2010-09-00

Natural Security for a Variable and Risk-Filled World

Sagarin, Raphael

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (September 2010), v.6 no.3

Natural Security for a Variable and Risk-Filled World

Raphael Sagarin

INTRODUCTION

Fish don't try to turn sharks into vegetarians. Living immersed in a world of constant risk forces the fish to develop multiple ways to live with risk, rather than trying to eliminate it. The fish can dash away from the shark in a burst of speed, live in places sharks can't reach, use deceptive coloration to hide from the shark, form schools with other fish to confuse the shark, it can even form an alliance with the shark, and all of these things may help the fish solve the problem of how to avoid getting eaten by the shark. But none of these adaptations will help the fish solve the general problem of predation, and they don't need to. The fish doesn't have to be a perfect predator-avoidance machine. Like every single one of the countless organisms it shares a planet with, the fish just has to be good enough to survive and reproduce itself.

The world in which we spend our daily lives is also full of risk. Acts of terrorism that seem to come out of nowhere. Wars that have carried on too long and show little progress toward resolution. Catastrophic failures of supposedly fail-safe oil rigs. Intensifying natural disasters fueled by global changes in climate. A distribution of food that leaves billions undernourished and millions of others facing an obesity epidemic. A cyber infrastructure that we've become increasingly dependent upon that also has become increasingly vulnerable to catastrophic attack. New diseases and new mutations of old diseases that threaten to become global pandemics. The major threats society faces today are ominous and complex interplays of human behavior and environmental change, global politics, and local acts of cruelty or carelessness, historical accidents, and long-simmering tensions. Some of these threats have plagued us as long as we have been human and yet we've made little progress against them, others are becoming more dangerous in synergy with rapid climatic and political changes, and still others are just now emerging.

Yet the responses we been offered or forced to accept by the experts we've entrusted to solve these problems often seem frustratingly ineffective, naïve, or just plain ridiculous. When increased body screening of airline passengers was implemented after 9/11, Richard Reid attempted to destroy an airliner with a bomb in his shoe. When shoes began to be screened in response to Reid's attack, al Qaeda plotted to use a liquid explosive attack. When liquids were banned, Umar Abdulmutallab used a powdered incendiary hidden in his underwear in an attempted attack. A wall constructed between parts of the U.S. and Mexico border at a cost of between $1 million and $10 million per mile, slows down illegal immigrants by an estimated twenty minutes, even in its most fortified areas.[1] And on a tiny island in the tiny town of Beaufort, North Carolina there is a tiny outpost of the National Ocean and Atmospheric Administration (NOAA) that studies fish populations and coastal ecology. There is little reason to suspect this outpost is on any terrorist's list of desirable targets. Yet when the NOAA coastal scientists wanted to renovate and add some space a few years back, they were forced by the Department of Homeland Security to install enormous Wal-Mart style parking lot lights on their facility as a required security measure. This was ironic, since the scientists working at the lab know full well that nighttime light pollution is a major threat to the ecology of the same coastal marine environments that they are paid by taxpayers to study.[2]

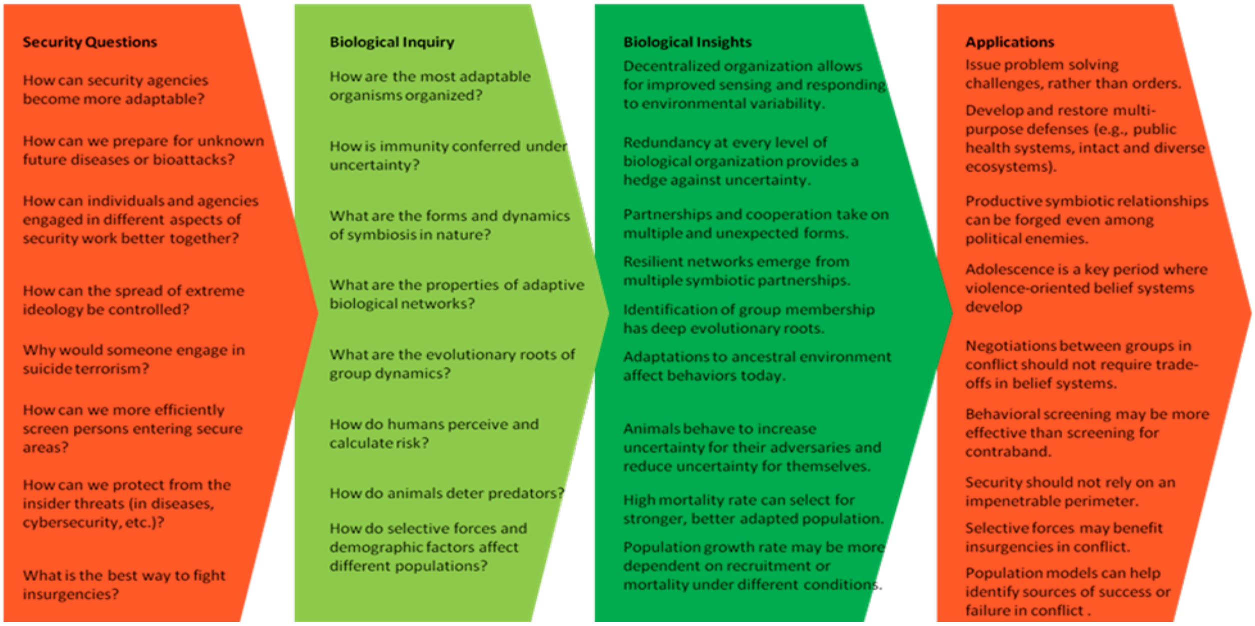
The most famous line of the 9/11 Commission report was that 9/11 represented a "failure of imagination,"[3] and this was certainly an apt description of the security situation up until 9/11. However, now that we imagine almost anything to be a threat to our security, a more pernicious problem faces all of our security systems: a failure of adaptation. Adaptation is the process of changing structures, behaviors, and interactions in response to changing conditions in the environment. *Adaptability* is the capacity to adapt to these changes – something that despite an unprecedented amount of attention, financial resources, and human lives sacrificed in the name of security since 9/11, has still largely eluded us.

Fortunately, we have at our disposal a vast storehouse of largely untapped knowledge that could guide us in developing adaptable security systems. It is a massive set of proven solutions (and teachable failures) to the very same problem that unites all of the threats we face – that is, how to survive and thrive in a risky, variable, and uncertain world. Remarkably, this database is completely unclassified and accessible to anyone. The solutions I'm referring to are all contained in the staggering diversity of life on earth – millions of individual living and extinct species, and countless individuals within those species – which have been developing, testing, rejecting, and replicating methods to overcome the challenges of living on a continually changing planet. These organisms have been experiencing security challenges and developing solutions since long before any presidential administration or Congress has developed their security agenda, since long before 9/11 finally woke most of us to the new post-cold war reality, since long before industrialization pushed our biogeochemical cycles into chaos, and long before humans ever walked the earth. Indeed, the 3.5 billion-year history of life imbues biological systems with more experience dealing with security problems than any other body of knowledge we possess.

And because we ourselves are biological creatures, our own species' evolution (and the modern manifestations of that evolutionary process) is not only an integral part of this natural database, but perhaps the most important set of data to consider. This means that in addition to the ecologists, paleontologists, virologists, and evolutionary biologists who have something novel to contribute to our security debate, so too do anthropologists, psychologists, soldiers, and first responders who have extensive behavioral observations of people and societies under the stress of insecurity in an uncertain environment.

I have been working with exactly these types of people for the last five years, primarily through my working group on "Darwinian Security" at the National Science Foundation-funded National Center for Ecological Analysis and Synthesis (NCEAS) in Santa Barbara, CA, and through interactive discussions with participants in several programs at the Center for Homeland Defense and Security (CHDS). The ideas developed in these lively discussions have been further honed in presentations to security think tanks and academic institutions, in corporate seminars and discussions with elected officials, and through response to our edited volume, *Natural Security: A Darwinian Approach to a Dangerous World* (University of California Press, 2008).

