive them. Even when informatics projects have explicitly identified an impact area or use context, much of the research tends to occur at a distance from the analytic workplace. Even national security R&D programs that are organizationally proximate to analytic workplaces are not necessarily integrated with the analytic and/or decision-making processes they seek to affect. This is not a new problem: As Huxtable laments, "Everyone in the community knows [the over the fence] approach doesn't work, yet the vast majority of analytic capability projects are executed this way, and most are unlikely to transition in any way that makes use of their apparent potential" [1].

For the national security community to realize return on its informatics investments, proponents of such methodologies must pay far greater attention to the characteristics of end-user communities. In this regard, social science theory and method can provide valuable frameworks and techniques for identifying key aspects of the organizational, political, and social contexts of national security and relating these to tool development. In the following pages, I suggest that information ecology can help proponents of biosecurity innovations appreciate the complex challenges associated with technology adoption in the national security community. Activity theory provides a complementary set of techniques and methods for eliciting the key aspects of work environments that bear on the usability, utility, and adoptability of new tools. Developing richer relationships with user communities inside the national security environment opens the door to effective collaboration, such as participatory modeling, a development approach specifically aimed at cultivating informed and committed stakeholders for modeling and simulation technologies.

Moving beyond "the user:" information ecologies

Over the past fifty years, the fields of human factors and human-computer interaction have established a set of well-recognized principles for designing technologies that fit the physiological and cognitive requirements of human users. However, the rapid evolution of personal computing, the Internet, and the explosion of collaborative technologies and social media has expanded technology design paradigms, so that it is no longer enough to consider the Everyman User in design. Instead, design thinking now emphasizes humans as actors engaged in the act of sense making: the assembly of meaningful narratives that explain what is happening, so that actors can respond appropriately. Technology must be designed to enable and empower people to engage, assess and act upon the social, political, and cultural contexts in which they are embedded.

One provocative example of this contextual, more humanistic trend in design thinking is Bonnie Nardi and Vicki O'Day's discussion of information ecologies [3]. Nardi and O'Day's biological metaphor makes this framework particularly appropriate for this special issue of Security Informatics. More importantly, however, the metaphorical casting of an office workplace as a living ecology helps break down taken-for-granted assumptions about what makes a technology "better" than its predecessors.

The ecologies that interest Nardi and O'Day are human settings where people collectively pursue the creation, maintenance, exchange, and retrieval of information. Libraries, school classrooms, the cubicle farms of an intelligence agency: these are not just workplaces, but living systems that engage human actors in meaningful activity. Importantly, unlike biological ecologies, information ecologies are socially purposive: inhabitants engage in goal-directed behavior toward the accomplishment of a broader, socially-sanctioned outcome - for example, the monitoring and interdiction of sub-state criminal networks that are involved in human trafficking. Because information ecologies are living and dynamic sets of "...people, practices, values and technologies in a particular local environment," write Nardi and O'Day, design work must begin with an understanding of the "...human activities that are served by technology" ([3]; emphasis added). They describe how different elements of an ecology - tools, specific methods, even humans who occupy specific roles - become established as niches that provide specific functions in support of human activity. As Nardi and O'Day explain, the most important niches are occupied by keystone species whose removal fundamentally change the nature of the ecosystem, even threaten its survival.

Consider the search engine vignette in relation to Nardi and O'Day's ecologies. The story illustrates the difficulty of changing a single element in a system without accounting for the full range of activities in which that element is embedded. Perhaps the search engine occupied a critical niche: i.e., human users had over time connected it with other elements of the system to support myriad functions, such as communication among analysts and information traceability. Even though the developers had visibly improved the search engine's primary function - retrieving information from a database - the existing system was deeply embedded in other processes and functions. Technologies that span multiple users, such search engines or email services, often play a keystone role in information ecologies. As Nardi and O'Day point out, removal of a keystone species can jeopardize the very survival of an ecology; for example, many forms of analytic work might grind to a halt if the search engine disappeared. Not surprisingly, people tend to react strongly (and often negatively) to abrupt changes in keystone species, because so many of their activities depend on the functions such species afford.

