Finalist Essays from the Center for Homeland Defense and Security's Fifth Annual Essay Competition, 2012

Essay Question

Identify a theory or insight from a field outside homeland security that has not been applied to homeland security but should be.

Winning Essay

What Biological Systems Can *Still* Tell Us About Information Security
Dorian Deane

Finalists

(listed in alphabetical order by last name)

The Foraging Tango: The Application of Optimal Foraging Theory to Counterterrorism Activities
Don Arp Jr.

Improving Homeland Security Through Loops and Links
John M. Hartzell

Fighting Fear Appeal; Adopting Social Psychological Models to Inform Government Risk Communication
Sage Moon

About the Competition

The Center for Homeland Defense and Security (CHDS) essay contest, now in its fifth year, is aimed at stimulating original thought on issues in Homeland Security and Homeland Defense. CHDS launched the contest in 2008 to provide people from around the country the opportunity to express their opinions on homeland security issues and to suggest new ideas. The variety of the essay topics submitted, as well as the backgrounds of the authors, highlights the vast scope of the impact that homeland security policies, programs, and challenges have on our communities and professions. This year's contestants were asked to answer the following question: *Identify a theory or insight from a field outside homeland security that has not been applied to homeland security but should be.*

Congratulations to this year's winners. We hope reading their essays will accomplish the contest objective of stimulating thoughts and ideas and promoting discussion and debate on homeland security and defense issues.

More information about the competition, including the question and guidelines for the current competition and an archive of questions and finalist essays from previous competitions can be found at the following web address:
http://www.chds.us/?essay/overview

WHAT BIOLOGICAL SYSTEMS CAN *STILL* TELL US ABOUT INFORMATION SECURITY

Dorian Deane

Infosec researchers regularly look to biology for inspiration but the look is more of a glance and the end results are often superficial. Let us explore what happens if we go one step further by asking an apparently easy question: Most people agree that we'll never have perfect digital security so how do we know when we have enough? For a given asset, what is a reasonable amount of time and money to spend protecting it? Accountants looking at the bottom line say we are already spending too much; the rest of us feel that we need more. Biological organisms provide one source of unbiased guidance, leading us to a pair of interesting conclusions: We may be spending enough, but we are probably not spending in the right places. Said another way, immunity is more than just an immune system. And we learn one more thing: Despite the myriad analogies and even shared words between the two disciplines, biological defense mechanisms remain a largely untapped source of inspiration for infosec defenders.

ARE WE THERE YET?

The idea of using biological defense mechanisms as a source of ideas for information security is not new. Security researchers tend to point to biology for inspiration and then they are done. This discussion tries to show how valuable it can be to dig deeper. By way of example, we'll ask a seemingly simple question: What if we wanted to figure out how much we spend on information security for an asset of a given value? What would we look at? For the most part, that's a relatively easy question. We'd look at the costs of security-specific appliances such as firewalls, the cost of their maintenance, the security staff and their salaries and overhead, the opportunity cost of incident response, reputational costs, and so on. Going further, we would not just look at the cost of antivirus software but the cost of the CPU cycles required to run the security software on every laptop, desktop, and server out there. We'd add the cost of time spent entering passwords, response-time delays, the cost of maintaining password reset facilities, helpdesk support... We could go on and on, with ever more granular vision and we would probably end up arriving at a fairly accurate estimate of security's true costs.

Since we will never arrive at perfect security, how do we know when to stop spending? This is a new field. It is hard to tell. Calculating the cost of an avoided event is tough. And if all those articles on calculating Return on Investment seem to solve that problem,

why is there a new article almost every week purporting to show how to get there? (Hint: because the numbers going into the equation are highly fluid.)

So what if we wanted to look outside our own field for clues? We might look to physical security here in the US. We spend for various defense agencies, Coast Guard, National Guard, all the levels of law enforcement, fire fighters/trucks, fire breaks, fire hydrants and their supply systems, security guards, home security systems, fences, door locks, ubiquitous insurance, and cameras everywhere. Some questions are difficult, such as attributing the cost of a wall--is the wall for warmth, or security? Should protection from cold count as a security cost? We get a sense that if we tried to spend the equivalent on cyber security, we'd go instantly broke. Particularly because this area reaches well into the political arena, we sense that this may not be a sufficiently helpful analogy.

What about the human organism? Not counting behavioral mechanisms such as running from danger, how much does a human "spend," in terms of biological resources and energy costs, on security? That is likely an unanswerable question. Why it is unanswerable is fascinating, and it provides the focus for this discussion.

There is sometimes a perception that the human immune system, specifically the adaptive immune system, has been over-discussed by infosec researchers. But the adaptive immune system is only one part of the body's vast array of defenses[1]. Focusing on the adaptive immune system has been a comfortable model because it allows us to think of security as separate from the rest of the body, just like we have firewalls that are separate from web servers. Now, let's move beyond our comfort zone.

BIOLOGY IS A MESS

To support the broader concepts of this article, a survey of a very few of the myriad biological mechanisms that are devoted fully or partially to defense is in order. To call this nano-survey "high-level" is an understatement. Each discussion area below has consumed the careers of thousands of scientists worldwide, sometimes for centuries. Another point is that this discussion does not explore biology-inspired *solutions*--the aim is to get a sense of the overwhelming panorama of biological defense mechanisms.

Biology is a mess, a highly complex, fault-tolerant mess. Somehow, we remain "healthy" even while fighting a pitched battle with millions of sophisticated microscopic invaders. We continue to function as expected despite absolutely constant assaults that make our most sophisticated network attack tools look like the feeble flailing of a baby.

The action starts even before living skin is reached. The body's surface is a rich, active ecology of bacteria, both hostile and friendly[2]. It is a battleground. The bacteria in or on the human body number about ten times that of "human" cells (bacterial cells are much smaller, of course). Resist the urge to run to the nearest sink to scrub yourself: that bacterial ecosystem plays a protective role. Without the help of the good bacteria, the bad bacteria would have an easier time getting past our defenses. It is not too speculative to say that the very first line of human defense is not even human. We have outsourced some of the work to foreign mercenaries living on our skin, in our mouth, and other entry points. What is the cost of this security mechanism to the human body? The costs are varied but two are the cost of controlling reproduction of these bacteria (since unhindered reproduction would be deadly to the human host) and the risk of occasional bacterial outbreaks, resulting in skin infections which are usually brought under control, though at some energy and nutrient cost to the human host.

If an attacker can breach the bacterial forest above our skin, it still must work its way through the true perimeter, the skin itself[3]. It is a perimeter with many layers, starting with a protective overcoat of dead skin cells and the oily, anti-bacterial secretion from the underlying dermis called sebum. The living skin itself is composed of many layers--the epidermis alone has several layers before reaching the dermis. An attacker breaching these outer layers encounters yet more defenses such as antimicrobial peptides before it even reaches the dendritic cells which make up the first outposts of the adaptive immune system. And, again complicating our attempt at a cost model, some of these peptides have other non-security functions in the organism--as does the aforementioned sebum which both moisturizes the skin and inhibits bacteria.[4] Note that anti-microbial peptides abound throughout higher organisms[5].

