Security Informatics
a SpringerOpen Journal

REVIEW Open Access

Natural security: how biological systems use information to adapt in an unpredictable world

Raphael D Sagarin[1*] and Terence Taylor[2]

Abstract

In this article, we analyze biological evolutionary systems to develop a framework for applying lessons of natural adaptability to security concerns in society. Biological systems do not waste resources attempting to predict future states of an inherently unpredictable and risk filled environment. Rather, biological organisms utilize adaptability to respond efficiently to a wide range of potential challenges, not just those that are known or anticipated.
Adaptability is a powerful, but often misused concept. Typically, dimensionless claims about adaptability, such as, "insurgents are more adaptable than us" are made without clear benchmarks against which to measure adaptability. Our framework for adaptability, which was developed over the course of several multi-disciplinary working groups of life scientists and security practitioners focused on what we can learn about security from biological systems, can be applied broadly to societal approaches to improving security.
Here we outline the "rules of engagement" for natural adaptable systems, which state that evolutionary systems do not predict, plan, or perfect the development of biological organisms. Given these constraints, we then outline four nearly universal features of adaptable biological organisms:

1. They are organized semi-autonomously with little central control
2. They learn from success
3. They use information to mitigate uncertainty
4. They extend their natural adaptability by engaging in a diverse range of symbiotic partnerships

For each of these attributes we identify how they work in nature and how we have failed to apply them in our responses to security concerns. Finally, we describe a pathway by which adaptable strategies can be incorporated into security analysis, planning and implementation.

Keywords: Adaptability, Evolutionary applications, Biologically inspired security, Symbiosis

Review

The Editors of this Special Issue have acknowledged that much effort has been spent in developing informatics approaches to predicting security threats with little to show for it. One of the charges of this Issue, then, was to show how biologically inspired approaches might improve predictability. As a biologist and biological warfare expert, however, we argue the opposite, that unpredictability should the starting point of any discussion about how biological systems can aid informatics approaches to security. This is because the fundamental commonality between human security problems and security problems faced by the rest of the biological world is that risks in the environment are ubiquitous and unpredictable.

Biological organisms have not responded to this unpredictability by wasting resources attempting to make predictions. Indeed, adaptable systems in nature haven't proven their record of success by demonstrating a high percentage of predictions that turned out to be correct, but rather by surviving and reproducing for 3.5 billion years and by diversifying into tens of millions of extant species living in the coldest, hottest, deepest, highest and most unpredictable niches on Earth. They have all done this by mastering the craft of adaptability. Natural adaptability is fundamentally different from merely reacting to a crisis (which is too late) or attempting to predict the

* Correspondence: rafe@email.arizona.edu
[1]Institute of the Environment and School of Natural Resources and the Environment, University of Arizona, Tucson, AZ 85721, USA
Full list of author information is available at the end of the article

next crisis (which is almost certain to fail, especially in species like humans when complex behaviors are involved). Adaptability controls the space between reaction and prediction, providing an inherent ability to respond efficiently to a wide range of potential challenges-not just those that are known or anticipated-as they arise in their environment.

Although, "adaptability" is now being thrown around as a popular buzzword among various security agencies and analysts, this potentially powerful concept is treated rather carelessly. Guidance on exactly what adaptability is and how it can be adopted in practice has been lacking. It is often presented as an ultimate, but ill-defined goal to attain. For example, after a perceived failure in security operations, it is argued that the agency in charge "needs to become more adaptable" with little guidance as to what more adaptable would look like. Likewise, dimensionless claims about adaptability, such as, "insurgents are more adaptable than us" are made without clear guidelines of how to measure adaptability.

Here we present a framework called "Natural Security", that places adaptability at the heart of understanding, and mounting effective responses to security threats, whatever form they take [1-3]. Natural Security can be viewed as a set of analytical and prescriptive tools that are based in the recognition that the function of adaptability has fundamental roots that go back as far in Earth's history as life itself. By deeply examining life history, including human evolution, we can discover proven solutions to surviving in a hostile and unpredictable world. These solutions have already been developed over 3.5 billion years of life history, but have largely gone unexamined in the analysis, planning and practice of security in modern human society. Insights from natural adaptive systems give us both clarity on our past survival as a species and guidance for dealing with unpredictable threats in the future. The concept of adaptability encompasses a broad diversity of security solutions in nature and accordingly provides a single unified framework for analyzing and guiding responses to the unpredictable threats. The Natural Security framework can be used regardless of the approach to security, but it will be particularly useful in an informatics context because—like the natural systems it was distilled from—it can improve its performance through a recursive process of transforming multitudes of observational data into ever more sharply defined responses to environmental change.