Yet innovation in system elements, even in keystone species, is important if an information ecology is to adapt and grow. Just as natural ecologies survive by adapting to the pressures of an evolving environment, so are information ecologies engaged in ongoing and dynamic process of evolution, as people perceive and respond to emerging trends and pressures. The fact of evolution should be inspiring to new technology developers, because it means that opportunities for innovation are always present in an information ecology. Indeed, information ecologies thrive on diversity in people, tools, roles, tasks, activities, technologies, and resources, because diversity lends resilience when external pressures or the failure of some internal element put stress on the ecology's systems [3].

Imaginatively recasting national security software users as species in a complex information ecology should give proponents of biologically-inspired informatics technologies pause and optimism. It is naïve, and probably counterproductive, to assume that "better" informatics technologies will be embraced by national security decision-makers purely because these technologies embody some type of scientific, mathematical, or computational superiority. However, because the national security workplace is a living ecology, there are always opportunities for cultivating and establishing viable niches for new sense making activities, with their accompanying technologies and expertise. The challenge is decomposing the ecology in question to identify the most viable niches for an envisioned innovation.

Ecologies and activities

Nardi and O'Day's metaphorical mapping between biological ecologies and office workplaces helps us re-think

our assumptions about human-tool relationships. However, its practical applications may not be immediately apparent. At this point, it is appropriate to introduce a related framework for studying human-technology interaction known as activity theory. Information ecology and activity theory are complementary, which is not coincidental; Bonnie Nardi is one of the United States' foremost proponents of activity theory-based approaches to technology design and development [37]. Like information ecology, activity theory emphasizes the embeddedness of individual human activity in broader systems of social relationships. However, activity theory's framework has very clear methodological implications for eliciting contextual factors related to the design and development of usable, useful, and adoptable software.

Activity theory is derived from the work of Soviet developmental psychology, which emphasized the importance of cultural and contextual factors in shaping human cognitive development and consciousness. In the 1980s, Scandinavian, British, and later American researchers adopted the principles of activity theory as an alternative approach to the individualist paradigms that dominated Western research on human communication, reasoning, work and learning [37-39]. Today, activity theory is widely seen as an important "post-cognitivist" and "post-technologist" approach to human-computer interaction and system engineering because it provides accessible and highly practical guidance for mapping what people are doing, what they are using and creating as they do it, and how social, organizational, and cultural factors make their activity meaningful [25,37,39].

Figure 1 illustrates activity theory's main conceptual relationships. As the name suggests, activity theory begins with the activity, or purposeful, goal-directed human action, as the unit of analysis. Activities comprise human actors who put various resources or instruments to use toward achievement of an object. At this very basic level, activity theory resembles established theories of human-computer interaction, such as Card and Moran's GOMS [39,40]. However, activity theory goes beyond the immediacy of micro-interactions between individuals and technologies to examine the relationship between individuals and social collectives.

Of particular importance in this regard is the concept of outcome, which indicates the broader set of values and purpose that lend meaning to human action. Outcomes explain why an individual's work matters to a larger set of human actors and individuals. In activity theory, that larger set is captured in concept of a community, which refers to objectively defined social location in which an actor is embedded (e.g., an intelligence analyst in a three-letter agency), as well as the actor's subjective sense of membership and responsibility vis-à-vis other actors (e.g., a young analyst is part of a group of novices being mentored by a particular expert). Roles and rules provide structure and regularity to communities. They comprise a mix of formal and informal elements that not only give individuals a sense of social location vis-à-vis other members; but which also support the achievement of organizational purpose by formalizing