Certain defense mechanisms within the skin itself seem to be more purely defense-related, such as the several types of white blood cells, each of which has an amazing array of destructive capabilities. Neutrophils are just one type, produced in the body by

the billions per day[6]. While one may be able to measure the energy cost to produce and maintain these short-lived defenders, there are still greater difficulties: how does one share the "cost" of the circulatory system which transports them while also transporting oxygen, hormones, nutrients, and so forth? It should become clear that, here, the important point is the astonishing array of integrated, overlapping defenses that are tightly coupled to every other aspect of the human organism.

There are "statistical assaults" on the integrity of the organism. Your body has made thousands of DNA replication errors in the time it took you to read this far.[7] Some are caused by outside forces such as UV radiation, but many others are a natural product of fundamental chemical processes. In any case, the likelihood that any of these errors will result in cancer is extremely small. The body has evolved repair mechanisms--integrity checkers--for most of these errors. The enzymes are right there in the cell, repairing the damage almost as soon as it occurs[8]. It might be possible, with great difficulty, to calculate the energy costs of creating those enzymes, providing space for them in the cell, and so on, but then we are stymied by the built-in security of the double helix, each strand of which acts as an integrity check--a reference point--for the other. (It is hard disk mirroring for living things.) And, yes, the repair mechanisms can distinguish between original and copy, though the mechanism is not yet entirely understood[9].

DEGENERATE RAPSCALLIONS!

Most of the above examples demonstrate how tightly defense mechanisms are coupled with other functions. An important related concept is degeneracy. This degeneracy is not the kind you hear older folks complaining about from their front porch rockers; in biology, it defines a condition in which multiple, often dissimilar mechanisms can accomplish the same goal[10]. The archetypal example in the literature describes how multiple codons will build the same amino acid;[11] examples are common throughout the biological world. This degenerate approach is in contrast to highly-designed (at least on paper) engineering solutions where the network firewall attends to network traffic, the intrusion detection system detects anomalies, the antivirus checker looks for virus signatures, and different types of data all exist within their own cozy boundaries. In the non-degenerate world, there may be redundancy, but that redundancy is provided by identical devices performing identical tasks in exactly the same way.

Degeneracy may sound like a simple concept and perhaps it is, but its application to information security should not be ignored. A system that is merely redundant cannot change its behavior as circumstances change. A system that has no redundancy is highly efficient under ideal conditions but may fail entirely with the failure of any of its components. Degenerate systems define a middle ground where different structures can, under certain circumstances, produce identical outputs. Besides the classic example of multiple amino acid encodings, some enzymes share the same function despite different underlying amino acid sequences. Even more impressively, under certain conditions, completely different metabolic pathways may accomplish the same task under a variety of environmental conditions[12],[13]. Examples of degeneracy abound in nature. They have been most studied in neurology but evolution's blind approach to problem-solving guarantees that even fairly simple organism show degenerate qualities.

Malice in Wonderland

It may be helpful to imagine what information security mechanisms might look like if they had evolved in the same evolutionary crucible as ourselves. To take a whimsical snapshot... the network firewall might correctly block network traffic most of the time but occasionally let the intrusion detection system take over for inscrutable reasons possibly related to packet size. If that system detected a certain malware signature, it would send out a broadcast signal which only the log analyzer would recognize and promptly switch from reading logs to generating a certain log record of its own. This new log type would cause the C compiler to use wind energy to separate hydrogen and oxygen from water to create hydrogen fuel cells which would then be used for an extra boost during the overload period. At odd intervals, the antivirus software would take over log analysis after receiving a stress signal from the network interface's firmware. Researchers would also discover that the firewall sometimes acted as a coprocessor for the CPU and the intrusion detector on rare occasions would respond to a detected virus by deleting its own files. Some readers will rightly think that we are already approaching that bizarre state of affairs; but this article posits that, while an extreme example, there may be value in this degenerate mess. Certainly an attacker, pondering the defenses from outside, would be left scratching her head.

Conclusion

It is sometimes enlightening to miss the point--as when a misheard phrase leads to a

good idea. Let us momentarily pretend to do so here by considering cost. Even if the biological model argues for a lot more security in the silicon sphere, we need to remember that costs should be proportional to what is being protected. Most of us would not spend the same amount of money to save the life of a pet hamster as we would a human child. And there the point is missed. In a degenerate security model, security is already a part of all the bits and pieces that make up the system. As a result, security becomes proportional to complexity. The silicon world's equivalent of a hamster--say, a gmail account[14]--would have all the layers of security that naturally come with a system of that level of complexity. In more complex systems, with more routers, switches, and load balancers, there would naturally be proportionally more security. Adding complexity would add security--although whether there would be a net gain, diminishing returns, or some other relationship is beyond the scope of this discussion. One might also add more security-specific devices, the equivalent of those more specialized pieces of the adaptive immune system, but the baseline level of security would already be capable of survival in the wild.

Degenerate security is also harder for an attacker to overcome. Not only does she have to overcome multiple layers of security, they do not work exactly the same way, so the same flaw that got her past one device would not necessarily work further downstream. It has been speculated that this is another reason that such a pastiche of defenses has evolved within our bodies--it makes it that much harder for micro-invaders to evolve new offensive strategies.

Much of what has been discussed here may seem obvious. The general premise has been expressed in a single paragraph[15]. Yet, despite widespread agreement that biological models are useful, that is often as far as it goes. Even systems that claim to be "bio-inspired" rarely resemble their stated Muse more than superficially. I have avoided that trap here by keeping my goal relatively simple: I wanted to show that, while our information systems and networks are starting to approach biological organisms in their complexity, our security systems are both insufficiently diverse and, probably, insufficiently numerous. And, "numerous" does not have to imply unsupportable expense. If every piece of the whole adds its own resources to the overall security effort, the costs are more equitably distributed.

There is a small amount of degeneracy present in Internet systems today. And, true to the biological models, those degenerate qualities tend to look the least "designed" and arise from solutions tacked on to unrelated architectures more for convenience than pursuit of design elegance. (E.g., the Quality of Service function built into OpenSSH[16].)

To some, this article may seem more like a discussion of evolution versus design as it applies to information security. This is a dichotomy worth at least a passing mention. Biological defense systems seem like a grab-bag approach. Random tricks that happened to work were incorporated into a species' genetic makeup and stuck around for at least as long as they were useful, sometimes longer. There is an accretion of defense mechanisms over time, not a carefully thought out modular defense system. The concept of design is notably absent. In the infosec world, there is an interesting equivalent: Java versus Javascript. Despite the name similarities, the two languages are unrelated. Javascript evolved from a very limited, simple language to a behemoth that is behind much of the content you see on almost any web site you go to. Java, conversely, was designed specifically with security in mind. Initially, the securely designed language easily beat the evolutionary model. However, over time, as Javascript has "evolved" to fix problems as they arose, the picture became less clear.[17] Interestingly, genetically modified organisms may already be providing an analogy. A strain of corn designed to resist the rootworm was an unqualified success, much as Java was seen to be; but over time, attackers in the cyberworld and rootworms in the ground caught up and a clear winner is no longer obvious[18]. What is clear is that systems are growing ever more complex and, despite amazingly clever solutions from brilliant people all over the planet, it is still far easier to attack than defend. And the more complex the system or network is, the more true that statement becomes. Nor are we in a position to redesign everything from the ground up. By necessity, we must tack on solutions after the fact, thus ensuring that evolutionary measures will one day overtake initial design measures.