We have found that there is an increased openness among biologists to apply ecological and evolutionary ideas beyond biology, and receptiveness among societal institutions to incorporate biological knowledge into practice in, for example, using ecosystem analysis to study the global financial collapse. While there have been attempts to copy designs from nature to apply to security concerns (for example, designing submarine hulls based on the hydrodynamic shape of a tuna), and applications of biological models to studies of conflict, our approach considers key questions across the broad spectrum of security concerns and seeks insight from natural patterns and dynamics (Fig. 1). It is from this rich store of human knowledge that I present the general rules, specific examples, and pertinent applications of naturally-inspired security that can be implemented in the analysis, planning and practice of security in society.



Security Questions

How can security agencies become more adaptable?

How can we prepare for unknown future diseases or bioattacks?

How can individuals and agencies engaged in different aspects of security work better together?

How can the spread of extreme ideology be controlled?

Why would someone engage in suicide terrorism?

How can we more efficiently screen persons entering secure areas?

How can we protect from the insider threats (in diseases, cybersecurity, etc.)?

What is the best way to fight insurgencies?

Biological Inquiry

How are the most adaptable organisms organized?

How is immunity conferred under uncertainty?

What are the forms and dynamics of symbiosis in nature?

What are the properties of adaptive biological networks?

What are the evolutionary roots of group dynamics?

How do humans perceive and calculate risk?

How do animals deter predators?

How do selective forces and demographic factors affect different populations?

Biological Insights

Decentralized organization allows for improved sensing and responding to environmental variability.

Redundancy at every level of biological organization provides a hedge against uncertainty.

Partnerships and cooperation take on multiple and unexpected forms.

Resilient networks emerge from multiple symbiotic partnerships.

Identification of group membership has deep evolutionary roots.

Adaptations to ancestral environment affect behaviors today.

Animals behave to increase uncertainty for their adversaries and reduce uncertainty for themselves.

High mortality rate can select for stronger, better adapted population.

Population growth rate may be more dependent on recruitment or mortality under different conditions.

Applications

Issue problem solving challenges, rather than orders.

Develop and restore multi-purpose defenses (e.g., public health systems, intact and diverse ecosystems).

Productive symbiotic relationships can be forged even among political enemies.

Adolescence is a key period where violence-oriented belief systems develop

Negotiations between groups in conflict should not require trade-offs in belief systems.

Behavioral screening may be more effective than screening for contraband.

Security should not rely on an impenetrable perimeter.

Selective forces may benefit insurgencies in conflict.

Population models can help identify sources of success or failure in conflict .

Figure 1: Naturally Inspired Security. Applying natural security is a reiterative process that begins with security questions in society and uses natural history-based inquiry to find analogies and models, which can then be applied to society. Applications can then be further refined with more detailed societal questions and biological observations. Examples given are illustrative, not exhaustive.

BASIC PROPERTIES OF NATURAL SECURITY SYSTEMS

Since we have incredibly limited communication with all but one species of the millions of natural security experts, how can we tap their knowledge? In some cases, we will have just the raw data to observe and work with – the remarkably diverse ecosystems, organisms, cells, and molecules that inhabit the earth. Still more knowledge can be gleaned from ancient observations of nature made since the earliest human societies, from painstaking natural history and evolutionary biology conducted over the 150 years since Darwin's revolutionary *On the Origin of Species*, and from the most cutting-edge biological research on protein folding, genome mechanics, and network analysis that have massaged these raw data into stories and models and theories about how biological organisms survive and thrive on a dangerous planet. What emerges from this vast and growing field of study are a few simple themes that are essential in understanding how to translate natural security to societal security.

First, patterns in nature appear similar across different levels of biological organization. By levels of biological organization I mean the progression from molecules to DNA to cells to bodies of individual organisms to populations of those individuals to communities of those individuals interacting with individuals of other species to ecosystems which include the species, habitats, chemical and energetic interactions between them all in a given area. What is remarkable is that similar patterns – for example, using non-centralized organization to sense and respond to the environment – appear at each level of this organization. This *nested* quality of biological systems arises from their *recursive* character, meaning that the rules and patterns occurring at one level are not just similar to those at the next level, but essential in defining what happens at the next level. All of this is a good sign for applying biology to security in society because it suggests that biologically-guided solutions successfully implemented at one level (say, within a single office in FEMA) will be applicable at a completely different level (e.g., throughout the Department of Homeland Security). It also invalidates the excuse that we can't change security policy unless our highest levels of government change. I argue that we can start at any level of society in instituting more adaptable security systems and, if we align our incentives correctly, these ideas can easily (in fact will almost inevitably) spread up and down different levels of organization in society.

Second, complex natural patterns and processes arise from very simple building blocks. The four basic molecules of DNA code for a vast diversity of organisms that live in completely different ways and deal effectively with vastly different challenges. Moving up the levels of biological organization, natural selection, which has molded millions and millions of species into their forms today, is an incredibly simple process requiring just three simple building blocks: variation between individuals, environmental conditions that favor (or select) certain variants over others, and a means to reproduce those variants that are better suited to the environment. At yet a higher level, the simple process of individual organisms trying to survive and reproduce ends up producing networked ecosystems that are complex and resilient. Accordingly, natural security isn't about rising to the complexity of the security threats we face by designing a hugely complex system with flow charts and acronyms and multi-variate statistical outputs. It's about finding simple processes that impart our security systems with the adaptability to deal with a wide range of threats.

Third, biological evolution doesn't plan, design, or set goals of perfecting an organism. Evolution proceeds by solving survival problems as they arise, resulting in organisms that are not perfect, but "good enough" to survive and reproduce themselves. Likewise, in society we do not need to design perfect solutions to security problems – when we try to, they inevitably waste enormous amounts of resources while at best only marginally improve our security. We do need to define what is "good enough" and recognize that, as in natural systems, that definition will change continually through time.

Fourth, good ideas in evolution are often easy to spot because they appear nearly exactly the same across many different kinds of organisms. Although the DNA codes for millions of different organisms, the basic structure of the molecule and the process by which it replicates itself is the same across much of the living world. Heat shock proteins, which go around the body repairing damaged proteins, are both present and nearly identical in almost all organisms on earth. Thus, the biologically inspired ideas I propose here are not just stab-in-the-dark guesses that happened to work out well for a snail or a soybean plant somewhere, but time-tested billion-year-old solutions that have worked out in the coldest, highest, darkest, hottest, most predator-full and water-starved places on earth.

Fifth, good ideas in evolution are often the things that evolved independently multiple times. Eyes, for example, are a good solution for finding your way around in a complex world, but there isn't one common type of eye that evolved billions of years ago and that we all share. This security solution arose independently several times in different types of organisms. Octopuses have incredible eyes that serve the same kinds of functions as our eyes, but they are unique to octopuses. This phenomenon, called *convergent evolution*, is evidence that evolution is not about taking one design and plopping it down all over, but about solving problems particular to a given organism in a given environment. Here I propose ideas for security that mimic natural solutions, but they may also have been explored by other people or organizations who didn't make any reference to nature at all. I consider these coincident solutions to be examples of convergent evolution – different people trying to solve the problem of how to be ensure security in society and coming up with similar solutions.

Sixth, under the lens of natural history, humans are special, but not that special. There are a number of adaptations we have – such as advanced cognition and language – that both set us apart from most other species and create a lot of the complex security threats we face, but we are, in the end, just another species that evolved through time to deal with security challenges in our environment. With over a billion people facing chronic nutrition shortages,[4] and a host of old and emerging diseases that threaten to turn into human pandemics, we are undoubtedly still subject to the pressures of natural selection. Moreover, the way we have evolved has changed our environment enough to force us to adapt further. This cuts several ways for us – we are extremely adaptable, but we also may have changed our world and way of living faster than some parts of us can evolve. Some of our adaptations, which first arose in societies and on a planet completely unlike that in which we live today, can get us into trouble now.

Finally, and most important, change and variation rule everything in nature. As Darwin mused during his long journey on the *Beagle*, "where on the face of the earth can we find a spot, on which close investigation will not discover signs of that endless cycle of change, to which this earth has been, is, and will be subjected?"[5]

Darwin was referring to geology, the task he was primarily assigned during his fateful journey, but variation and change were very much at the heart of his subsequent biological studies. He felt it was essential to understand even the most minute variations – such as the microscopic differences between anatomies of the many species of barnacles that he cataloged in an enormous two-volume treatment[6] – to understand that "mystery of mysteries" of where life comes from. The simple lesson from this is that no effective security solution can be deployed and not modified or changed with time, because everything around it will be changing.