We developed this framework from a multi-year, multi-disciplinary working group we initiated in 2005 at the National Center for Ecological Analysis and Synthesis (NCEAS) that was fueled by a simple question: "what can we learn from biological organisms and evolution about how to be more adaptable to societal security concerns?" Participants in these discussions included life scientists from many fields including evolutionary biology, anthropology, psychology, network analysis and behavioral ecologists, along with security analysts, first responders, military and public health experts. Because we are not informatics experts, we make no attempt here to design algorithms or present quantitative models to bear out our biologically inspired framework for adaptability. Nonetheless, our outsider perspectives means that we come with no preconceived agenda or favored informatics approaches. Rather we offer our key findings from an in-depth study of natural systems as an adaptable framework from which multiple types of approaches, including more effective data mining, "crowd sourcing", and network analyses, can be built.

Here we present this framework in three parts. First we discuss the key rules of engagement that all biological systems operate under. Then we drill down into how adaptable systems work, pulling out four interrelated concepts focused on:

1. How adaptable systems are organized
2. How they learn
3. How they use information to mitigate uncertainty
4. How they extend their adaptable capacities through symbiotic relationships

Finally, we make recommendations as to how to apply these lessons and create adaptable security systems that closely mimic natural adaptive systems without forcing a complete reorganization of security infrastructure or violating common human ethical norms.

Adaptable systems: the rules of engagement

If there are rules (beyond elementary thermodynamics) under which biological evolution, and by extension the organisms that arise through evolutionary processes, works they amount to a prohibition against three "P's". That is, evolution doesn't predict, doesn't plan, and doesn't perfect biological organisms.

First, despite 150 years of modern evolutionary biology, biologists are almost never able to predict an evolutionary event beyond simple generalizations like "bacteria will evolve resistance to antibiotics". Evolved adaptable organisms themselves don't make predictions simply because the complex world of continually changing and interacting biological organisms acting within the dynamic and networked matrix of biogeochemical stocks and flows that they live in is not predictable. At best organisms anticipate events that come in well defined cycles—thus, many organisms have strong "circadian rhythms" that allow them to respond to light/dark cycles and many coastal marine organisms move in anticipation of tidal rhythms. They may also use their keen sensory abilities and stored sensory observations to

act in anticipation of unusual events as evidenced by wild and domestic animals responding to the 2004 Indian Ocean Boxing Day tsunami well in advance of humans living in the same area [4], but this is not predicting an unknown future event. Making and responding to predictions that are very unlikely to be correct is a waste of resources that are better spent finding food, avoiding predators and mating. The 2011 tsunami in Japan and its devastating effects on the nuclear power infrastructure, the Arab spring, and the outbreak of antibiotic resistant E. coli in Europe were all threats to security that were possible to anticipate (along with an almost infinite number of other security threats that did not come to pass during the previous year) but impossible to predict. It has been argued that all of the most destabilizing political, economic, and environmental events in human history have been unpredictable [5].

Second, there is no scientific evidence to support the notion that evolved biological systems are "intelligently designed" or planned in advance. There are numerous natural examples to illustrate this point, but one of the most striking is the ocean sunfish *Mola mola*. This large flattened fish slowly plies the surface waters of the Pacific sucking jellyfish through an undersized mouth, paddling with two flippers attached to a raggedly flat back end that looks as if the fish's proper tail was bitten off. If some intelligent designer decided to create a fish, it would never make a *Mola*. Yet, despite its scant resemblance to our common image of a fish, the *Mola* has survived as a fish for millennia because it adapted to its environment through time and ultimately found a niche that no other organism had capitalized upon. An unlikely creature such as the *Mola* emerged because the process of evolution doesn't tend toward any endpoint. It doesn't try to make an eye or an immune system or a beautiful fish. Evolution proceeds by solving survival problems as they arise. Security systems in society, by contrast, are littered with meticulously planned designs—the Maginot Line comes to mind—that were entirely unable to solve emerging threats from the environment.