The biological cost question turns out to be unanswerable yet still enlightening. We learn that there are new directions to try and many more layers to develop. Security solutions should not focus on separate, loosely-coupled systems. Every function, method, and subroutine should add its own ingredient to the security soup. Perhaps no single security mechanism will ever stand up long to a determined attacker but we have a right to expect that, when every piece of the whole pulls its own weight, successful

attacks will at least be difficult.

Finally, if this discussion causes anyone to revisit the question of what biological defense systems can teach us about defense in depth, that is no accident. The initial cost question was an excuse, a frame on which to hang the larger picture. If such simple questions as this can result in useful insights, imagine what a deeper investigation can do. Even the adaptive immune system--mostly ignored here but oft-discussedby security researchers--is still largely untapped. The feedback systems among the types of white blood cells alone should provide a lifetime of inspiration.[19]

[1] Security researchers tend to focus on a few key aspects of the innate immune system and focus more on the learning capabilities of the adaptive immune system. For simplicity, I am broadly painting all these things under the heading of "adaptive."
[2] Skin Microflora and Bacterial Infections of the Skin, Journal of Investigative Dermatology Symposium Proceedings (2001) 6, 170–174, Katarina Chiller, Bryan A Selkin and George J Murakawa
http://www.nature.com/jidsp/journal/v6/n3/full/5640052a.html
[3] Skin Anatomy, from Heather Brannon, MD, former About.com Guide, Updated April 09, 2007
http://dermatology.about.com/cs/skinanatomy/a/anatomy.htm
[4] Cutaneous Defense Mechanisms by Antimicrobial Peptides
Marissa H Braff, Antoanella Bardan, Victor Nizet† and Richard L Gallo
http://www.nature.com/jid/journal/v125/n1/full/5603230a.html
[5] Mechanisms of Antimicrobial Peptide Action and Resistance
Michael R. Yeaman and Nannette Y. Yount
http://pharmrev.aspetjournals.org/content/55/1/27.full
[6] "neutrophil" *Encyclopædia Britannica. Encyclopædia Britannica Online*. Encyclopædia Britannica Inc., 2012. Web. 15 Jan. 2012, http://www.britannica.com/EBchecked/topic/410999/neutrophil
[7] DNA Replication and Causes of Mutation, Pray, L. (2008) DNA replication and causes of mutation. Nature Education, http://www.nature.com/scitable/topicpage/dna-replication-and-causes-of-mutation-409
[8] Vanderbilt University. "Newly discovered DNA repair mechanism." *ScienceDaily*, 4 Oct. 2010. Web. 15 Jan. 2012, http://www.sciencedaily.com/releases/2010/10/101004112156..htm
[9] DNA repair, Journal of Cell Science, 2004, Oliver Fleck and Olaf Nielsen
http://jcs.biologists.org/content/117/4/515.full
[10] Degeneracy and complexity in biological systems, Gerald M. Edelman and Joseph A. Gally, The Neurosciences Institute, La Jolla, CA 92121 http://www.pnas.org/content/98/24/13763.%20long
[11] http://www.sci.sdsu.edu/~smaloy/MicrobialGenetics/topics/rev-sup/wobble.html
[12] The Soluble and Membrane-bound Transhydrogenases UdhA and PntAB Have Divergent Functions in NADPH Metabolism of Escherichia coli
Uwe Sauer, Fabrizio Canonaco, Sylvia Heri, Annik Perrenoud and Eliane Fischer
http://www.jbc.org/content/279/8/6613.long
[13] Ecological genetics: The decline and fall of a metabolic pathway in yeast
R C MacLean, http://www.nature.com/hdy/journal/v94/n3/full/6800632a.html
[14] Apologies to both pet hamsters and gmail account users with particular emphasis on gmail-using hamsters.
[15] http://www.schneier.com/essay-007.html (The paragraph that starts, "It's hard to fight...")
[16] http://www.openbsd.org/cgi-bin/man.cgi?query=sshdconfig&sektion=5
[17] I am well aware that I am stepping onto the battlefield of yet another ongoing holy war. I informally surveyed a variety of statistics, many of them found at http://www.securelist.com/en/statistics#/en/map/oas/month to support my unscientific conclusion. Suffice it to say that this question is an interesting one and is, in this author's opinion, worthy of more research.
[18] IO9: Pesky insects becoming resistant to genetically modified corn, 01/01/2012
http://io9.com/5872304/pesky-insects-becoming-resistant-to-genetically-modified-corn
[19] "New Nano Device Detects Immune System Cell Signaling" ScienceDaily.com, Sep. 3, 2008,
http://www.sciencedaily.com/releases/2008/09/080903172412.htm

THE FORAGING TANGO: THE APPLICATION OF OPTIMAL FORAGING THEORY TO COUNTERTERRORISM ACTIVITIES

Don Arp Jr.

Terrorism is the ever-present specter of our times. Individuals and groups of all dogmas, creeds, religions, and other motivations exist with the goal, actualized or not, to convey their messages with violence. The motivating ideologies of the groups are complicated, with much significance being placed on understanding these belief systems in order to mitigate the threat. What results is a daunting, confusing, and often jumbled ideological safari. To add operational clarity to this pursuit, analysts should also look at the basest elements of terrorist behavior, actions that cut across all groups, and use this to gain focus in order to develop counter-terror strategies. Terrorists, at their cores, are hunters, searching for prey that meets their needs. This search is controlled by many variables that, unbeknownst to the terrorist, control what targets are pursued. This behavior can be best understood through application of Optimal Foraging Theory (OFT), a construct of anthropology that seeks to understand human foraging and hunting. Extrapolating OFT to homeland security gives the field a tool to model behavior, understand trends, and develop strategies.

OPTIMAL FORAGING THEORY

OFT is evolutionary in its philosophy. OFT "models assume that foragers have a goal, which is to maximize their net rate of return while foraging because by doing so they are ultimately able to maximize their fitness."[1] This fitness and natural selection are central to OFT and the much broader concept of Human Behavioral Ecology (HBE). Cronk notes that HBE "may be defined as the study of the evolutionary ecology of human behavior. Its central problem is to discover the ways which the behavior of modern humans reflects our species/ history of natural selection."[2] OFT uses a proxy currency for analyzing these efforts, namely energy gained, to determine fitness. Foraging activities are governed by deciding what to eat, where to find it, and how long to spend in the process. This being said, foraging activities can be judged for their overall value based on a simple ratio of energy gained to time spent in finding and processing the prey, which is a simple cost-benefit exercise to an extent. The less time spent finding and handling the prey maximizes the value of the activity - - you get more for less.