These basic tenets of evolution provide the outside parameters for developing an adaptable approach to security, but careful study of nature reveals general trends and patterns that can be used to provide specific guidance for applying nature's lessons to security in society.

SPECIFIC PROPERTIES OF NATURAL SECURITY SYSTEMS

Adaptable Organization

The most adaptable and successful organisms, though wildly diverse in appearance and behavior, are all organized in a similar manner. Universally, they avoid the trap of centralized, top-down control by giving wide ranging power to multiple independent sensors to observe and respond to environmental change and threats.[7] 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.

By contrast, many of our security responses trend towards increased centralization. The most prominent security response after 9/11 was to create the massive Department of Homeland Security (DHS), which quickly displayed its shortcomings during and after Hurricane Katrina, the response to which represented the worst post-9/11 security breach in the United States. A common question during and after Katrina was "Where was FEMA?" – referring to the Federal Emergency Management Agency, which was ostensibly in charge of disaster relief efforts. Because it is a bureaucracy, the best way to find FEMA is by looking at the "Org" chart of its parent organization, DHS, at the time of Katrina (Fig. 2). FEMA is literally buried in a huge stack of blocks, all representing their own enormous bureaucracies – such as the Coast Guard and the Transportation Security Administration (TSA) – all required to run decisions up the chain of command to the secretary of Homeland Security and, consequently, all vying for the secretary's attention.

An organization like this might work fine in carrying out a planned set of tasks that continue routinely day after day. It's like an early circuit board with a finite number of pathways through which the energy of decision-making can pass. But security problems are such precisely because they are not routine; they are highly variable and unpredictable. If one of the organizations inside one of those boxes needs to do something completely different than normal – as FEMA needed too after Katrina – it has little recourse to do so.

That's not to say that some organizations didn't demonstrate some amazing responses to Katrina. The United States Maritime Administration, a branch of the Department of Transportation that maintains and contracts a fleet of ships to make vessels available during wars and national emergencies, quickly set up shipboard spaces that the various security agencies used as command centers. And of course, many individuals within all of the agencies, as well as individual citizens, improvised all sorts of effective responses to the hurricane.

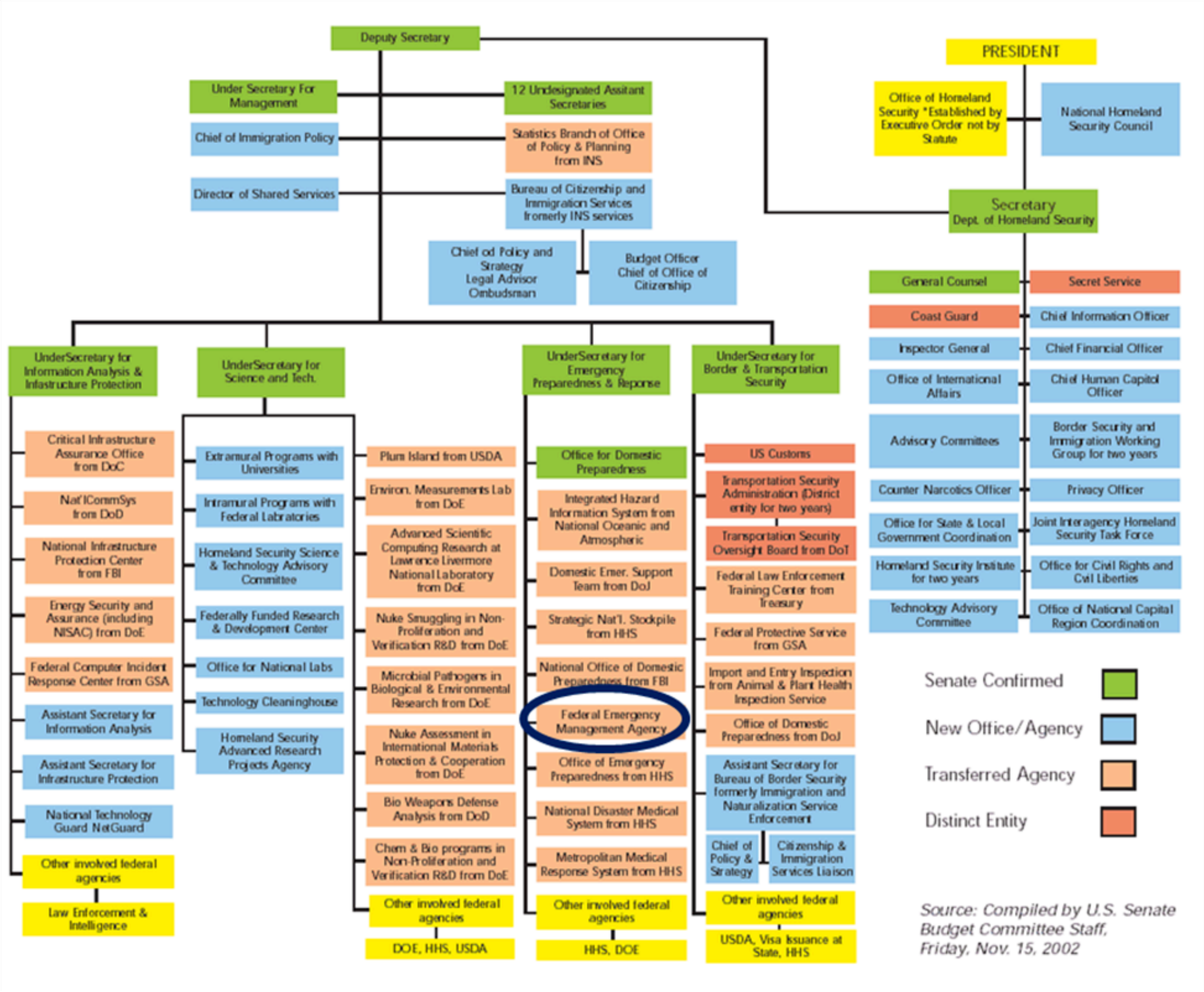

Deputy Secretary
PRESIDENT
Under Secretary For Management
12 Undesignated Assitant Secretaries
Office of Homeland Security *Established by Executive Order not by Statute
National Homeland Security Council
Chief of Immigration Policy
Statistics Branch of Office of Policy & Planning from INS
Director of Shared Services
Bureau of Citizenship and Immigration Services fromerly INS services
Secretary Dept. of Homeland Security
Chief od Policy and Strategy Legal Advisor Ombudsman
Budget Officer Chief of Office of Citizenship
General Counsel
Secret Service
Coast Guard
Chief Information Officer
Inspector General
Chief Financial Officer
Office of International Affairs
Chief Human Capitol Officer
UnderSecretary for Information Analysis & Infastructure Protection
UnderSecretary for Science and Tech.
UnderSecretary for Emergency Preparedness & Reponse
UnderSecretary for Border & Transportation Security
Advisory Committees
Border Security and Immigration Working Group for two years
Critical Infrastructure Assurance Office from DoC
Extramural Programs with Universities
Plum Island from USDA
Office for Domestic Preparedness
US Customs
Nat'lCommSys from DoD
Intramural Programs with Federal Labratories
Environ. Measurements Lab from DoE
Integrated Hazard Information System from National Oceanic and Atmospheric
Transportation Security Administration (District entity for two years)
Counter Narcotics Officer
Privacy Officer
National Infrastructure Protection Center from FBI
Homeland Security Science & Technology Advisory Committee
Advanced Scientific Computing Research at Lawrence Livermore National Laboratory from DoE
Transportation Security Oversight Board from DoT
Office for State & Local Government Coordination
Joint Interagency Homeland Security Task Force
Domestic Emer. Support Team from DoJ
Federal Law Enforcement Training Center from Treasury
Homeland Security Institute for two years
Office for Civil Rights and Civil Liberties
Energy Security and Assurance (including NISAC) from DoE
Federally Funded Research & Development Center
Nuke Smuggling in Non-Proliferation and Verification R&D from DoE
Strategic Nat'l. Stockpile from HHS
Federal Protective Service from GSA
Technology Advisory Committee
Office of National Capital Region Coordination
Federal Computer Incident Response Center from GSA
Office for National labs
Microbial Pathogens in Biological & Environmental Research from DoE
National Office of Domestic Preparedness from FBI
Import and Entry Inspection from Animal & Plant Health Inspection Service
Senate Confirmed 🟩
Technology Cleaninghouse
Federal Emergency Management Agency
Office of Domestic Preparedness from DoJ
New Office/Agency 🟦
Assistant Secretary for Information Analysis
Homeland Security Advanced Research Projects Agency
Nuke Assessment in International Materials Protection & Cooperation from DoE
Office of Emergency Preparedness from HHS
Assistant Secretary for Bureau of Border Security formerly Immigration and Naturalization Service Enforcement
Assistant Secretary for Infrastructure Protection
Transferred Agency 🟧
Bio Weapons Defense Analysis from DoD
National Technology Guard NetGuard
National Disaster Medical System from HHS
Distinct Entity 🟥
Chief of Policy & Strategy
Citizenship & Immigration Services Liaison
Other involved federal agencies
Chem & Bio programs in Non-Proliferation and Verification R&D from DoE
Metropolitan Medical Response System from HHS
Other involved federal agencies
Other involved federal agencies
Other involved federal agencies
Law Enforcement & Intelligence
DOE, HHS, USDA
HHS, DOE
USDA, Visa Issuance at State, HHS
Source: Compiled by U.S. Senate Budget Committee Staff, Friday, Nov. 15, 2002