Finally, a common misconception about evolution is that it is about seeking perfection, as encapsulated in the term "survival of the fittest". This interpretation is infused in misguided applications of Darwinian thought such as eugenics, and it is reflected in more legitimate societal applications such as business performance analysis where "optimization" is seen as a laudable goal. In fact, evolution is neither about survival of the "fittest" nor about optimizing systems. It just doesn't matter how close the organism is to its own theoretically optimal performance. It might work at 25% of its capacity and still survive just fine in a given environment. There is, in fact, no metric with which to measure how perfect or how optimal a given organism is. Would a coyote that produces five pups be more perfect if it could produce six? Not necessarily if it can't care for all six in that particular spring. Is a counter-terrorism strategy optimal if no terrorist attack occurred during its first five years of operation? Not if the same result could have been accrued using half the resources. Even the science of trying to predict optimality in organisms has proved itself to be almost comically wrong in case after case. For example, the first time depth sensors were attached to a live penguin, the animal dove to depths greatly exceeding its optimal performance as determined in painstaking applications of mathematical theory and laboratory physiological experiments [6].

The successful results of evolution are organisms that are not perfect, but "good enough" to survive and reproduce themselves. In society when we try to design perfect solutions to security problems we inevitably waste enormous amounts of resources while at best only marginally improving our security. For example, screening 100% of passengers at airports or people entering sensitive buildings is an attempt at creating a perfect security barrier that has failed to stop accidental smuggling of contraband, deliberate informal and formal test beaches, and actual terrorists such as Richard Reid and Umar Abdulmutallab. Likewise cyber security experts acknowledge that forty years of attempting to perfect "firewall" type security systems has only resulted in a cyber infrastructure that is more vulnerable than ever and becomes especially prone to damage once an attacker inevitably gets inside the security wall [7].

How adaptable systems work

The rules of engagement listed above would seem to deflate most of our enthusiastic responses to security problems. Almost all calls for improved security systems implore us to improve predictability. Making a security "plan" provides concrete evidence that we have done something to prepare us for a crisis. And the need to "optimize" rolls off the tongues of business gurus and security experts with scarcely a second thought to the impracticability of the concept. Yet biological systems, including humans themselves, have operated under de facto prohibitions against predicting, planning and perfecting all the while surviving, thriving and improving their performance for billions of years. Remarkably, despite the massive diversity of forms that have resulted from this vast evolutionary history, just a small number of simple themes adequately capture how adaptability is utilized in most organisms. Adopting these themes in our own practice will help put us on a pathway towards more adaptable social systems that can become self sustaining, rather than maintained through a centrally planned model.

Organizing to adapt

The organization of adaptable systems relies on a large number of semi-autonomous agents to sense and respond to environmental change with little central control [8,9]. Organisms have done this by evolving specialized organs, developing highly sensitive sensory mechanisms, specializing functions into differentiated clones, and organizing nerve cells into networked clusters operating closest to the environmental interaction. An octopus uses millions of cells spread across the surface of its skin to sense and respond to the world around, instantly changing shape and color to perfectly match each cells' immediate surroundings. Our own immune system, which can instantly identify and mount a response to an invading pathogen with no guidance from our central brain, is an exemplar of this type of organization.

Decentralized and distributed organizational systems are adaptable for three main reasons. First, multiple sensors all looking or experiencing the environment from their own perspective provide more opportunities to identify unusual changes and unexploited opportunities. When we let a single entity take complete charge of security, the number of observers goes down, along with the probability of identifying a threat to security. Second, multiple agents committed to the security mission in their own local area create opportunities to specialize tasks, so that energy isn't wasted in having every part of the organism doing the same things, but rather those doing the most important things (e.g., providing defense when hostile enemies are around or reproducing when populations are low) get the resources to replicate their activities. We have often ignored this lesson in distributing resources for homeland security. Recently, state Governors were appalled to find that to receive Federal funding from the Department of Homeland Security, they had to commit 25% of their budgets to defense against Improvised Explosive Devices [10]—a huge threat in foreign conflicts, but extremely low in importance relative to other threats facing domestic states. Third, distributed sensors respond to the most immediate environmental conditions in time and space—they see the environment for what it "is" rather than what it "should" be according to some preconceived notion. This way, the octopus that is transferred from its natural setting to a lab tank isn't paralyzed by the new environment. It simply uses its eight tentacles and thousands of suckers (which can smell) to feel out its new surroundings, search for food, or find an escape route.