EXPANDING OFT

The application of HBE and OFT to new fields is ripe. One expert noted that HBE concepts are most prevalent in anthropology and psychology but, "It has been resisted in departments such as sociology and political science where the findings on human evolution are either ignored or regarded as irrelevant."[3] This is interesting consider that approaches like OFT take concepts from other fields. Foraging theory borrows terminology and methods from economics, decision theory, and operations research.[4] Human development does not happen in a vacuum and all processes can be understood from an evolutionary perspective. So, the time for cross pollination and expansion is overdue.

APPLYING OFT

Base Assumption

Although OFT seeks to understand the individual's role in selection and avoids group concepts, given their often unifying basic ideologies, for the purposes of this essay it is necessary to see terror actors, whether they are groups or individuals, as a theoretical, cohesive entity like an individual.

The Profitability Calculation

OFT uses energy as its proxy currency for fitness - - the more energy you can gain from foraging activities, the more fit for survival you are and thus the more offspring you can have. For the most part this scheme can be considered mathematically where the profitability of an activity is measured by dividing the gain, in OFT's case this is calories, by the amount of time it took to find and handle the prey. Here's the equation:

$$\text{Profitability} = \text{Gain} \div \text{Resources}$$

The currency is critical in setting up the ratio to determine profitability and must be balanced against a control such as time. In the essay here, currency is best called *impact* and can be seen as body count, property damage, financial loss, and/or changes to lifeways. Further, time needs to be expanded to the more general concept of *resources* including time, people, money, and material. Success is governed by how this ratio works. The more resources required, the more the gain is reduced. Considering the profitability equation and OFT's divisor of time, one can see how

manipulating this ratio is used to develop strategies for survival. Organisms with shells, quills, spikes, and spines all increase processing time, which requires energy, and thus reduces energy gain. In the math, a prey that requires too much handling is abandoned for another unless some other benefit makes the investment worthwhile. In counterterrorism, we can extrapolate a defensive strategy using the ratio, namely the more resources a group needs to use to achieve its goal, the less likely they are to find the investment profitable.

WHAT TARGETS ARE THEY GOING TO SELECT?

In foraging activities, whether for prey or targets, limitations abound. Difficulty in handling prey is secondary to what prey is available, and this is controlled by environment. The nature of the environment and the prey possible greatly controls the outcome of the profitability equation. Generally, unproductive environments require prey diversification, whereas productive environments produce specialization. For the most part, terrorism is rather specialized in target selection given wide range of possibilities in urban and semi-urban areas. Other approaches have been implemented to address selection issues. For example, roadside improvised explosive devices are designed for a type of target (like a car, truck, or convoy) and not a specific target. This developed because of target hardening in other areas, forcing a somewhat more diverse target selection strategy in less secured, but more variable conditions. Groups focused on weak points (transportation columns) and hit whatever came by.

Target size can also impact selection. In the same manner that a hunter might choose to pass on small game or overly large game, the foraging terrorist is the same. Committing resources to an attack on a target that is too large or defended is counter-productive, as is wasting resources on a target that is too small. A balance must always be considered.

THE FORAGING TANGO: EXAMPLES OF USING OFT TO RESPOND

The Low Cost Attack

Terror groups have already discovered the return on investment concept inherent in OFT. The group al-Qaeda in the Arabian Peninsula (AQAP) touted that it spent slightly more than $4,000 to attempt to mail two parcel bombs to the United States. The parcels were intercepted and failed to detonate.[5] This was a significant step in strategic sophistication. If the bombs destroyed the plane or arrived at the intended destination, then AQAP had a level of success. But even with the bombs found, AQAP had significant success in that the attack will no doubt cause significant security investment on

the part of shipping companies. Attacks on shipping, fuel supply, domestic transport, and basic infrastructure like water treatment and electricity would all have a similar impact.

Response

The investment theory is in the wild, so what can be done as a strategy to address the threats? We know the terror groups are behaving according to OFT to save resources, so we can use OFT to address what is happening. Clearly, the profitability equation needs to be tilted in another direction. In attacks conducted or planned in accordance with OFT, the leader of the group is not as important as the sources of money and technical knowledge. Targeting a group's banker and engineer will be more effective and beneficial than taking out the leader, no matter how integrated into strategy that person may be. Further, if small attacks or attempted attacks can be linked, then we know the theory behind the events and can escalate targeting of different persons and resource caches, and try to avert costly overreaction.

The Costly Investment Attack

Certain types of attacks are going to be serious resource investments for terrorist groups, but to them the investment is worth it because the gain is much higher. September 11 is an example. The cost in people, training, time, and support were significant for al-Qaeda, but from their perspective the investment was worth it due to the possible impact.

Response

If intelligence is available that a major attack is planned, back-calculating the OFT equation can be of use. Much like the previous attack, focusing on sources of cash is critical, as well as infrastructure both domestically and abroad. Removing related cells limits sources of support. Removing suspected safehouses and escape routes increases pressure. Hitting foreign resources like operational advisors and engineers is also critical. In this instance, we are not trying so much to shift the balance of the equation, but rather deny the group of the resources needed for the calculation. Further, if sources of major investment can be removed, the impact on the organization as a whole can be tremendous and can subvert other operations.

CONCLUSION

Terrorist attacks are evolving in operational and strategic sophistication. Alongside car bombs and body count, groups are also considering resource impact on their side and financial impact on the

other side. A cheap attack that can result in tying up millions of dollars in new security processes is, at times, more effective than high property damage operations. As terrorists look for new targets, they are operating no differently than hunters and gatherers foraging for food. The environment, resources, and gains all govern the activity. With each effort, more efficient strategies are developed that maximize gain and likewise evolutionary fitness. By deploying the concept of Optimal Foraging Theory to our analysis of terrorist activities, we can gain a better understanding of the adaptive strategies employed by terrorist groups and use this insight to respond in the necessary manner.

---

[1] Hames, R. (2001). "Human Behavioral Ecology" in *International Encyclopedia of the Social & Behavioral Sciences*. Elsevier Science Ltd., pg. 6948.
[2] Cronk, L. (1991). "Human Behavioral Ecology" in *Annual Review of Anthropology*, No. 20, pg. 25.
[3] Hames, pg. 6951.
[4] Smith, E. "Anthropological Applications of Optimal Foraging Theory: A Critical Review" in *Current Anthropology* Vol. 24, No. 5, pg. 626.
[5] Yemen group vows small-scale attacks, November 21, 2010, CBC News

IMPROVING HOMELAND SECURITY THROUGH LOOPS AND LINKS

John M. Hartzell

The September 11, 2001 terrorist attacks on the United States unalterably changed the status quo ante. Billions of dollars were spent, numerous laws and regulations written, policies developed, and new agencies, departments, and a military combatant command created to protect the United States and its citizenry through new governmental constructs. Despite these unprecedented efforts, Homeland Security remains an unfinished job. Strategic and governmental challenges and other shortfalls limit the effectiveness of the United States' efforts to protect the country against future attacks. Moreover, the focus on counterterrorism undermines the effectiveness of first responders to the natural disasters they are more likely to face.