Fig. 2. Organizational chart for the Department of Homeland Security. FEMA is circled in dark blue. Source: U.S. Senate Budget Committee Staff, Nov. 15, 2002.

It is often assumed that the stack of boxes leading to one central controller is the natural and inevitable way an organization develops. And people working within such an organization often assume that there is no way to change that system of organization without destroying the entire organization itself.

The first assumption is, in fact, completely false, as proven by most successful biological organizations on earth. And challenging the second assumption, which is beginning to happen in societal organizations throughout the world, is the key to turning non-adaptable *organizations,* like DHS, into adaptive *organisms* that truly do keep us safer. Indeed, independent of our biological perspective, a number of sources have recognized the adaptability of decentralized organization in the context of business,[8] social activism,[9] and international governance.[10]

Even large entities have learned to develop adaptable, distributed organization structures. Google, Inc. uses a decentralized system for encouraging development of many of its products, which are then tested by billions of independent internet users.[11] For example, Google Flu Trends analyzes search behavior by internet users, specifically focused on flu-related search terms such as, “flu symptoms” and “flu remedies” under the assumption that more people will search such terms when flu is becoming more prevalent. Google Flu Trends show remarkable similarity to official U.S. Centers for Disease Control and Prevention (CDC) flu trend reports (which are compiled and published by CDC from doctor and hospital surveys) with one major exception: Google Flu Trends are available one to two weeks prior to the release of centrally controlled CDC data.[12]

Adopting an adaptable organizational system does not require a complete reorganization of our security bureaucracies. Almost any organization can inculcate adaptable systems by shifting from giving commands to issuing challenges – essentially open contests to solve a clearly stated security problem. Most security practice today is designed by a small number of experts and implemented through a central authority issuing orders to civilians (e.g., surrender your bottled water to TSA officials in airports) or contractors (e.g. design an aircraft that does X for Y amount of money). By contrast, challenges essentially create adaptable security organizations by encouraging multiple independent agents to find the best solution to a problem, then rewarding the most successful agents, and in the best cases, repeating the challenge to replicate and improve on the best designs from the previous iteration.

Even complex challenges can be successful at low cost and in relatively short time frames. For example, in 2002 the U.S. Defense Advanced Research Projects Agency (DARPA) presented an open challenge to a diffuse population of civilian groups to create autonomous vehicles that could navigate an obstacle course. The first iteration of this “Grand Challenge” in 2004 was fraught with failure. But groups learned from one another, and independently modified the wide variety of first-generation designs, selecting out poor performers and replicating successful components, resulting in high success in the second year which encouraged DARPA to issue yet more complex challenges in subsequent years. The most recent DARPA challenge (to find ten weather balloons scattered around the United States) was solved within a few hours by activating thousands of independent observers on the internet. [13]

Harnessing Uncertainty

A decentralized organizational structure works because it allows organisms to deal with uncertainty. Uncertainty that is created by variation lies at the core of a wide range of security concerns. Organisms in nature actively exploit uncertainty and turn it to their advantage by creating uncertainty for their adversaries and reducing uncertainty for themselves. Predators create uncertainty by stalking from hidden vantage points, but when possible, prey reduce this uncertainty by vocally or behaviorally signaling the presence of predators – a strategy that both warns fellow prey about the threat and indicates to the predator that the element of uncertainty has been removed.[14] To be effective the signaling must be directly tied to immediate threats. For example, ground squirrels will make vocal signals to bird and mammal predators (which can hear) but switch to “tail flagging” displays to deter snakes (which cannot hear), and will additionally heat their tails only when encountered by particular snakes (pit vipers) that can sense infrared signals.[15] By contrast, when organisms in a community make constant alarm calls regardless of the immediacy of the threat they only increase uncertainty for other members of the group, who must waste resources determining if the alarm is true or false.[16] Analogously, the U.S. National Threat Advisory, which has remained at level "orange" for aviation since August 2006,[17] is not aimed at deterring a particular threat and does little to reduce uncertainty among innocent travelers. We can vastly increase the uncertainty for our adversaries by just doing a small amount of random things every day in our security procedures. Currently we waste enormous resources to screen 100 percent of the people passing through security with little benefit. Laying aside the fact that this doesn't even work to find the things we are looking for (knives, guns, explosive materials, and 6 oz. tubs of strawberry yogurt, all have which have been brought through security in recent years without detection),[18] it also gives us almost no extra protection from real attackers.

A low frequency of random screening (as opposed to a high level of screening equally applied to all) can deter someone who wants to evade detection.[19] This is particularly true in the case of a terrorist attack because there is a very high cost of failure in such a plot, as there is for any predator. A lioness hunting an antelope must have very little uncertainty that her attack will be successful because if she fails, she has not only wasted energy and gotten hungrier, but she has also left her pride hungrier as well. A terrorist who gets caught not only fails to achieve the goal, but also puts his entire organization at grave risk of being discovered or counter-attacked. Indeed, this aversion to uncertainty drove several delays of the 9/11 attacks and may have led senior al Qaeda leaders to abort the attacks on 9/11 had they known one of the secondary operatives had been arrested.[20]

What is attractive about randomizing security procedures is that it can actually drastically reduce the amount of time we waste in security lines (by screening much less than 100 percent of people for most things) while reducing the likelihood of an attack. These multiple benefits are not just serendipitous – natural security systems create positive feedback loops. For example, increasing uncertainty for a predator reduces the need for constant vigilance by the prey organism, which can then spend more resources on eating or mating or other needed security strategies. The Transportation Security Administration (TSA) has been experimenting with randomization and uncertainty in its 2010 Surface Transportation Security Priority Assessment, about which it testified that "random screening teams are among DHS' most effective deterrence and detection tools for countering terrorist threats,"[21] as well as through its Screening of Passengers through Observation Techniques (SPOT) behavioral detection program which deploys trained TSA agents to search for characteristic signs of stress and deception among passengers. Behavioral recognition has the advantage of returning control of uncertainty to the population it is trying to protect because it can be conducted from hidden vantage points or video. As a head behavioral screener at Dulles Airport (one of 161 airports where behavioral screening was initially deployed by TSA)[22] remarked, "The observation of human behavior is probably the hardest thing to defeat. You just don't know what I am going to see."[23] Nonetheless, the scientific basis for behavioral detection has not been well established,[24] and the efficacy of layering discrete behavioral screening with other levels of verbal and non-verbal intent detection systems is currently being investigated.[25]

Learning Through Evolution

A main reason that security walls and contraband screening don't work against attackers is that they quickly learn what the barrier is and how to get around it. This problem has been recognized by cyber security experts who have recently acknowledged that forty years of attempts to make "perfect" systems protected by firewalls have only led to an increasingly vulnerable cyber infrastructure.[26] One simple and effective cyber attack that has been successful in deliberate simulations and actual attacks involves physically scattering virus-infected USB drives in a parking lot and letting employees with security clearance inadvertently introduce the virus behind the firewall when they insert the drives into their workstations.[27]

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. Even the process of how animals learn is not immutable. That is, animals have some basic capacity for learning, but they can learn in accelerated ways depending on the environment they are put in. Monkeys, which are generally considered to have the learning capacity of a human two-year-old, can be trained in experimental settings to learn like a nine-year-old, including understanding a sense of their own self as a unique entity interacting with and affecting the world around them.[28] The capacity for learning reminds us that no security adaptation should be assumed to be a safe and everlasting solution, because there is always the potential for an adaptable enemy to learn how to overcome it.