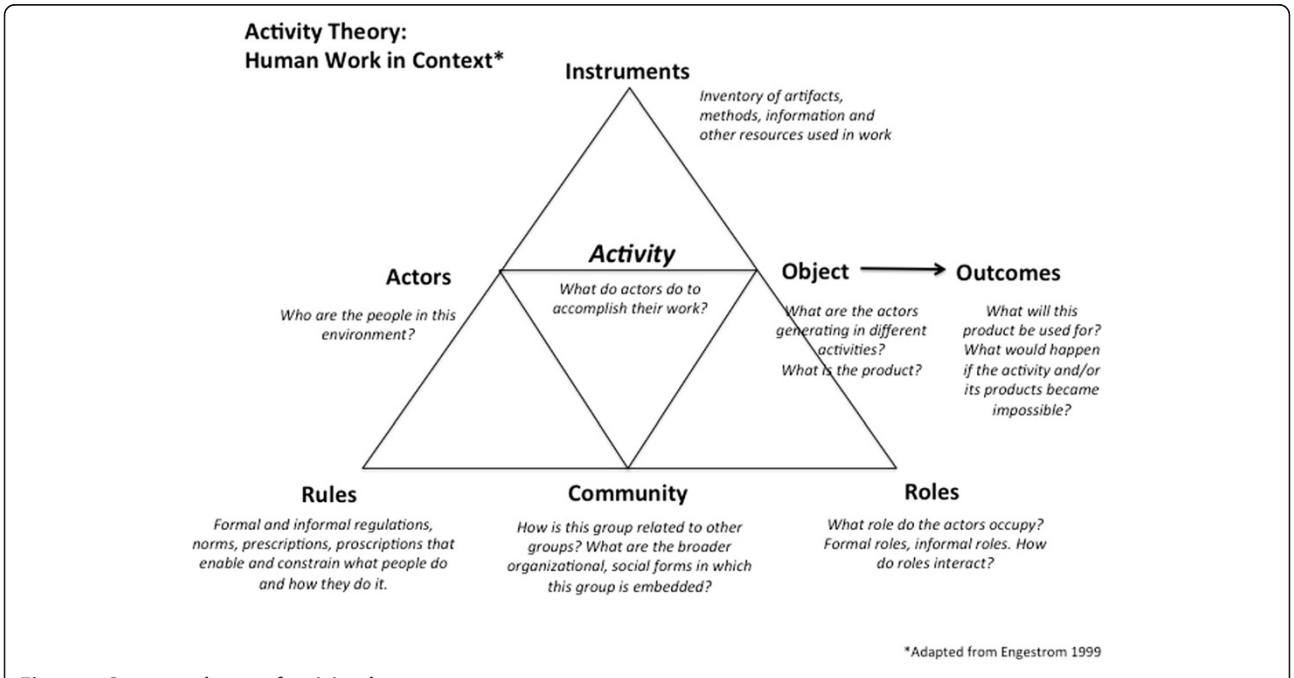

Figure 1 Conceptual map of activity theory.

the distribution of responsibilities, resources, power, and labor across a community.

Over the past decade, activity theory has become an increasingly popular framework because the approach generates rich descriptive data that helps designers identify relationships that bear on the introduction of new technologies. Although a full description of activity theory's methods is beyond the scope of this article, some of the questions that that emerge from activity theoretic approach are depicted in Figure 1. These questions can be used to identify and categorize key elements in a work environment. For example, a hypothetical activity might consist of an intelligence analyst (the actor, occupying a particular role) who uses a search engine (a computer software/hardware instrument) to identify high-quality satellite imagery covering a particular geographical region during a given time period (identifying imagery is object of the search activity; imagery is also an instrument). Once the imagery is retrieved, the analyst will conduct a systematic search of the imagery (the imagery, the displays, the software, and even the analyst's search methods are instruments) to identify indicators of illicit activity (the object of the search). The analyst will assemble a report (the object of the search and analysis activities), which she will mark with appropriate distribution restrictions (marking requirements are rules) so that she can distribute the report to law enforcement (which she identifies as part of the national security community) to support an investigation into maritime criminal activity (the outcome).

Activity theoretic studies are typically iterative, because digging into one area of the framework is likely to raise questions or reveal information about other areas. For example, as people identify instruments and resources, they will probably describe how they use particular resources in performing various tasks, which leads to identifying activities, their objects, and the intended outcomes. Indeed, when trying to build familiarity with a new user community, it is often easiest to begin at the apex of the triangle and conduct an inventory of the instruments that people use in their work. This is because physical resources are relatively easy to identify and can include computers, software, books, maps, communication devices, and displays; as well as key places - offices, conference rooms, cubicles.