These shortcomings are not the malicious product of saboteurs, but the inefficiencies naturally developed in a governmental system that requires compromise, where progress is incremental, and where policy develops by "muddling through."[1] Efforts to minimize the inherent challenges of a federal structure, from identification of critical infrastructure, to fusion centers and the development of broad strategies and policies, have helped create a focus. But the reality remains that federal agencies with different cultures,[2] an overlay of Homeland Security responsibilities on top of existing missions,[3] and state and local responders who have vastly different objectives, all require incredible flexibility to maximize opportunities for success.

Developing individual strategies that will apply to each agency, regardless of type or governmental level – local and state police forces, federal agencies, and emergency service providers of all services, yet alone the military – is possible through adopting a strategic tool that will allow agencies to develop common conceptual pictures, while acknowledging the differences in the culture, style and capability of each organization. Such a tool exists in the Boyd cycle, or OODA Loop, a construct developed by the late John Boyd, a retired U.S. Air Force Colonel.[4] Under this construct federal, state, and local agencies can develop the strategic insights that will enable them to anticipate, plan for, and respond to threats in manners uniquely relevant to their own culture and challenges, while following similar constructs. Through this, U. S. Homeland Security can rapidly evolve into a more dynamic and robust group of capabilities.

THE CURRENT CHALLENGE

Homeland Security evolved out of a federal response to a crisis. As often occurs in a response to a failure, the federal government developed a hierarchical, top-down model, where direction and control was centralized in a federal agency, the Department of Homeland Security.[5] Such an approach seemed logical in light of the threat of terrorism. This method recognized "the standard administrative approach to complex problems" where hierarchy establishes control, allocates responsibilities and reporting requirements, defines tasks, and attempts to create reliability and responsibility in work flow.[6]

While such an approach is logical, it fails to recognize a number of constructs of emergency response. First, state and local agencies have primacy in responses to local disasters, with federal assistance being required only after the disaster has been considered major.[7] Second, local response requires a multitude of skills: emergency medical services, firefighting, law enforcement, and search and rescue, among others. Each of these different capabilities suggests different organizations and skills, and accompanying cultures, values, and priorities. Lastly, emergency responses to crises – to terrorist attacks, or natural disasters – are incredibly dynamic efforts that require intense coordination in short order across a multitude of disciplines, issues, and concerns. These responses do not align well with hierarchical control and direction.

Common constructs and ideas are necessary as unifying concepts. The National Strategy for Homeland Security published by President George W. Bush in October 2007 provided four goals for our nation: (1) prevent and disrupt terrorist attacks; (2) protect the American people, our critical infrastructure, and key resources; (3) respond to and recover from incidents that do occur; and (4) continue to strengthen the foundation to ensure our long-term success.[8] Various executive branch agencies have been involved in the production of a plethora of policies and directives that echo the focus on protection of key infrastructure and prevention of terrorist attacks. Dozens of Homeland Presidential Security Directives have been written, providing guidance on topics as diverse as Arctic Region Policy (HSPD-25), National Preparedness (HSPD-8), and Management of Domestic Incidents (HSPD-5). However, each of these policies requires months of refinement through the interagency process, and the flexibility necessary for tactical and operational response is not evident.

An additional challenge is that despite the investment in state, local and regional fusion centers under the auspices of the 9/11 Commission Act and predecessor programs, fusion centers are limited in their impacts because of their construct. They were developed to provide tactical intelligence, to fuse information from different sources, and to perform intelligence analysis. But,

while these facilities are focused on preventing terrorist attacks, they do not create a common strategic viewpoint. Further, programmatic reviews of fusion centers have shown mission creep toward traditional law enforcement functions, weak guidance concerning data mining standards, as well as considerable challenges at different fusion centers over appropriate targets on investigation.[9] From a larger perspective, fusion centers provide information, but not the greater understanding that helps each organization understand its individual role, or develop unique interactive capabilities.

To effectively function in the new homeland security milieu, each organization – whether federal, state, or local – needs to understand its role in the greater sphere. Such understanding requires internal reference. Organizational study requires understanding of the cultural, organizational, societal, and value-based concepts that define and undergird each entity. This internal evaluation is necessary to understand the beliefs each organization uses as its own, the methodology used in examining external stimuli, and the best means of developing organizational understanding.[10]

THE OODA LOOP

The OODA Loop is an iterative decision cycle, similar to other processes used in business and governmental applications. Unlike others, however, the OODA Loop provides self-referential analysis, as well as feedback loops. These feedback loops, which evolved out of the systems theory approach to organizational theory, build on the concept of organizations as adaptive systems relying on self-regulation.[11]

The OODA loop develops its unique name as a mnemonic for the four-part cycle it describes: Observe, Orient, Decide, and Act. The OODA Loop developed from the life study of Colonel John Boyd, an F-86 fighter pilot who combined an understanding of quick decision making skills from the cockpit with a lifetime study of military history and intellectual constructs.

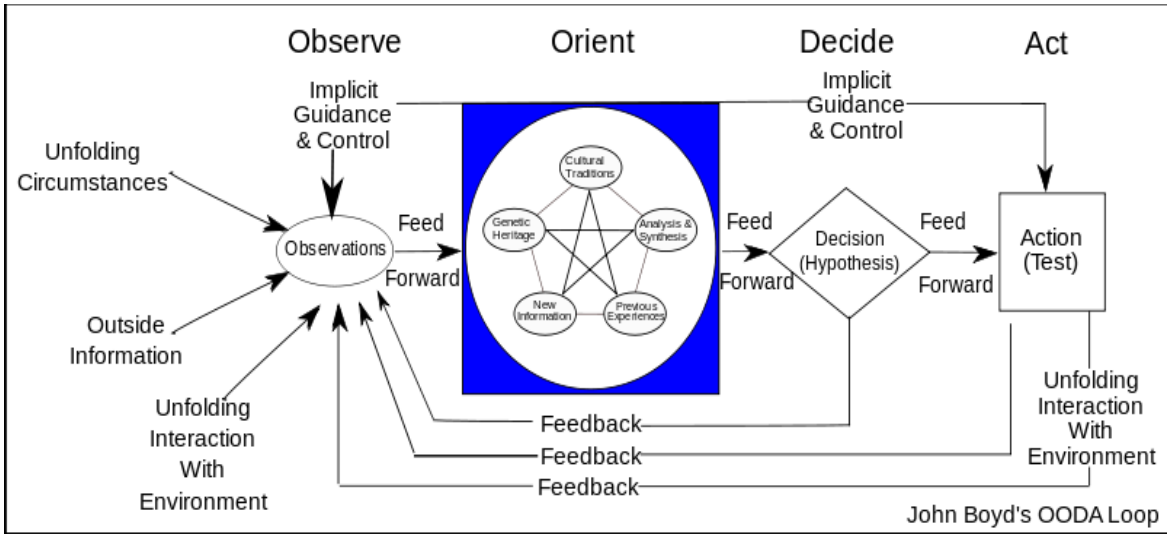

Figure 1. Boyd's OODA Loop.