A more formalized way to look at natural learning is through the framework of adaptation by natural selection. Examining the changing security environment in a Darwinian context that breaks down the three components of adaptive evolution – variation, selection, and replication – provides insight into how individuals and institutions learn from experiences with environmental threats. These factors may explain why the insurgents have been relatively successful against coalition forces in recent conflicts. Johnson argues that the nearly invariant ratio of insurgents killed or captured per U.S. soldier killed or captured throughout the Iraq war may be attributable to stronger selection pressure exerted by the more powerful side (the U.S.),[29] which leads to faster adaptation among insurgent fighters, strategies, and technologies. This selection works on a more variable population of insurgents, who both come from more diverse origins than U.S. forces and utilize a wider range of tactics than U.S. forces, which are constrained by standard procedures, international conventions, and other norms.

Ground observations support this analysis as the average time for insurgent fighters to adapt to new tactics, techniques, or procedures of U.S. troops is reported by counterinsurgency officers to be about fourteen days; insurgents apparently have learned to identify the signs of troop rotation and step-up attacks immediately following the arrival of new troops.[30] This rapid adaptation is a well-appreciated problem. U.S. Secretary of Defense Robert Gates remarked at a congressional hearing in March 2007 that "as soon as we ...find one way of trying to thwart their efforts, [the insurgents] find a technology or a new way of going about their business"[31].

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.[32] In addition to creating a more threatening environment, learning can also greatly aid our security. For example, until 9/11 the normal response to a plane hijacking was to put up no resistance as hijackers made demands that were eventually negotiable and lethal threats were unlikely to be carried out. But on the same day that terrorists began using passenger planes as weapons of mass destruction, humans used networked technology to share information about the change in hijackers' tactics and passengers on one hijacked plane immediately adapted a more active defense, risking their own security to protect a larger (and largely unrelated) group of humans. Subsequent airborne attack attempts by Reid and Abdulmutallab were similarly stopped by passengers.

Using Symbiosis to Extend Adaptability

All organisms are constrained in their adaptability at some point, but they can utilize symbiotic relationships to extend their inherent adaptive capacity to exploit new resources and environments. 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. Where these relationships appear cooperative in humans or other organisms, there is still debate over whether they: are codified through positive feedback, must be enforced by punishment, are conducted with the expectation of reciprocity, or arise in response to genetic relationships between kin.[33] Regardless of the underlying mechanism, individual symbiotic relationships can confer multiple benefits to the larger environment. Studies on monkeys and apes show that when individuals are forced to begin a cooperative relationship (to help one another get food, for example), conflict overall between the animals is reduced.[34] 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.[35]

Cooperation among humans is far more complex than that among fish or monkeys, but the same surprising diversity of symbiotic relationship characterizes successful partnerships that diffuse security risks. New types of symbiotic partnerships between the most unlikely of collaborators are developing and ameliorating potential security crises around the globe. My colleague Terence Taylor, for example, has helped incubate symbiotic partnerships between Israelis, Palestinians and Jordanians,[36] as well as practitioners from five traditionally hostile countries on the Mekong River, all working together to identify and neutralize disease outbreaks on whatever side of borders they occur. Several features of these cooperative networks should be recognized. First, the networks have demonstrated success even beyond the feat of getting members of mutually hostile nations to work with one another. Network practitioners were quietly allowed into notoriously restricted Myanmar to do their work days, not weeks, after the catastrophic cyclone there. Second, 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. Third, the networks were not designed to tackle the much larger and complex issues of creating peace between their member states, though they very well may be an opening to further peace agreements. Finally, the networks greatly expand the capacity of any individual member state, giving them a built-in impetus to continue; without the network, each individual state would not only be powerless over outbreaks in neighboring states, but would also be much less capable of tackling diseases within its own borders.

HUMAN FACTORS

Complex human behaviors also appear at the origins of many security problems. Taking a natural history approach to human behaviors, which involves looking at both their evolutionary roots and their commonalities across human groups, can provide valuable insight into their present manifestations. Seemingly irrational behaviors, such as radical fundamentalist belief systems, make more sense when viewed in the context of an evolutionary bias toward forming strong group identity in opposition to outsiders,[37] a bias that has evolutionary origins long predating humans.[38] Villarreal argues that human belief systems are simply the evolved manifestation of self recognition systems that have helped nearly all organisms maintain their autonomy since the earliest interactions between bacteria and viruses. Belief systems can spread through relationship networks. These human networks also share key characteristics with biological networks such as ecosystems, food webs, and social insect relationships.[39] In particular, they show resilience which emanates from many individual components engaged in improving their own fitness. Many successful terrorist networks were found to originate through adolescent friendships developed in radical mosque-sponsored soccer leagues.[40] Although human belief systems have diversified, they show common features across societies – for instance, adolescence as a nearly universal period when ideological, religious, and other beliefs are either abandoned or solidified.[41] These three aspects of belief systems – their deep evolutionary roots, their network-reinforced resilience, and their universal features – suggest that they can't be eliminated entirely, but that alternative pathways provided for adolescents (e.g., soccer clubs sponsored by secular or non-radical religious groups) may be effective in diffusing their most dangerous expressions.

Nonetheless, applying Darwinian ideas to human society inevitably raises ethical issues. Biological evolution is often a tinkering process of trial and error and many individuals die under natural selection. Most societies don't ethically accept the notion of sacrificing individuals to improve security, although engaging in armed conflict implicitly carries some aspects of this (and accordingly raises ethical deliberations). But biologically inspired security systems will not be perfect mimics of nature and they do not have to be beholden to the same forces of selection that operate on natural organisms. We can deliberately select the aspects of natural security systems we would like to incorporate, devise artificial tests of their efficacy, and selectively reproduce only those systems that demonstrate improvements. Already, realistic amateur and professional probing has been used to test the efficacy of security systems, but the results have not necessarily been used to select for better systems. For example, the fallibility of systems that attempt to screen contraband carried by people entering secure buildings and airport gates was revealed in tests well before Abdulmutallab smuggled incendiary material onto a plane,[42] but the response to both the simulated and actual failure of contraband screening systems has been, in part, to appropriate *more* resources to them.

This equation of human societies rewarding security failures stands in stark contrast to how the rest of the living world deals with failure. In the natural world, failed experiments are eliminated through the process of natural selection, while successful adaptations are rewarded and replicated through survival and relatively higher reproduction. We focus far less on success than on failures in society. For example, the U.S. Coast Guard was roundly criticized for its performance after the relatively small 40,000-gallon Cosco Busan oil spill in San Francisco, but its admirable performance in containing and cleaning 9 million gallons of oil spilled after Hurricanes Katrina and Rita was almost completely ignored.[43] In fact, the massive Townsend after action report on Katrina identified seventeen "Critical Challenges," 125 recommendations, and 243 action items, covering everything from search and rescue to transportation infrastructure to human services, but none of them addressed oil spill cleanup, the one unqualified success after Katrina.[44] At the time, the oil spilled from Katrina was one of the largest oil spills on record, approximately two-thirds the size of the Exxon Valdez spill. Yet so forgotten were the oil spills caused by Katrina that by the time of the 2008 presidential campaign, Republican candidate Mike Huckabee was able to argue publicly that "not one drop of oil was spilled" due to Katrina.[45]

Both the engineering literature and the "organizational learning" literature place a strong emphasis on learning from failure. David Garvin, a leader in studies of organizational learning, argued that BP capitalizes on "constructive failure" which he defined as a failure that provides the critical learning components of "insight, understanding, and thus an addition to the commonly held wisdom of the organization."[46] The image of BP as an organization to emulate was shattered in April 2010, when BP's Deepwater Horizon rig exploded and led to an ecological and economic catastrophe. No doubt, the BP disaster will provide the company with all the components of "constructive failure" as Garvin defined them, but at a cost of greater than $1 billion to the company and with the uncertain economic and environmental impact on the Gulf of Mexico, it's hard to see this kind of learning from failure as something to aspire to.