Activity theory is not the only way to approach studies of work, but it does provide an efficient way to bootstrap one's knowledge of a work context. It also helps designers identify specific work activities that deserve more intensive study, as through cognitive task analysis [41,42]. Most importantly, however, activity theory helps technology developers build relationships with the people whose work they seek to impact: as Kuutti points out, activity theory "...aims at reconstructing contexts in practice so that people are not just objects or subordinate parts, but regain their role as creators" [43]. In this sense, activity theory is complementary with another paradigm that may be useful to proponents of biologically-informed informatics: namely, participatory modeling.

Cultivating a niche: participatory modeling

Participatory modeling is a methodology that leverages the principles of user-oriented design to ensure that computational applications, including modeling, simulation, and informatics technologies, are comprehensible to stakeholders in a decision space. Participatory approaches use the development of analytic technologies, such as models, to integrate multiple goals and perspectives across stakeholder communities. Participatory approaches developed in the context of natural resource decision-making, where stakeholders often have diverse and conflicting goals for management of shared resources. Successful management of shared resources requires that stakeholders comprehend and trust the decision-making process, including data, information, and analysis. The participatory modeling philosophy is expressed in a number of methodological frameworks that vary according to the mechanisms and degree of stakeholder participation: Barreteau has noted, participatory modeling and simulation paradigms are quite diverse in the details of their implementation [44,45]. However, all seek to build comprehensibility and trust by incorporating stakeholders as active participants in the modeling process: negotiating a shared conceptual framework, identifying data and information, examining and mitigating sources of bias, establishing appropriate contexts of use, and setting goals for verification and validation of the model's software and products.

This emphasis on trust, transparency, and the creation of comprehensible analytic processes and tools maps well to the challenges that informatics proponents face when engaging the national security community. As previously discussed, analysts are often reluctant to adopt computational technologies that they do not understand; it makes sense that incorporating end-users in development process is might generate the contextual knowledge required to make sense of a modeling approach. If nothing else, coupling participatory modeling approaches with the activity theoretic approach described above can help technology developers appreciate the goals, constraints, outcomes, and impacts associated with national security analysis and decision-making. However, participatory modeling is also consonant with the political philosophy of activity theory, which explicitly calls for users to have an ownership role in the design and development of technologies that will impact their work and lives. In addition, activity theoretic investigations of national security workplaces engage users in the derivation of design principles careful study of a use environment. The resulting relationships can be leveraged

toward participatory development of next-generation informatics technologies. In doing so, developers can mitigate lack-of-knowledge issues that might otherwise prevent end-users from, for example, appreciating the benefits and limitations and associated with using bee colony metaphors to understand political memes.

Review and conclusion

This paper has provided a cursory overview of three related theoretical frameworks - information ecologies, activity theory, and participatory modeling - for approaching design challenges associated with informatics for national security decision-making. Mainstream software engineering is a starting point for rethinking how we introduce new analytic approaches into the national security workplace. For example, professional associations have identified standards associated with basic usability, while the software engineering literature provides a variety of methods for eliciting user requirements. However, while an elegant user interface and well-written documentation can enhance a tool's usability, utility, and adoptability, the cognitive and epistemological complexity of interdisciplinary informatics requires additional investment in building relationships between researchers and intended user communities.

Humanistic, holistic frameworks like information ecology, activity theory, and participatory modeling emphasize that qualities like usability, utility, and adoptability are more than "interface deep." Successful transition of new informatics technologies will require the entire community - funders, users, researchers - to evolve models of success beyond software- and model-oriented measures, such as algorithmic elegance or the quality of software implementation. Instead, when people adopt an innovation, they are making a conscious (if subtle) decision to change how they engage with some area of their lives, work, and perhaps even their relationships with a community of peers. Not only can new tools change how individuals solve problems, but the adoption of new technologies can stimulate far-reaching changes in community identity and culture, challenging established norms for "who we are" and "how we do things here" [46].