The OODA Loop has been praised for many reasons by diverse practitioners, including business theorists, military action proponents, strategic thinkers, and intellectuals. Proponents have appreciated the quick responses of users of the OODA Loop and the ability of the construct to lead to the defeat of slower adversaries, as well as the OODA Loop's applicability to Grand Strategy.

The OODA Loop starts with Observe (Observation), or the detection of some activity. The second phase is the Orient (Orientation) component of the Loop. It is here that the construct is so unique. Orientation requires self-awareness, and what one sees is dependent upon the observer's own background: Thomas Kuhn called it the "previous visual-conceptual experience," while Boyd considered it the interplay of cultural traditions, genetic heritage, previous experiences, and unfolding circumstances.[12] The Orient phase requires both internal reflection, as well as analytical application of the same construct upon the opponent, or upon the different circumstances with which the observer may be required to interact. Those focused on rapid success and quick tactical solutions may only consider the last of these internal components, or "unfolding circumstances."[13] However, application of the entire Orient phase, both internally and externally, as well as evaluation of insights gained, provide unique benefits. Survival and growth in a complex, ever changing world of conflict requires insight, vision, focus, and direction. This requires efficient and effective orientation, which necessitates "quickly and accurately developed mental images, or schema, to help comprehend and cope with the vast array of threatening and non-threatening events we face."[14]

The OODA Loop then moves forward to the Decide (Decision) phase, where actors or

organizations decide among alternatives that are developed in the Orientation phase. The Act (or Action) phase requires rapid application of the chosen activity, and the application of the decision provides testing of the action developed during the Decide phase (also called the hypothesis).[15] These activities provide feedback on the appropriateness of the Orientation phase, and are not a simple "feed forward" mechanism, but a process providing feedback and corrective direction at every phase of the cycle.[16]

Boyd's OODA Loop is not merely a decision mechanism for military command and control, nor the latest version of a quick-action process that originated in the cockpit of a first generation jet fighter. Instead, it is an iterative activity incorporating the scientific process, learning, neo-Darwinists, and the approaches of many great thinkers and strategist, in a complex adaptive system.[17]

THE OODA LOOP'S APPLICATION TO HOMELAND SECURITY

How does such a tool provide greater insights and applicability in Homeland Security? By allowing different organizations, in different contexts, to ensure they have the ability to strategically plan for activities in specific environments, and at the same time to allow other organizations to rapidly and accurately respond in operational situations. The OODA Loop provides this flexibility for strategic, operational, and tactical situations, while also providing planning and response capabilities for different organizations, from military to emergency response.

Theorists examining the multi-agency response to the World Trade Center attacks of September 11, 2001, found that the dynamic, extreme environment "presented an extraordinary test of [public agencies'] capacity to function under the most severe conditions of disruption and destruction."[18] The researchers found that responding organizations required the ability "to adapt quickly and effectively to rapidly changing conditions."[19] Such environments require structures and approaches that allow the organizations to rapidly receive large volumes of information and observations, and to learn and self-organize from those inputs. Such an approach is considered an auto-adaptive system.[20]

Boyd's OODA Loop provides organizations these enhanced capabilities, aligning well with auto-adaptive concepts. Comfort and Kapucu identify the following sequential steps for an auto-adaptive response organization: information search, information exchange, sensemaking, adaptation, and auto-adaption.[21] The OODA Loop's Observation phase aligns with both information search and information exchange, assuming that the organization's mission requires close coordination with

other organizations. The Orientation phase of the OODA Loop aligns with sensemaking, the two constructs being remarkably similar in their means of developing insights and referencing cultural and other organizational value constructs. Both the Decision and Action components of the OODA Loop align well with adaptation, where the organization modifies its interactions with the unique environments or situations. Auto-adaption is not merely a phase of the OODA Loop, but the entire process, and the OODA Loop's innate ability to change direction and responses due to the myriad feedback loops and other corrective components included within the Loop. Thus, the OODA Loop provides the capabilities theorists believe will assist an organization most responsive to emergency crises.

The OODA Loop is also scalable, which provides additional value. An Australian Army Officer suggested the OODA Loop provides great value in assessing strategy for the U.S. Homeland Security mission. While Lieutenant Colonel Thomas' article analyzed numerous Boyd concepts in the context of the 9/11 Commission Report, a central construct is that the OODA Loop highlights "the importance of continuous orientation and, in particular, the need to understand culture (friendly, adversary, and that of the operating environment)."[22] Thomas truncated OODA Loop analysis of the U.S. efforts prior to the 9/11 attacks suggests both the contemporary failure of federal agencies to apply this construct prior to the attacks, as well as the potential benefit of its future use to defeat terrorist machinations.[23]

CONCLUSIONS

The OODA Loop has developed a strong following in military and strategic thinking, and is valued in many circles. For instance, the application of this approach and other Boydian constructs were praised by a retired United States Marine Corps Commandant in a letter following John Boyd's death in 1997.[24] But while the OODA Loop provides utility from a number of perspectives, it will never devolve to the level that an OODA Officer will sit next to a Fire Department Battalion Chief at an operational command post, ensuring that the disaster response properly evaluates cultural and environmental differences. Such an application would be a formalistic approach that would miss the importance of the concept's application to broader activities, and the need for re-tooling that will infuse the entire organization with the elements required for the construct's successful use.

The unique challenge of Homeland Security is that numerous agencies, organizations, and groups, at all levels of government, from volunteer to professional, with varying missions, and using tools as varied as lethal force to humanitarian rescue hoists, all have to find their own means of succeeding at their mission. Moreover, success must occur in any number of different environments,

with the organizations being mindful of their own cultures, values, beliefs, and norms. Guiding national policies help, but they cannot provide the granularity necessary, or the specific approaches required for each organization. The OODA Loop construct can meet this challenge and allow linkages to networks of similarly challenged organizations attempting the same, all while allowing organizations to manifest their unique cultures.[25] Such an approach is necessary to succeed in the unique challenges that will face our nation for many years to come.