Numerous recent societal examples illustrate that we are capable of creating such distributed organizational systems. Small bottom-up organizations around the world are rapidly becoming far more effective at promoting environment protection and social justice than the huge centralized and much better funded NGOs and governments. Businessman and social activist Paul Hawken likens this growing network of local organizations to an immune system, in that it is widely distributed yet connected, and grows larger not for its own sake, but through the process of local populations identifying additional needs and replicating their successful efforts [11]. Similarly, Ori Brafman and Rod Beckstrom have chronicled the struggles of traditional centralized business models in competing with new distributed networks of competitors. For example, highly decentralized music file sharing networks—typically run by college students on hundreds or thousands of independent machines that are constantly changing—have been successful at eluding the copyright protection efforts of the much better funded and highly centralized Recording Industry Association of America [12]. Most impressively, Google Flu Trends, an application that tracks users' "Googling" words associated with the flu, such as "flu symptoms", "flu remedies", and "flu vaccines", tightly matches the Center for Disease Control and Prevention's (CDC) official flu tracking, which is based on Doctor and hospital survey data that have to be returned to and compiled by the CDC, with one major difference. The decentralized Google Flu provided data on outbreaks two weeks faster than the centralized CDC data [13]. When it comes to the rapidly mutating flu virus, two weeks advance notice could easily be the difference between a mild nuisance and a global pandemic.

Learning from success

Having an adaptable organization allows adaptable systems to learn through a process of selection to respond effectively to threats. Learning is essentially a force of nature that acts across generations and within an organism's own lifetime. Even in relatively simple organisms, learning sets off a continual process of escalating threats and adaptive defenses. Birds learn that certain color patterns in spiders indicate the presence of poison and they avoid those patterns. Through time, other non-poisonous spiders develop the color patterns of the poisonous types and thus avoid being eaten themselves; a selectively induced learning passed down through generations. Humans' ability to learn is advanced relative to most other species and accelerated through a high degree of parental care, symbolic language, and communication networks that allow us to learn from environmental threats without actually experiencing them [14].

Natural learning is driven by Darwinian selection, a simple, yet powerful process that relies on just three elements—variation, selection, and reproduction of successful variants. Dominic Johnson, a member of our Natural Security working group, has shown that the

different selective forces acting on insurgents compared to US war fighters help to explain the relative lack of improvement in killing or capturing insurgents during the Iraq conflict [15]. In essence, insurgents come from a more variable population in terms of their origins and tactics and they are under stronger selection because they are killed or captured in much greater numbers than US forces, which results in the concentration and replication (through recruitment and training by the survivors) of stronger insurgents through time.

The selective learning process in nature acts on both failures and successes, but for an individual, learning from failure is literally a dead end--only success is rewarded by allowing a gene or a cell or an individual to grow and replicate itself. In nature, success is the creative process that recursively builds yet further successes. By contrast, we are unduly enamored, especially in the literature on organizational effectiveness, of the concept of "learning from failure" [16,17]. It is necessary for our security responses to learn from past failures, but we have placed far too little emphasis on learning from past successes. "After Action" reports are filled with perceived failures, but consistently underplay opportunities to identify and replicate the best performances. Our failure to learn from success is clear in disaster response, where the one unqualified success of the Hurricane Katrina response, the Coast Guard's containment and cleanup of nearly 9 million gallons of oil under logistically difficult circumstances, went almost completely unnoticed. The massive Townsend After Action report on Katrina does not mention oil spill cleanup, but it does identify 17 "Critical Challenges", 125 recommendations, and 243 action items, covering everything from Search and Rescue to transportation infrastructure to proper routing of foreign assistance [18]. None of these lessons from failure were all that useful for the next great Gulf disaster—the BP Deepwater Horizon oil well blowout—but lessons from the oil containment success likely would have been.

Using information to mitigate uncertainty

Not surprisingly, there are myriad ways adaptable systems learn to use information from the environment, but the wide array of natural information use coalesces around a single overarching theme: organisms seek to reduce uncertainty for themselves and increase uncertainty for their adversaries. The need to create uncertainty for an adversary and reduce uncertainty for oneself and one's allies explains many complex behaviors in nature. Birds flock to cause uncertainty for a predator about any individual's vulnerability, while predators use camouflage to create uncertainty about when and from where their attack will come. Periodical cicadas, which emerge *en masse* to mate and deposit eggs after periods of 7, 13, or 17 years lying dormant underground have evolved to exploit the mathematical uncertainty of prime numbers to avoid emerging during banner years for predators [19].

Another way organisms mitigate uncertainty through information is by broadcasting signals either from one individual member of a species to another or from one species to another species. While some of this signaling is deceptive (like an animal whose coloration mimics a poisonous animal) or secretive (cuttlefish send signals to one another in polarized light bursts), a counterintuitive outcome in natural information use is the ubiquity of "honest" signaling. Male peacocks make honest signals to females through the decoration of their feathers which gets more opulent and bright the more energy they are able to put into their display. A malnourished peacock, which would make a less fit mate, cannot put the energy into making a flashy signal. Deceptive signals, like the budget-strapped Argentine jail that staffed guard towers with mannequins, are quickly discovered as fraudulent under exposure (several prisoners promptly escaped) [20]. When signaling to enemy predators—a common practice that eliminates uncertainty by letting the predator know the prey is aware of its presence--organisms must not only signal honestly (or be able to maintain a bluff), but must have a keen sense of how their signal will be received. Ground squirrels for example, will make shrill alarm calls aimed at deterring bird and mammal predators (who can hear) but when faced with a snake (which doesn't hear), they don't call, but rather puff up and shake their tails. If that snake happens to be a rattlesnake rather than a gopher snake, the squirrel also heats up its tail because rattlesnakes are unique in that they perceive infrared radiation [21].