In this regard, proponents of analytic innovations, including biologically-inspired informatics, must ask themselves if methodological improvements in national security analysis will be driven by technological innovation. From the perspective of ecology and activity theory, this assumption is tremendously naïve because it neglects the agency of human analysts as users who decide how they will perform their work. These theories suggest that novel computational science approaches can only be successful if everyone - funders, researchers, and analysts - actively seek ways to bridge the organizational, cultural, and epistemological divides that separate "researchers" from "analysts."

In this regard, proponents of national security informatics should look for ways to incorporate analysts and researchers together into the development of new technologies. For example, a specialist analysis cell might be asked to design its own call for proposals in conjunction with a funding agency. The deal would require a commitment from the analyst cell and a research team to work side-by-side for a period of time. Not only would the researchers begin to understand the analysts' activities, resources, goals, outcomes, and constituents; but the analysts would have the opportunity to become familiar with researchers' techniques and theories, so that approaches like the biologically-inspired ones described in this issue become less exotic and more comfortable. Frameworks such as activity theory can help guide these relationships; questions derived from its elements can help technology designers and analysts jointly identify critical elements and relationships in a workplace. This structured relationship building can establish foundational trust relationships, adding momentum to the participatory development of a new informatics technology.

If modeling and simulation technologies are to bring the revolutionary analytical changes that they promise, modelers and analysts alike must be encouraged to recast themselves as co-owners of new technologies. In particular, researchers who want their technologies to have real-world impacts must become familiar with, even become participating members of, the very security ecologies they seek to influence. Just as biologically-inspired informatics are an interdisciplinary creation, so too must their application bring disparate communities into collaborative relationships. Paying attention to context is critical to establish a viable niche for informatics, modeling, and simulation as methodological species that add diversity and strength to the constantly evolving ecology of national security.

Endnotes

[a]A reviewer of an earlier draft pointed out that usability, utility, and adoptability are not the only problems associated with using new computational science approaches in national security. In fact, they might not even be the most important ones: Empirical evaluation using high-quality datasets is rarely performed; and standards for verification, validation, and accreditation technologies are largely undefined. While the paucity of validation quality data and robust verification, validation, and accreditation approaches are indeed problematic, that topic is beyond the scope of this paper.

Competing interests

The author declare that he have no competing interests.

Acknowledgements

The author wishes to thank Jennifer Perry of the Defense Threat Reduction Agency's Advanced Systems and Concepts Office for her insight and support of work related to this paper. In addition, Timothy Trucano, Rich Colbaugh, Kristen Glass, and numerous intelligence analysts in several federal

workplaces have contributed to the author's thinking on the topics discussed in this paper. Any errors or omissions are solely the responsibility of the author.
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Received: 16 January 2012 Accepted: 7 September 2012
Published: 6 November 2012