---

[1]Charles Lindblom, "The Science of 'Muddling Through,'" *Public Administration Review* 19, no. 2 (Spring 1959): 88.
[2]Donald F. Kettl, *Systems under Stress: Homeland Security and American Politics,* 2d ed. (Washington, DC: CQ Press, 2007), 42-43.
[3]Ibid., 58.
[4]Grant T. Hammond, *The Mind of War: John Boyd and American Security* (Washington, DC: Smithsonian Institution Press, 2001), 2-5.
[5]Thomas A. Birkland, "Disasters, Catastrophes, and Policy Failure in the Homeland Security Era," *Review of Policy Research* 26, no. 4 (2009): 428.
[6]Louise K. Comfort and Naim Kapucu, "Inter-Organizational Coordination in Extreme Events: The World Trade Center Attacks, September 11, 2001," *Natural Hazards* 39, no. 2 (2006): 312.
[7]James F. Miskel, *Disaster Response and Homeland Security* (Stanford, CA: Stanford University Press, 2008), 19-20, 34.
[8]U.S. President, *National Strategy for Homeland Security,* October 2007, https://www.hsdl.org/?view&did=479633.
[9]Torin Monahan, "The Future of Security? Surveillance Operations at Homeland Security Fusion Centers," *Social Justice* 37, nos. 2-3 (2010-2011): 87-95.
[10]Gareth Morgan, *Images of Organization* (Beverly Hills, CA: Sage Publications, Inc., 1986), 321-337.
[11]Jay M. Shafritz and J. Steven Ott, *Classics of Organizational Theory,* 5th ed. (Belmont, CA: Wadsworth Group/Thomson Learning, 2001), 241-245.
[12]Daniel Ford, *A Vision So Noble: John Boyd, the OODA Loop, and America's War on Terror* (Durham, NH: Warbird Books, 2010), 22.
[13]Ibid., 22-23.
[14]Frans P. B. Osinga, *Science, Strategy and War* (London: Routledge, 2007), 230.
[15]Ibid., 232.
[16]Ford, 23.
[17]Osinga, 232.
[18]Comfort and Kapucu, 310.
[19]Ibid., 312.
[20]Ibid., 313.
[21] Ibid., 324-326.
[22]Jason Thomas, "Abandoning the Temple: John Boyd and Contemporary Strategy," *Australian Army Journal* 7, no. 3 (Summer 2010), 103.
[23]Ibid., 100-101.
[24]Hammond, 3-4.
[25]Jonathan R. White, *Terrorism and Homeland Security,* 6th ed. (Belmont, CA: Thomson Wadsworth, 2009), 446-455.

FIGHTING FEAR APPEAL; ADOPTING SOCIAL PSYCHOLOGICAL MODELS TO INFORM GOVERNMENT RISK COMMUNICATION

Sage Moon

INTRODUCTION

Message effects models from the realm of social psychology have the potential to add significant value to current government risk communication in the field of homeland security but have not been sufficiently considered in public messaging tactics. Effective communication extends beyond audience identification and message delivery. Government risk communications do not presently factor social psychological analyses into messaging strategies which has resulted in an inherent lack of understanding of how messages are processed and acted upon by the public. In place of such analysis, all too often government risk communicators blindly use fear tactics to ensure messages are understood.

Heuristics, social norms, and mental models predict human behavior based on typical thought processes and each provides insight into the outcomes hypothesized by popular message effects models. Three relevant models set forth by Kenzie A. Cameron (2009)—the Protection Motivation Theory, Extended Parallel Process Model, and the Language Expectancy Theory—are particularly applicable to the field of homeland security where behavior change in the public often results in lives, property, and money saved. These models and social psychological insights help clarify the existing global context which may affect message interpretation, identify mental processes (both rational and irrational), and recognize pre-conceived notions held by the public regarding how things ‗ought' to work.

Homeland security can directly benefit from the application of social psychological tools in order to bypass the failures of common fear-based communications and enhance message success. Social psychology and risk communication theories tell us that persuasive communication can be effective; however, despite its regular use, fear is not the proper tool to ensure message efficacy.
This paper seeks to explain why fear is not the most appropriate communication tool and further, based on social psychology and message effects models, what tools are effective when seeking to

influence public behavior.

FEAR APPEALS

Fear appeals are messaging tactics that attempt to stimulate fear in order to achieve a particular response. Emergency management and the broader field of homeland security often rely on fear appeals to ensure a desired public reaction. However, current models show that ‗coping appraisals' predict responsive actions more so than threat perception and that processes initiated by individuals to control their emotion interfere with their motivation to act as instructed (Ruiter). Heuristics—mental short-cuts; social norms—behavioral expectations within society; and mental models—pre-conceived frameworks, may affect both an individual's fear control process as well as their threat perception which further affects the weight assigned to the message and ultimately the individual's interest in, and ability to, act.

PERSUASIVE COMMUNICATION

Individuals respond differently to messages and communicators must be strategic in understanding and applying psychological processes if their intent is to change behavior.

According to Cameron, persuasive communication includes three stages: ―…response shaping, response reinforcing, and response changing.‖ Response shaping is defined as ―…the creation of responses to a new stimulus…‖ Response reinforcing is, ―reinforcing a decision…‖ and response changing is simply behavior change. Cameron indicates that, ―A critical factor across all three processes is that persuasion is constrained to intentional behavior.‖ While communicators are limited to the persuasion of intentional behavior, they must still account for and understand the emotional and immediate thinking which will affect both intentional and unintentional behavior.

HEURISTICS

Bazerman and Moore (2009) discuss the power of heuristics in Judgment in Managerial Decision Making. The ‗availability' heuristic affects an individual's perception of a threat by convoluting logic with an emotional connection—the individual's ability to imagine potential damages. Threat perception can be influenced by previous communications, experiences, or preexisting understanding. Bazerman and Moore provide the following example: ―An event that evokes emotions

and is vivid, easily imagined, and specific will be more available than an event that is unemotional in nature, bland, difficult to imagine, or vague.‖ An attempt to scare the public into action when a threat is not emotionally available will possibly result in control of the immediate emotional response (fear) rather than response to the danger thus rendering the message ineffective. Consideration of this heuristic will create relevance for the intended audience and bypass the possibility of disregard due to lack of emotional connection.

Emotional reaction is further addressed by Slovic et. al. (2004) who divide an individual‘s thought process into the —experiential system‖ and the —analytic system.‖ The —analytic system‖ uses deliberate processes such as logic and the rational cycle of risk assessment. The —experiential system‖ reflects an individual‘s immediate and intuitive reaction. The language used by governments to communicate risk can affect how an individual perceives the severity of a threat as well as how an individual perceives their own ability to mitigate the risk. The process is two-fold; information communicated may or may not make it past an individual‘s —experiential system‖ and if it does, it will either be acted upon (often emotionally) or processed through their —analytic system.‖ Zajonc (1980) argues that an individual‘s instinctual reaction actually guides how additional information is processed by the analytic system. The structure of risk communication is imperative as the first few seconds of an individual‘s immediate reaction will guide their engagement in preparedness activities or response to threat information. This idea of System 1 versus System 2 thinking is paramount to the analysis of fear appeal efficacy. In fear-based communications, fear is the immediate, experiential response, and the emotion alone will guide the ‗logic‘ to follow which may lead to undesired reactions.

Heuristics are important in homeland security risk communication because they give communicators an understanding of the intended audience‘s baseline thought processes—a map of the mental shortcuts people ‗typically‘ take. This insight, when considered, can guide messaging in a way that contributes to the success of homeland security goals and the overall safety and wellbeing of the public.