By contrast, most of the security screening we conduct tragically reverses the uncertainty rule of nature—that is, it makes life less uncertain for our adversaries and more uncertain for ourselves. When we widely advertise what we are looking for and how we are looking for it in security screening (which we must do when we order everyone passing through security to be screened in an identical fashion), our adversaries greatly reduce their uncertainty. They now know exactly what is being looked for and they can then work on adapting ways to get around the screening.

At the same time we increase our own uncertainty by constantly crying "predator!" (or, as the case may be, "terrorist!") which continually erodes our confidence that anyone really knows what is going on. Over the decade that TSA used its color coded Homeland Security Threat Level Advisory System--the five color warning scheme prominently displayed in airports and other public facilities—it rarely changed the warning level. In airports, the threat level stayed constantly at "Orange"

from August 2006 until the program's demise five years later. This was not a convincing message to our enemies that we actually did know what they were up to, and it also didn't give clear information to the population it was supposed to protect.

Extending adaptation through symbiosis

When faced with the limits of their own abilities, adaptable systems use *symbiosis* to extend their adaptive capacity. Symbiotic relationships are diverse and ubiquitous in nature, including relationships between species – such as predatory fish and much smaller fish – that would appear to have no reason to cooperate. Indeed, many symbiotic relationships arise out of previously antagonistic relationships. Symbiotic relationships can confer multiple benefits to the larger environment. Studies on monkeys and apes show that when individuals are coerced to begin a cooperative relationship (to help one another get food, for example), conflict overall between the animals is reduced [22]. Small coral reef fish known as wrasses set up "cleaning stations" where large fish can have their parasites cleaned off, provided they don't eat the smaller fish. The large fish in this symbiosis are not only less aggressive to their cleaning partners, but towards all other fish on the reef as well [23]. Biological research is increasingly concluding that humans are naturally cooperative, but mutually beneficial symbiotic relationships are vastly underutilized as a security strategy.

Symbiotic partnerships between US forces and even previously hostile Iraqi groups marked a turning point in the IED threat there. A precipitous decline in IED attacks in summer 2007 directly followed an increase in tips about bombs and bomb makers to US forces [1]. The power of symbiotic partnerships is more fully realized in the disease surveillance networks being facilitated by coauthor Taylor. These symbiotic partnerships--between Israelis, Palestinians and Jordanians [24], as well as practitioners from six traditionally hostile countries on the Mekong River—were created to identify and mitigate disease outbreaks on whatever side of borders they occur. Network practitioners share data, technologies, and techniques. These networks weren't mandated by high levels of government or through international treaties, but have emerged from the ground up as local, adaptive responses to a real need to protect regional food supplies and human health from pathogens that know no borders. The networks were also not designed to tackle the much larger and complex issues of creating peace between their member states, but by providing indispensible capacities to member states that are only available through symbiosis, they very well may be an incentive to further peace agreements. Finally, their success, like a properly functioning evolutionary feedback cycle, has encouraged further success. Large corporations such as IBM have been impressed by these networks and have contributed with vital database technology. Better still, new consortia are being replicated, for example in southern Africa, based on the successful performance of the original Middle East Consortium for Infectious Disease Surveillance.

Creating an adaptable cascade

A paradox of adaptation when applied to human social systems is that individual humans and small groups of humans appear to be more adaptable to security challenges than the organizations they design to deal with security. For example, troops on the ground in Iraq, operating as multiple semi-independent sensors, quickly identified IEDs as the greatest threat to their security and they adopted tactics and armor as best as they were able with the resources they had. By contrast, it took the Department of Defense, with vast resources, several years to bring mine resistant vehicles (MRAP) to Iraq, by which time over 1500 US soldiers and Marines had died due to IEDs [1]. Arguably, those same MRAP vehicles are poorly adapted for conditions in Afghanistan, where they force warfighters into predictable routes and can be easily outmaneuvered by enemies in lighter and considerably cheaper second hand Toyota pickups. In other words, we "intelligently design" security systems that are less adaptable to security threats than the humans for which they are intended.