References

1. P. Huxtable, Leveraging Computational Social Science for National Security, in *Challenges in Computational Social Modeling and Simulation for National Security Decision Making*, ed. by L. McNamara, T. Trucano, C. Gieseler (Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Ft. Belvoir, VA, 2011), pp. 157–168
2. L.M. Murphy, P.L. Edwards, *"Bridging the Valley of Death: Transitioning from Public Sector to Private Sector Funding," National Renewable Energy Laboratory (NREL)* (Golden, Colorado, 2003)
3. B. Nardi, V.L. O'Day, *Information Ecologies: Using Technology with Heart* (MIT Press, Boston, 1996)
4. National Intelligence Council, *Iran: Nuclear Intentions and Capabilities* (Office of the Director of National Intelligence, Washington, DC, 2007)
5. National Commission on Terrorist Attacks Against the United States, *The 9/11 Commission Report* (United States Government Printing Office, Washington, DC, 2004)
6. L. Resnyansky, The internet and the changing nature of intelligence. IEEE Technol. Soc. Mag. **28**, 41–48 (2009). Spring 2009
7. D.C. Andrus, *The Wiki and the Blog: Toward A Complex Adaptive Intelligence Community* (Central Intelligence Agency, Washington, DC, 2005). June 15
8. *Palantir Technologies*. Available: http://www.palantirtech.com/
9. *Analyst's Notebook*. Available: http://www.coplink.com/us/products–services/analysis-product-line/analysts-notebook
10. P. Galison, *Image and Logic: A Material Culture of Microphysics* (University of Chicago, Chicago, 1997)
11. D. Byrne, Simulation - a way forward. Sociol. Res. Online **2** (1997). http://www.socresonline.org.uk/socresonline/2/2/4.html
12. C. Cioffi-Revilla, S. O'Brien, *"Computational Analysis in US Foreign and Defense Policy," presented at the First International Conference on Computational Cultural Dynamics* (College Park, MD, 2007)
13. Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences* (National Research Council, National Academy of Sciences, Washington, DC, 2011)
14. S. Magnuson, Military swimming in sensors and drowning in data. Nat. Def. (2010). http://www.nationaldefensemagazine.org/archive/2010/January/Pages/Military%E2%80%98SwimmingInSensorsandDrowninginData%E2%80%99.aspx, 2010
15. R.L. Popp, D. Allen, C. Cioffi-Revilla, Utilizing Information and Social Science Technology to Understand and Counter the Twenty-First Century Strategic Threat, in *Emergent Information Technologies and Enabling Policies for Counter-Terrorism*, ed. by R.L. Popp, J. Yen (IEEE/John Wiley and Sons, Hoboken, NJ, 2006)
16. Human Social Behavior Culture Modeling Program, HSCB Phase One and Two Summary, in *Human Social Culture Behavior Modeling Program Newsletter Winter 2010*, ed. by D. Schmorrow, vol. 3rd edn. (Strategic Analysis, Inc./Deputy Undersecretary of Defense for Science and Technology, Arlington, VA, 2010)
17. Human Social Behavior Culture Modeling Program, DoD-Wide Programs, in *Human Social Behavior Culture Modeling Program Newsletter, Spring 2010*, ed. by D. Schmorrow (Strategic Analysis, Inc./Deputy Undersecretary of Defense for Science and Technology, Arlington, VA, 2010), p. 8
18. H. Liu, J.J. Salerno, M. Young, *Social Computing, Behavioral Modeling and Prediction* (Springer, New York, 2008)
19. S.K. Chai, J.J. Salerno, P. Mabry, *Lecture Notes in Computer Science: Advances in Social Computing*, vol. 2010: 6007th edn. (Springer, New York, 2010)
20. R. Goolsby, Ethics and defense agency funding: some considerations. Soc. Netw. **27**, 95–106 (2005)
21. R. Goolsby, Combating terrorist networks: an evolutionary approach. Comput. Math. Org. Theory **12**, 7–20 (2006)
22. J. Scholtz, E. Morse, T. Hewett, *"In Depth Observational Studies of Professional Intelligence Analysts 2005," presented at the International Conference on Intelligence Analysis* (MacLean, VA, 2006)
23. J. Scholtz, E. Morse, M.P. Steves, Evaluation metrics and methodologies for user-centered evaluation of intelligent systems. Interact. Comput. **18**, 1186–1214 (2006)
24. J. Nielsen, Guerrilla HCI: Using Discount Usability Engineering to Penetrate the Intimidation Barrier, in *Cost-Justifying Usability*, ed. by R.G. Bias, D.J. Mayhew (Academic, Boston, MA, 1994), pp. 245–272. available at http://www.useit.com/jakob/publications.html