In part, this discrepancy lies in the selective forces at work or not. In nature, selection is cleanly parsed out in life and death. In society, the selective agents are not so sharp. In both statute and practice, BP was allowed to operate without the necessary backup systems and safeguards;[47] there was no pressure to improve performance in this part of their operations. We would like to think that our congressional representatives could do a better job of rewarding better performance among security and safety agencies, but the complex politics of congressional appropriations (which are often more closely tied to seniority of representatives than the merits of the funded projects) have created an enormous disconnect between performance and reward that is not likely to be repaired soon.

It is often news media that plays the strongest selective agent. After the Cosco Busan spill, images of hundreds of frustrated San Francisco volunteers waiting to clean up oiled birds, but held back by Government bureaucrats, were rolled on national media.

These kinds of images result in calls to Congress and demands for investigations. By contrast, the Coast Guard's work on the post-Katrina and Rita oil spills hardly made newsworthy footage relative to images of people stranded on the roofs of their flooded houses. Because so much of the selective force on government agencies, especially when it comes in the form of media attention, focuses on mistakes (cost overruns, terrapin-like foot dragging, and botched responses), adapting based on success is not something that can be instilled from the top down. We cannot (and would not want to) order media outlets to only report good news.

Accordingly, the onus is on operatives at much smaller levels of government – battalion commanders, local police chiefs, and bureau heads – to identify successes, even if they were just one part of an operation that mostly failed, and to reproduce them. Sometimes this will mean promoting the people responsible for the success. Sometimes it will mean allocating more of a budget to activities that demonstrated success. But even where these local agents lack the power or resources to dole out these material rewards, they do have a very powerful and very inexpensive resource at their disposal. They can reproduce successes by teaching others in their field how to adopt their successful activities. This kind of teaching and learning is best facilitated through small informal networks of practitioners. For example, the armed forces have used intranets, such as NCOcorps.net, to give soldiers in Iraq and Afghanistan a forum to share information about successful practices as experienced by troops in the field.[48] This peer-to-peer training turns out to be an invaluable resource to new soldiers who come into combat with much less experience, and therefore much less adapted, than the insurgents that they will be fighting. Indeed, this method of replication brings us full circle back to the adaptability of decentralized organizations, as illustrated in the following case study of improvised explosive device (IED) attacks in Afghanistan and Iraq.

A CASE STUDY: IED Attacks in Iraq and Afghanistan

The case of IED deaths in Iraq and Afghanistan illustrates several points relevant to natural security. The issue of IED came to most civilian's attention in a dramatic fashion on December 8, 2004, during a televised visit between Secretary of Defense Donald Rumsfeld and National Guard soldiers preparing for deployment in Kuwait. To the cheers of the soldiers assembled, Specialist Thomas Wilson, a thirty-one-year-old Tennessee National Guardsman, pointedly asked the secretary why he and his fellow soldiers were being forced to rummage through garbage dumps to find armor to strap on to their vehicles, which provided inadequate protection in the combat zone. Rumsfeld was initially taken aback, then tartly retorted "you go to war with the Army you have."[49]

The terse exchange belied a critical difference in *adaptability* between soldiers like Specialist Wilson and a large security organization like the Department of Defense. For the troops on the ground, the process of adapting began soon after the invasion of Bagdad. They "went to war with the Army they had" (to paraphrase Rumsfeld), and it worked brilliantly for a while. With superior firepower, training, and air superiority, even the most feared of Saddam Hussein's forces virtually collapsed in front of the advancing coalition force. But as the old regime collapsed, the ground became rich for any number of new threats to sprout up. The threat environment radically changed. Suddenly, thousands of soldiers, independently as individuals and linked through the units they fought with, were observing that hidden improvised explosive devices (IED) were becoming their biggest threat to security. Whereas the DoD had planned for a war against AK-47s, Scud Missiles, and weapons of mass destruction, soldiers on the ground began to see their enemies as random trash piles, sudden fender benders in downtown traffic, and cell phones; hiding, distracting from, and detonating IED. By the time Wilson was so incensed as to dare breach military protocol to give a superior officer a dressing down, 266 of his colleagues had been killed due to IED.[50] (Fig. 3)

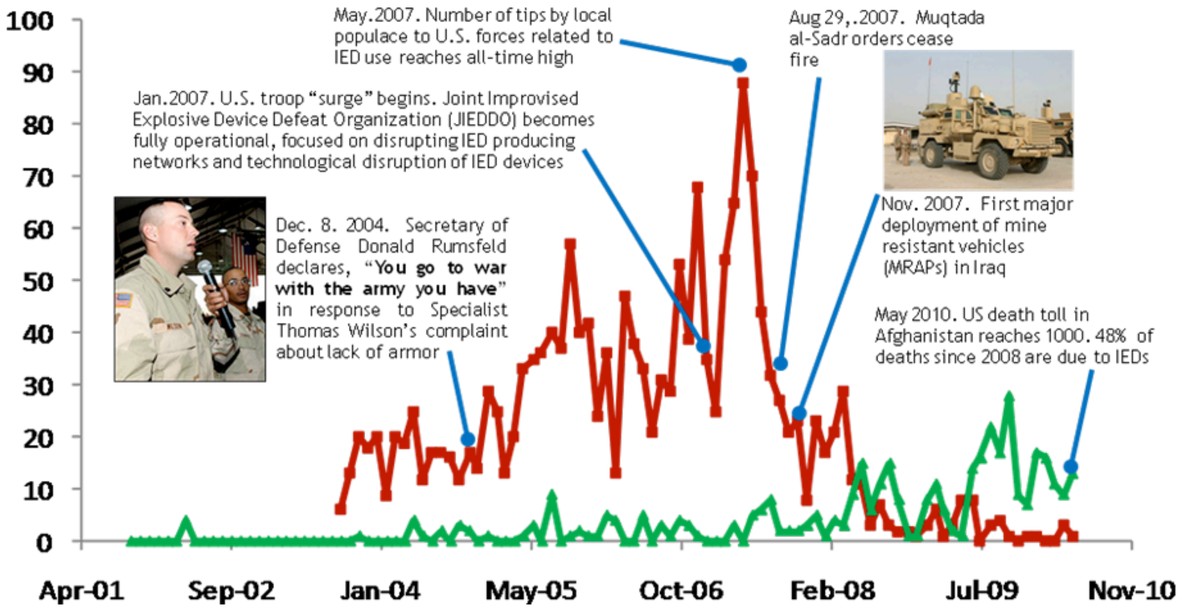


Figure 3. Deaths per month of U.S. troops in Iraq (red) and Afghanistan (green) and associated security related events. Data source: www.icasualties.org.

The soldiers adapted the best that they could, welding metal plates to their vehicles, blocking up culverts to eliminate the most obvious niches for bombers to use, and learning to identify the signs of hidden bombs in otherwise unremarkable debris. But their ability to adapt was limited by forces beyond their control – by the equipment they were given, by the available scrap metal, by the rules of engagement that they were ethically and legally bound by – and the casualties mounted.