This disconnect can be paralyzing. We tend to assume that because most security systems pass through large centralized bureaucracies that they can never be made to be adaptable. But that view makes the mistake of looking for a complete or perfect solution. The massive diversification of life and its continual change is the result of small, imperfect mutations and changes at the scale of molecules that improved on ancestral solutions to problems. Nor does this change need to take millions of years or generations. We now know that evolution can occur quite rapidly, and as human designers of security systems, we can speed up the process further by creating our own evolutionary processes and providing our own sources of selection.

The key is creating an adaptable cascade, in which some small adaptable actions set off other adaptable actions that ultimately lead to a system that generates its own momentum toward ever more adaptability. The first step for creating an adaptable cascade is to transform whatever sounds like an order into a challenge and to create whole new challenges. An order is anything created by a small elite group (or powerful individual) that is forced upon anyone else in the group under the expectation that it will be followed to the letter. A challenge, by contrast is an open solicitation for help to solve an identified problem. Issuing a challenge is not about relinquishing control or completely overturning

an existing hierarchy. The person or group issuing the challenge still has the power to design it, shape the incentives that will attract people to it, set the rules, and determine who will get to participate in the challenge. In other words, switching to a mode of issuing challenges doesn't have to radically alter the structure or power dynamics of a given organization. At the same time it can radically alter how problems are solved. Challenges work because they emulate the natural adaptive organization of nature where multiple semi-independent agents are solving problems where they occur. In more human terms they give ownership of a problem to the people who have to work on solving it.

The Defense Advanced Research Projects Agency (DARPA) has effectively used low cost challenges given openly to citizens to solve technological problems, such as designing a completely autonomous land vehicle, and informational problems, such as minimizing the time to find lost assets in a large geographic area. With both these types of challenges DARPA has reaped multiple effective solutions at a miniscule cost and in a rapid time frame that has in some cases even surprised the DARPA challenge organizers.

As individuals work on a challenge and share their results, learning outcomes will improve as an adaptive cascade takes its course. Like learning in nature, learning will happen automatically as an organization becomes more adaptable. Too many business books and corporate seminars and consultants try to institutionalize learning, but if an organization is not learning, it is not because it hasn't discovered some playbook on how to learn. Any plan for learning will become redundant as an organization becomes adaptable. Sagarin, for example, has found that experimental undergraduate teaching methods in which students are challenged to create the course syllabus, rather than be ordered to follow the "intelligently designed" syllabus of the professor, result in much greater participation and better learning outcomes (Sagarin and Turnipseed, unpublished data).

If an adaptable problem solving system is in place, the incentives necessary to bring out and replicate success are in material terms fairly minor, but they must be aligned correctly. Employees who respond to 3M's "Pollution Prevention Pays" challenge, which has reduced over a billion tons of pollution since its inception in the late 1970s and has saved the company over $3 billion, get little more than a statement of recognition from corporate headquarters. Yet, to date over 8,100 employee directed pollution reduction projects have been recognized by 3M [25]. In order to continually keep incentives aligned, documenting the level of response to different challenges (is interest growing or waning, for example) is as important as documenting the content of the responses themselves.

Among organizations that are used to planning, a concern about issuing open challenges is that there is a lot of uncertainty about what will come back in response. In an ecological context, this can be seen as an asset. The uncertainty that multiple problem solvers bring with them is its own form of naturally emerging diversity, which provides rich ground for adaptation. Moreover, by monitoring the adaptive cascade closely, a challenge organizer can mitigate uncertainty by changing the parameters of the challenge as needed. For example, DARPA could use results of their open challenges to seed a second generation of challenges that are more narrowly issued to participants with security clearances.

Invariably, new symbiotic partnerships will be borne out of the adaptive cascade. Although symbiotic partnerships are essential to adaptation, creating these partnerships cannot be done as a mandate from the top down. The government has mandated many "interagency task forces" designed to create partnerships between agencies that rarely talked to one another. But with a narrow set of allowable tasks and a required number of annual meetings, these task forces tend to become exercises in which representatives from each member agency, who have little power to make decisions, come to check off a box. Real symbiosis arises automatically when different entities find out that they can solve imminent problems better together than they could on their own. Symbiotic relationships may flash away as quickly as they were formed, or they may become long term partnerships, if both parties find at least some additional benefit from staying together. In this sense the central challenge of the adaptive cascade becomes the catalyst that new symbiotic partnerships are built around. The more perspectives that are brought in to address the challenge, the more opportunities to develop new symbiotic relationships emerge.