25. J. Nielsen, Usability Engineering, in *The Computer Science and Engineering Handbook*, ed. by A.B. Tucker (Chapman and Hall/CRC Press, Boca Raton, FL, 2004), pp. 1139–1160
26. C.W. Turner, J.R. Lewis, J. Nielsen, Determining usability test sample size. Int. Encycl. Ergon. Hum. Factors **3**, 3084–3088 (2006)
27. B. Nardi, Activity Theory and Human-Computer Interaction, in *Context and Consciousness: Activity Theory and Human-Computer Interaction*, ed. by B. Nardi (MIT Press, Cambridge, MA, 1996)
28. E. Rogers, *Diffusion of Innovations*, 5th edn. (Free Press, New York, 2003)
29. K. Vredenburg, J.Y. Mao, P.W. Smith, T. Carey, *"A Survey of User-Centered Design Practice," presented at the CHI '02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Changing our World* (Changing Ourselves, Minneapolis, MN, 2002)
30. J. Scholtz, A User-Centered Approach to Social Modeling and Simulation for Decision Making, in *Challenges in Computational Social Modeling and Simulation for National Security Decision Making*, ed. by L. McNamara, T. Trucano, C. Gieseler (Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Ft. Belvoir, VA, 2011), pp. 227–240
31. K. Knorr-Cetina, *Epstemic Cultures: How the Sciences Make Knowledge* (Harvard University Press, Cambridge, MA, 1999)
32. N. Gilbert, Modellers claim wars are predictable. Nature **462**, 836 (2009)
33. L. Resnyansky, Social modeling as an interdisciplinary research practice. IEEE Intell. Syst. **23**, 20–27 (2008). July/August 2008
34. J.G. Turnley, Assessing the Goodness of Computational Social Models, in *Challenges in Computational Social Modeling and Simulation for National Security Decision Making*, ed. by L. McNamara, T. Trucano, C. Gieseler (Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Ft. Belvoir, VA, 2011), pp. 241–254
35. M. Al-Fayoumi, S. Banerjee, P.K. Mananti, Analysis of social network using clever ant colony metaphor. World Acad. Sci. Eng. Technol. **53**, 970–974 (2009)
36. S. Li, L. Gao, G. Xu, *"The Best Bidding Price Based on Ant Colony Algorithms in Electric Power Markets," presented at the Sustainable Power Generation and Supply* (Nanjing, China, 2009)
37. B. Nardi, Studying Context: A Comparison of Activity Theory, Situated Action Models, and Distributed Cognition, in *Context and Consciousness: Activity Theory and Human-Computer Interaction*, ed. by B.A. Nardi (MIT Press, Cambridge, MA, 1995), pp. 70–102
38. Y. Engeström, *Developmental Studies of Work as a Testbench of Activity Theory: The Case of Primary Care Medical Practice* (Cambridge University Press, New York, 1996)
39. Y. Engeström, Activity Theory and Individual and Social Transformation, in *Perspectives on Activity Theory*, ed. by Y. Engeström, R. Miettinen, R.L. Punamäki (Cambridge University Press, New York, 1999), pp. 19–38
40. S.K. Card, T.P. Moran, A. Newell, *The Psychology of Human-Computer Interaction* (Lawrence Erbaum Associates, Hillsdale, NJ, 1983)
41. B. Crandall, G. Klein, R.R. Hoffman, *Working Minds: A Practitioner's Guide to Cognitive Task Analysis* (MIT Press, Cambridge, MA, 2006)
42. R.R. Hoffman, L.G. Militello, *Perspectives on Cognitive Task Analysis: Historical Origins and Modern Community of Practice* (Psychology Press (Taylor and Francis), New York, 2009)
43. K. Kuutti, Activity Theory, Transformation of Work, and Information Systems Design, in *Perspectives on Activity Theory*, ed. by Y. Engeström, R. Miettinen, R.L. Punamäki (Cambridge University Press, New York, 1999), pp. 360–376
44. O. Barreteau, Our companion modelling approach. J. Artif. Soc. Soc. Simul. **6**, 1 (2003)

45. W. Dare, O. Barreteau, A role playing game in irrigated system negotiation: between playing and reality. J. Artif. Soc. Soc. Simul. **6** (2003). http://jasss.soc.surrey.ac.uk/6/3/6.html
46. P.E. Becker, *Congregations in Conflict: Cultural Models of Local Religious Life* (Cambridge, New York, 1999)

doi:10.1186/2190-8532-1-17
Cite this article as: McNamara: **Biologically-inspired analysis in the real world: computing, informatics, and ecologies of use.** *Security Informatics* 2012 **1**:17.