By contrast, the Department of Defense had virtually unlimited resources, especially after 9/11 when no politically-minded congressperson or senator would ever turn down a military appropriation request. What the DoD lacked was adaptability. Even as Specialist Wilson and his comrades were frantically tracking the rapidly changing tactics of insurgents, the DoD was slowly churning away on weapons systems and fighting procedures that had been dreamed up long ago in places far away from the streets of Baghdad and Fallujah. Rumsfeld's retort to Wilson revealed a centralized view where small numbers of intellectuals design a battle plan and the accompanying technology years in advance, *and that's what you go to war with*. Moreover, even to bring the idealized technological solutions to deal with the threats theorized by DoD experts, the Department was bound by a ponderous top-down procurement system in which a small number of large contractors submitted bids for development of weapons systems that inevitably ran over budget and beyond the estimated timeline. Even after congressional outrage from the exchange between Wilson and Rumsfeld fueled calls to speed up production and deployment of mine-resistant ambush-protected vehicles (MRAP), they did not arrive in Iraq in until November 2007 – nearly three years later. By that time, an additional 1,589 of Wilson's colleagues had been killed in IED attacks.

The DoD solution certainly arrived too late to save their lives, but also too late to even deal with the original threat. A rapid downward trend in IED attacks and deaths was already well on its way by the time the MRAP arrived in Iraq. This downward trend can largely be linked to the successful fostering of two sets of symbiotic relationships in Iraq. First, General Petreaus authorized a shift in strategy towards engaging local populations to break up IED-producing networks, which resulted in increasing numbers of tips to soldiers about IED operations. Second, an inter-service partnership between ground soldiers and electronic warfare experts that devised methods to disarm wirelessly detonated IED greatly reduced the effectiveness of the remaining IED.[51]

The lesson here is that adaptation is primarily forged out of behaviors and relationships that can respond to a changing environment, not out of material solutions. Indeed, the MRAP that arrived too late in Iraq were ready just in time for a renewed offensive in the long-simmering war in Afghanistan. They have undoubtedly saved the lives of soldiers who were hit by IED, but they certainly haven't led to a decline in IED attacks or deaths, and may in fact have attracted more IED attacks. This is because the environment of Afghanistan is much more rugged than that of Iraq, making most of the country downright impassable to 14- to 24-ton vehicles like the MRAP.[52] Taliban operatives in inexpensive second-hand Toyota pickup trucks (probably the most adaptable vehicle ever built) could operate at will without interference from the lumbering U.S. forces. The few roads in Afghanistan that were MRAP accessible quickly became targets for IED attacks (which had been only a minimal threat up until this point) so that travel became a cumbersome affair, sometimes taking all day to move twelve kilometers or so.[53] In fact, after only two years of deployment, nearly half of the 16,000 MRAP produced (at a cost of $500,000 each) are being put on "inactive status".

What does this tale of differential adaptation tell us? First, adaptation requires leaving or being forced from your comfort zone and into a place where you observe and experience new threats to your security. Second, adaptation takes resources, but resources don't guarantee adaptation. Third, parts of an organization can be adaptable even if the organization is non-adaptable as a whole. Fourth, an adaptation developed for a given threat in a given environment may be useless, or even counterproductive, in a different environment.

LESSONS FOR AN ADAPTABLE FUTURE

It is important to recognize that the untapped secrets of natural security systems are not classified in any way. Rather, they are laid out in the structure of fossil and living organisms, in fragments of DNA, and in the observable behaviors of the organisms themselves. Translating ideas from nature into usable security solutions in society requires sensitivity to both how humans and human societies are different from other evolutionary systems, but also their common roots and analogous dynamics. Overall, the goal of a natural security system is to help society live with risks, rather than waste resources trying to eliminate them, by developing and maintaining adaptive security systems. An analysis of biological security systems suggests that a cascading set of interrelated strategies can provide the best means for dealing with the variation and uncertainty in nature.

In society, a cascade towards adaptive security can be initiated by giving more power to individual agents to sense and respond to threats. These agents could be individual people in a community, or individual offices, agencies, or states responsible for discrete aspects of a larger security mission. They do not operate completely independently, but rather are empowered through problem-solving challenges issued by an agency that has the resources or power to implement solutions. Multiple agents devising and testing a variety of security systems will provide greater likelihood of finding efficient solutions, redundancy to hedge against poor solutions, and potential for more rapid adaptation if selection pressures (such as budgets or media coverage) can be aligned to reward successful adaptations. Symbiotic partnerships between these agents can then extend their utility by bringing new skills and perspectives into emerging problem solving networks.

Given the vast diversity of life, we have only scratched the surface of potential lessons from nature for security in society. For example, biologists understand that organisms in nature inherently accept that risk is inevitable in the environment and, through selection, manage to balance the costs and benefits of developing new adaptations. But we have little ability to predict why certain types of adaptations will arise in a given place or time, which could then reflect on how society could optimally manage a portfolio of emerging and existing risks. Getting closer to this understanding may involve a deeper appreciation (using appropriate biological models such as the immune system and host-parasite interactions) of how particular adaptations take place in a range of situations – are they the product of escalation through repeated direct interactions, a response to chronic stress, or a generalized response to cope with a potential range of natural variation? Additionally, focusing on rapid adaptation and rapid feedback cycles – such as occur with retroviruses which manage to hijack the adaptive machinery of the immune system and use it against the host body – could be enormously important as a model for understanding how radical ideas are now rapidly spread peer-to-peer using simple messaging between previously unlinked terror groups. This same model could be adapted to aid with the likely need to adapt rapidly to climate change. Finally, my group has largely focused on evolutionary successes, but the history of life is replete with apparently well-adapted organisms that went extinct. What are the conditions under which even organisms that sense the environment well and reduce their own uncertainty go extinct and what can this tell us about our own failures? This reminds us of a sobering basic tenet of natural security: those who embrace the process of adaptation survive and thrive, those who don't, go extinct.

Raphael Sagarin is a marine biologist and research scientist at the Institute of the Environment at University of Arizona. Dr. Sagarin's work on using biological evolution as a guide for improving societal security systems began during his tenure as a Geological Society

of America Congressional Science Fellow in the office of U.S. Representative (now Labor Secretary) Hilda Solis. His research has appeared in Science, Nature, Conservation Biology, Foreign Policy *and other leading journals. He received his doctorate from the University of California, Santa Barbara in 2001. Dr. Sagarin may be contacted at* rafe@email.arizona.edu.

[1] "Migrants Finding Ways to Climb 18-foot-tall Border Fence," *Arizona Republic*, November 15, 2008, http://www.tucsoncitizen.com/ss/related/102700.

[2] See, for example, NOAA Technical Memorandum NMFS-SEFC-278 (NOAA Scientific Publications Office), http://spo.nwr.noaa.gov/.

[3] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: 2004). Several major news organizations and private blogs from different political persuasions used the "failure of imagination" line in their headlines or leads in coverage following the release of the report, including: National Public Radio, http://www.npr.org/911hearings/; *Perrspectives*, http://www.perrspectives.com/blog/archives/000010.htm; Radio Free Europe Radio Liberty, http://www.rferl.org/content/article/1053987.html; *The Christian Science Monitor*, http://www.csmonitor.com/2004/0723/p01s03-uspo.html; CNN.com, http://www.cnn.com/2004/ALLPOLITICS/07/22/911.report/index.html.

[4] Food and Agriculture Organization of the United Nations, *Hunger in the Face of Crisis* (New York: United Nations, 2009).

[5] Charles Darwin, *Voyage of the Beagle* by Charles Darwin, with a new introduction by David Quammen (Washington, DC: The National Geographic Society, 2004).

[6] Stott, Rebecca, *Darwin and the Barnacle* (New York: W.W. Norton & Company, 2003).

[7] Geerat Vermeij, *Nature: An Economic History* (Princeton, NJ: Princeton University Press, 2004).

[8] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Group, 2006).

[9] Paul Hawken, *Blessed Unrest: How the Largest Movement in the World Came into Being and Why No One Saw It Coming* (New York: Viking Press, 2007).

[10] Jean Francois Rischard, "Global Issues Networks: Desperate Times Deserve Innovative Measures," *The Washington Quarterly* 26, no. 1 (2002): 17-33.

[11] Bala Iyer and Thomas H. Davenport, "Reverse Engineering Google's Innovation Machine" *Harvard Business Review* (2008): 58-68.