Finally, adaptive pathways are not valuable if created solely within a theoretical or experimental environment. All the ethical, political, economic and social factors that apply to any policy discussion should be brought to bear when applying biologically inspired ideas to security in societal systems. These factors are not unlike the many constraints that biological organisms have no choice but to acknowledge and deal with in order to survive. Fortunately, humans have an unmatched ability as a species to look at the environment both from an immediate perspective and from a detached viewpoint. This allows us to deliberately choose the types of adaptable strategies we want to employ and to modify them as needed to fit the constraints of our own social environment.

Conclusions

Our biologically inspired approach to security, which is based on the collective observations of natural adaptive

systems by generations of naturalists and life scientists, provides a framework on top of which can be a lain a number of informatics approaches to solving security challenges. Although we do not advocate any one informatics-based approach, we can distill several general lessons for biologically inspired security informatics. The finding that biological systems use de-centralized organization to sense and respond to environmental change suggests that informatics approaches will be most effective when the data used to train or validate models are gathered by multiple quasi-independent sources. Models should also be weighted toward rewarding successes by including recursive feedback elements that replicate successful tests, because learning from success generates a creative process of problem solving in adaptive systems. Biological models suggest that how information is projected is as important as how it is received and indeed senders and receivers of information are locked in a mutually interdependent evolutionary trajectory. In this regard, informatics approaches must be cognizant that the nature of information itself is continually changing along with the environment in which that information resides. Finally, informatics approaches should not underestimate the power and potential scope of symbiotic relationships. Such relationships can, for example, completely change network topologies and can form bridges between previously isolated networks. We believe that a number of approaches—technological, informational, psychological and political—will be necessary to address security challenges in societal systems. By referring all these approaches to a common underlying force—the need to maintain adaptability in a dynamic and unpredictable world—we can develop a common language and metrics with which to measure their effectiveness.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
RDS wrote the manuscript based on ideas developed during the course of working groups co-facilitated with TT. TT assisted with writing and editing the manuscript. Both authors read and approved the final manuscript.

Authors' information
Raphael Sagarin is a marine ecologist and environmental policy analyst at the University of Arizona in Tucson, AZ. Sagarin applies basic observations of nature to issues of broad societal interest, including conservation biology, protecting public trust resources, and making responses to terrorism and other security threats more adaptable. He is currently documenting the transformation in science back towards primarily observational, rather than experimental, methodologies. He uses unusual historical data sets from writers, naturalists, artists, and gamblers to re-assemble historical patterns of ecosystem change and responses of natural systems to climate change, including reconstructing changes to the Gulf of California since the 1940 expedition of John Steinbeck and Ed "Doc" Ricketts. For his work in these areas he was recently awarded a Guggenheim Fellowship. Dr. Sagarin has served as a Geological Society of America Congressional Science Fellow in the office of U.S. Representative (now U.S. Secretary of Labor) Hilda Solis. He has taught ecology and environmental policy at Duke University, California, State University Monterey Bay, Stanford University and University of California, Los Angeles. His research has appeared in *Science*, *Nature*, *Conservation Biology*, *Ecological Monographs*, *Trends in Ecology and Evolution*, *Foreign Policy*, *Homeland Security Affairs* and other leading journals, magazines, and newspapers. He is the author of *Learning from the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease* (2012, Basic Books). Terence Taylor is the President of the International Council for the Life Sciences (ICLS), Washington DC. Prior to his current appointment, Terence Taylor was Vice-President, Global Health and Security at the Nuclear Threat Initiative (NTI), and earlier Assistant Director at the International Institute for Strategic Studies (IISS) in London and was President and Executive Director of IISS-US. He has substantial experience in international security policy matters as a UK government official (both military and diplomatic) and for the United Nations both in the field and at UN Headquarters. He was a Commissioner and one of the Chief Inspectors with the UN Special Commission on Iraq with particular responsibilities for biological issues. He was a Science Fellow at Stanford University's Center for International Security and Cooperation. He was an officer in the British Army with experience in many parts of the world including UN peacekeeping, counter-insurgency and counter-terrorism operations. He is co-editor, with Dr Raphael Sagarin of the volume *Natural Security: A Darwinian Approach to a Dangerous World* (2008, University of California Press).

Acknowledgments
RDS acknowledges the support of a John Simon Guggenheim Memorial Foundation Fellowship. We acknowledge the contributions of the members of RDS' "Darwinian Security" Working group, sponsored by the National Center for Ecological Analysis and Synthesis, a National Science Foundation funded entity. Additional insights and responses to these ideas were provided by participants in a June 2010 forum on "Operational Adaptation" sponsored by the US Office of Naval Research Global and the University of Edinburgh, as well as multiple discussions with the Center for Homeland Defense and Security's Master's in Homeland Security and Executive Leaders programs.