SOCIAL NORMS AND MENTAL MODELS

Despite the use of documented facts and expert opinions, message recipients hold ‗mental models‘ – the foundation of their comprehension—which affect their assessment of threats as well as their own self-efficacy. A fear appeal merely raises the stakes. According to McComas, —[when] people have

greater affective responses (e.g., more worry) and feel greater social pressure to learn more about the risk, they tend to perceive a greater need for information.‖ A fear appeal can create greater affective responses but it can also prompt inaction—in such a case, an individual‘s response may be guided by what they feel is socially acceptable rather than what is safe or advised. Social norms are simply a compilation of mental models with a focus on the most common or socially approved. Mental models are created based on feelings, knowledge, rumors, associations, and inferences of the risk. The three message effects models discussed in this paper are greatly shaped by heuristics, mental models, and social norms.

MESSAGE EFFECTS MODELS

Message effects are a category of theoretical models that provide frameworks for decision making and creation of message content that affect System 1 and System 2 process outcomes. The most controversial function of message effects models is the use of fear appeals. The Extended Parallel Process Model, Protection Motivation Theory, and Language Expectancy Theory are all message effects models that illustrate possible outcomes from various communication strategies; including the use of fear appeals.

Extended Parallel Process Model (EPPM)

The Extended Parallel Process Model developed by Witte (1994) posits two review processes that occur when risk is communicated (both with and without the use of fear appeals): threat and efficacy. An individual first identifies their perception of the threat; if they do not perceive the threat to be high then they do not move any further in the model and disregard the message. If they perceive the threat to be relevant, they then appraise their self-efficacy as well as the efficacy of the recommended action. Action will be taken if the threat is perceived to be high and if the individual finds the recommendation credible and their own ability to perform the recommended actions realistic. One of the main concerns with the use of fear appeals, as illustrated by the EPPM, is that individuals may attempt to control the danger after assessing the threat and identifying their self-efficacy as high, which is ideal, or they may attempt to control their fear based on a low perception of self-efficacy which leads them to ignore the precautions recommended simply because they do not believe they are capable of taking action.

The literature suggests that fear arousal may result in what Ruiter et. al. consider —avoidant coping.‖ They suggest that, —A greater focus on precautionary information and the promotion of action at the

expense of prompting fear arousal is likely to be more consistently effective than attempts to frighten people…‖ Ultimately, the precautionary or preparedness actions that can be taken to lessen the impact of a threat should be at the forefront of communications rather than the potential consequences of inaction. This holds true during all phases of emergency management and similarly can be applied across all homeland security agencies when communicating risk.

Protection Motivation Theory

The Protection Motivation Theory addresses danger control, not fear control. This theory is useful in understanding circumstances in which an individual has a high perception of a threat and a high perception of self-efficacy. The theory posits the four following ideas: the probability of hazard occurrence leads individuals to perceive their susceptibility, discussion of the possible magnitude leads individuals to perceive the severity they will experience, discussion of the effectiveness of recommendations leads individuals to perceive the efficacy of the recommendations, and discussion of any one individual's ability to perform the recommendations leads the individual to perceive their own self-efficacy. All are shaped by the emotions, experiences, knowledge, and inferences made by the individual prior to receiving the message. For instance, susceptibility to a flood can be inferred by the discussion of probability in the message just as much as it can be shaped by social norms or personal experience in a flood prone area.

Language Expectancy Theory

Closely connected to social norm theories, the Language Expectancy Theory illustrates the positive and negative connotations associated with language used in persuasive messages. Society creates general rules as to what is good, bad, dangerous, safe, and overall, what is relevant. Messaging that does not align with social perceptions can incite attitudinal shifts in the receiver as they possibly misunderstand the message or the intention of the communicator.

Under this model, fear appeals can decrease credibility, trust, and cause anger toward or disbelief in an agency if the tactic is misaligned with social norms and acceptable levels of fear tactics. This theory leads us to believe that it would be best to address rumors, and talk about differences in perception rather than attempting to either scare the public into acting differently or messaging what is factually true despite varying public understanding or agreement.

CONCLUSION

Unfortunately, because fear is an emotional, System 1 response, fear appeals are often used to

communicate threat information. Perhaps we cannot change fear appeals used by mainstream media, but we can change the press releases we feed them and what we communicate on behalf of our agencies. Federal, tribal, state, and local governments are not only tasked with communicating effective messages in order to incite behavior change but also with monitoring media and making attempts to quell rumors that affect agency credibility. For these reasons, application of social psychology and message effects models are vital to the success of risk communication in homeland security. Our agencies are expected to show results and through the application of these models and academic theories, the field of homeland security has the potential to increase public action and build trust; ultimately saving lives, property, time and money.

Each model described in this paper incorporates different aspects of risk communication that are discussed individually in the literature but have yet to be combined into one messaging model. Risk communication intersects with several other social psychological and scientific fields, presenting an opportunity for the sharing and compilation of best practices in order to compile a homeland security-specific model that addresses: social norms, mental models, decision making, trust, transparency, active listening, behavior change, fear control, danger control, reliance on experts, use of target audience as test receivers, and evaluation of communication strategies combined with scientific research within the field of homeland security. Good communication can only strengthen the security of our nation.

Works Cited

Mental Models Approach. Cambridge University Press 2002. Retrieved from: http://books.google.com/books?hl=en&lr=&id=kfM1OZNjeAwC&oi=fnd&pg=PR9&dq=risk+communication+a+mental+models+approach&ots=lCwlAOwaL6&sig=hOpleaAEVt3ske_wkyOuU_OxX1E#v=onepage&q&f=true

Bazerman, Max H., and Don A. Moore. *Judgment in Managerial Decision Making.* Wiley, 7th edition. August 2008.

Burgoon, M., & Miller, G.R. (1985). An expectancy interpretation of language and persuasion. In H. Giles & R. Clair (Eds.) *The social and psychological contexts of language* (pp. 199-229). London: Lawrence Erlbaum Associates.

Cameron, Kenzie A. —A practitioner's guide to persuasion: An overview of 15 selected persuasion theories, models and frameworks.‖ Journal of *Patient Education and Counseling*. 74 (2009) 309-317.

Department of Homeland Security. Citizen Corps Personal Behavior Change Model for Disaster Preparedness. Citizen Preparedness Review: Community Resilience through Civic Responsibility and Self-Reliance. Issue 4. Fall 2006. Retrieved from: http://citizencorps.gov/pdf/citizen_prep_review_issue_4.pdf

McComas, Katherine A. —Defining Moments in Risk Communication Research: 1996-2005.‖ *Journal of Health Communication.* 11:75-91, 2006.

Mileti, Dennis. *Disasters by Design.* Joseph Henry Press. May 1999.

Ruiter, RAC, C Abraham, and G Kok. "Scary warnings and rational precautions: a review of the psychology of fear appeals." *Psychology & Health* 16.6 (2001): 613-630. *CINAHL Plus with Full Text*. EBSCO. Web. 30 May 2010.

Slovic, Paul, Melissa Finucane, Ellen Peters, and Donald G. MacGregor. —Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality.‖ *Risk Analysis*. Vol. 24, No. 2, 2004.

Witte, K. —Fear control and danger control: A test of the extended parallel process model.‖ *Communications Monographs*. 1994. 61(2), 113-134.

Zajonc, R. B. —Feeling and thinking: Preferences need no inferences.‖ *American Psychologist.* 1980. Vol. 35(2), 151–75.