[12] J. Ginsberg, M. H. Mohebbi, R. S. Patel, L. Brammer, M. S. Smolinski, and L. Brilliant, "Detecting Influenza Epidemics Using Search Engine Query Data," *Nature* 457, no. 7232 (2009): 1012-U4.

[13] These results can be found at https://networkchallenge.darpa.mil.

[14] D.T. Blumstein, "The Evolution, Function, and Meaning of Marmot Alarm Communication," *Advances in the Study of Behavior* 37 (2007): 371-400.

[15] Aaron S. Rundus, Donald H. Owings, Sanjay S. Joshi, Erin Chinn, and Nicholas Giannini, "Ground Squirrels Use an Infrared Signal to Deter Rattlesnake Predation," *Procedings of the National Academy of Science* 104, no. 36 (2007): 14372-76.

[16] D.T. Blumstein, L. Verneyre, and J.C. Daniel, "Reliability and the adaptive utility of discrimination among alarm callers," *Proceedings of the Royal Society of London Series B-Biological Sciences* 271 (2004): 1851-1857, doi:10.1098/rspb.2004.2808.

[17] Data available at http://www.dhs.gov/xabout/history/editorial_0844.shtm.

[18] John Nance, "Has Airport Security Improved Since 9/11 or Not?" *ABC News*, October 31, 2006, http://abcnews.go.com/Technology/story?id=2618488&page=1; Jeanne Meserve, "Airport screeners failed to find most fake bombs, TSA says," *CNN*, October 18, 2007, http://www.cnn.com/2007/TRAVEL/10/18/airport.screeners/index.html.

[19] S.E. Martonosi and A. Barnett, "How Effective Is Security Screening of Airline Passengers?" *Interfaces* 36, no. 6 (2006): 545-52.

[20] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: 2004), referring to the arrest of Zacarais Moussaoui.

[21] United States Department of Homeland Security, "Statement of David Heyman, Assistant Secretary for Policy," in *Senate Committee on Commerce, Science, and Transportation* (2010), http://commerce.senate.gov/public/.

[22] A full list of these airports is available at http://www.tsa.gov/press/where_we_stand/training.shtm.

[23] Doug Mills, "Faces, Too, Are Searched at U.S. Airports, " *New York Times*, August 17, 2006.

[24] United States Government Accountability Office, "Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges" (Washington, DC: GAO, 2010).

[25] J.K Burgoon, D. P. Twitchell, M. L. Jensen, T. O. Meservy, M. Adkins, J. Kruse, A. V. Deokar, G. Tsechpenakis, S. Lu, D. N. Metaxas, J. F. Nunamaker, and R. E. Younger, "Detecting Concealment of Intent in Transportation Screening: A Proof of Concept," *IEEE Transactions on Intelligent Transportation Systems* 10, no. 1 (2009): 103-12.

[26] William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity.," *Science* 326 (2009): 943-44.

[27] Industrial Control Systems Cyber Emergency Response Team, "USB Drives Commonly Used as an Attack Vector against Critical Infrastructure" (U.S. ICS-CERT, 2010), http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf.

[28] Laura Spinney, "Tools maketh the monkey," *New Scientist,* October 11, 2008, 42-45.

[29] Dominic D. P. Johnson, "Darwinian Selection in Asymmetric Warfare: The Natural Advantage of Insurgents and Terrorists" *Journal of the Washington Academy of Sciences* (Fall 2009): 89-112.

[30] Air National Guard Maj. N. Lipana, personal communication with the author.

[31] P. Eisler, "Insurgents Adapt Faster Than Military Adjusts to IEDs," *USA Today*, July 16, 2007.

[32] J. Henrich and R. McElreath, "The Evolution of Cultural Evolution," *Evolutionary Anthropology* 12, no. 3 (2003): 123-35.

[33] E.I. Svensson, "Understanding the Egalitarian Revolution in Human Social Evolution," *Trends in Ecology & Evolution* 24, no. 5 (2009): 233-35; K. Sigmund, "Punish or Perish? Retaliation and Collaboration among Humans," *Trends in Ecology & Evolution* 22, no. 11 (2007): 593-600.

[34] John Horgan, "The End of War," *NewScientist*, July 4, 2009, 38-41.

[35] K.L. Cheney, R. Bshary, and A. S. Grutter, "Cleaner Fish Cause Predators to Reduce Aggression toward Bystanders at Cleaning Stations," *Behavioral Ecology* 19, no. 5 (2008): 1063-67.

[36] A. Leventhal, A. Ramlawi, A. Belbiesi, and R.D. Balicer, "Regional collaboration in the Middle East to deal with H5N1 Avian Flu," *British Medical Journal* 333 (2006): 856-858.

[37] M.E. Hochberg, "A Theory of Modern Cultural Shifts and Meltdowns," *Proceedings of the Royal Society of London Series B-Biological Sciences* 271(2004): S313-S316, doi:10.1098/rsbl.2004.0172.

[38] Luis P. Villarreal, "From Biology to Belief," in Raphael Sagarin and Taylor Terence, eds., *Natural Security: A Darwinian Approach to a Dangerous World* (Berkeley, CA: University of California Press, 2008), 42-68.

[39] E.G. Leigh and G. J. Vermeij, "Does Natural Selection Organize Ecosystems for the Maintenance of High Productivity and Diversity?" *Philosophical Transactions of the Royal Society of London Series B-Biological Sciences* 357, no. 1421 (2002): 709-18; Simon A. Levin, "Ecosystems and the Biosphere as Complex Adaptive Systems," *Ecosystems* 1 (1998): 431-36.

[40] House Appropriations Subcommittee on Homeland Security. *The Making of a Terrorist: A Need for Understanding from the Field* (Washington, DC: March 12, 2008).

[41] Richard Sosis and Candace S. Alcorta, "Militants and Martyrs: Evolutionary Perspectives on Religion and Terrorism," in Raphael Sagarin and Taylor Terence, eds., *Natural Security: A Darwinian Approach to a Dangerous World* (Berkeley, CA: University of California Press, 2008), 105-24.

[42] "Airport insecurity," *The Seattle Times* , July 11, 2004); M.L. Goldstein, "Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities is Hampered by Weaknesses in its

Contract Security Guard Program" (Washington, DC: United States Government Accountability Office, 2009).

[43] Coast Guard Lt. Rhianna Strickland in personal comments to author, Febrary 2009.

[44] The White House, *The Federal Response to Hurricane Katrina Lessons Learned* (Washington, DC: 2006).

[45] "Fox News contributor Mike Huckabee falsely claimed 'not one drop of oil was spilled' during Hurricane Katrina," *MediaMatters,* July 27, 2008, http://mediamatters.org/research/200806270005.

[46] D.A. Garvin, "Building a Learning Organization," *Harvard Business Review* 71, no. 4 (1993): 78-91.

[47] M.Turnipseed, R. Sagarin, P. Barnes, M. C. Blumm, P. Parenteau, and P. H. Sand, "Reinvigorating the Public Trust Doctrine: Expert Opinion on the Potential of a Public Trust Mandate in U.S. and International Environmental Law," *Environment* 52, no. 5 (2010): 6-14.

[48] Information available at http://www.ncocorps.net/more/army_nco_site.htm.

[49] "Troops grill Rumsfeld over Iraq," *BBC News,* December 8, 2004, http://news.bbc.co.uk/2/hi/middle_east/4079201.stm; "Rumsfeld gets earful from troops," *Washington Post,* December 8, 2004, http://www.washingtonpost.com/wp-dyn/articles/A46508-2004Dec8.html; "Soldiers must rely on 'hillbilly armor' for protection," *ABCNews.com* (n.d.), http://abcnews.go.com/WNT/story?id=312959&page=2.

[50] IED casualty figures are drawn from www.icasualties.org.

[51] Major Noel Lipana, Air National Guard, personal comments to author, September 2009.

[52] Andrew Feickert, "Mine-Resistant, Ambush Protected (MRAP) Vehicles: Background and Issues for Congress," Congressional Research Service, ed. (Washington, DC: Library of Congress, 2008).

[53] Reporter Nir Rosen, personal comments to author, January 29, 2010