Author details
[1]Institute of the Environment and School of Natural Resources and the Environment, University of Arizona, Tucson, AZ 85721, USA. [2]International Council for the Life Sciences, 7925 Jones Branch Drive, Suite LL130, McLean, VA 22102-3365, USA.

Received: 6 December 2011 Accepted: 7 September 2012
Published: 12 September 2012

References
1. RD Sagarin, Natural security for a variable and risk-filled world. Homeland Security Affairs **6** (2010)
2. RD Sagarin, CS Alcorta, S Atran, DT Blumstein, GP Dietl, ME Hochberg, DDP Johnson, S Levin, EMP Madin, JS Madin et al., Decentralize, adapt and cooperate. Nature **465**, 292–293 (2010)
3. R Sagarin, *Learning from the Octopus: How Secrets from Nature Can Help Us Fight Terrorism, Natural Disasters, and Disease* (Basic Books, New York, 2012)
4. M Mott, Did Animals Sense Tsunami Was Coming? National Geographic News (2005). January 4
5. NN Taleb, *The Black Swan: The Impact of the Highly Improbable* (Random House, New York, 2007)
6. RJ Moll, JJ Millspaugh, J Beringer, J Sartwell, Z He, A new 'view' of ecology and conservation through animal-borne video systems. Trends in Ecology & Evolution **22**, 660–668 (2007)
7. WA Wulf, AK Jones, Reflections on cybersecurity. Science **326**, 943–944 (2009)
8. G Vermeij, *Nature: an Economic History* (Princeton University Press, Princeton, 2004)
9. G Vermeij, Security, Unpredictability and Evolution: Policy and the History of Life, in *Natural Security: A Darwinian Approach to a Dangerous World*, ed. by R Sagarin, T Taylor (University of California Press, Berkeley, 2008)
10. E Schmitt, D Johnston, *States chafing at U.S. focus on terrorism* (The New York Times, New York, 2008). May 26
11. P Hawken, *Blessed Unrest: How the Largest Movement in the World Came Into Being and Why No One Saw it Coming* (Viking, New York, 2007)

12. O Brafman, RA Beckstrom, *The Starfish and the Spider: the Unstoppable Power of Leaderless Organizations* (Penguin Group, New York, 2006)
13. J Ginsberg, MH Mohebbi, RS Patel, L Brammer, MS Smolinski, L Brilliant, Detecting influenza epidemics using search engine query data. Nature **457**, 1012–1014 (2009)
14. J Henrich, R McElreath, The evolution of cultural evolution. Evolutionary Anthropology **12**, 123–135 (2003)
15. DDP Johnson, Darwinian Selection in Asymmetric Warfare: The natural advantage of insurgents and terrorists. Journal of the Washington Academy of Sciences Fall, 89–112 (2009)
16. T Harford, *Adapt! Why Success Always Starts with Failure* (Farrar traus and Giroux, New York, 2011)
17. DA Garvin, Building a learning organization. Harv Bus Rev **71**, 78–91 (1993)
18. The White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (The White House, Washington, DC, 2006)
19. GF Webb, The prime number periodical cicada problem. Discrete and Continuous Dynamical Systems-Series B **1**, 387–399 (2001)
20. BBC News, *Two escape from an Argentine jail guarded by a dummy* (2010). July 20
21. AS Rundus, DH Owings, SS Joshi, E Chinn, N Giannini, Ground squirrels use an infrared signal to deter rattlesnake predation. Procedings of the National Academy of Science **104**, 14372–14376 (2007)
22. J Horgan, The end of war. New scientist, 38–41 (2009). July 4
23. KL Cheney, R Bshary, AS Grutter, Cleaner fish cause predators to reduce aggression toward bystanders at cleaning stations. Behav Ecol **19**, 1063–1067 (2008)
24. A Leventhal, A Ramlawi, A Belbiesi, RD Balicer, Regional collaboration in the middle east to deal with H5N1 avian flu. British Medical Journal **333**, 856–858 (2006)
25. 3M, Pollution prevention pays. (2011) [http://solutions.3m.com/wps/portal/3M/en_US/3M-Sustainability/Global/Environment/3P/]

doi:10.1186/2190-8532-1-14
Cite this article as: Sagarin and Taylor: **Natural security: how biological systems use information to adapt in an unpredictable world.** *Security Informatics* 2012 **1**:14.