Finalist Essays from the Center for Homeland Defense and Security's Sixth Annual Essay Competition, 2013

Essay Question

What is a dangerous idea you have about homeland security, and why is it dangerous?

Winning Essay

On a Dangerous Idea for Homeland Security
Jeff Dunne, Chief Scientist, Cyber Assessments at Johns Hopkins University Applied Physics Laboratory

Finalist

Homeland Security: Trusting the Public
Erik Archibald, Research Assistant, University of Delaware: Disaster Research Center

About the Competition

The Center for Homeland Defense and Security (CHDS) essay contest, now in its sixth 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: "What is a dangerous idea you have about homeland security, and why is it dangerous?"

Congratulations to this year's winner and finalist. 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 IS A DANGEROUS IDEA YOU HAVE ABOUT HOMELAND SECURITY, AND WHY IS IT DANGEROUS?

Jeff Dunne
Chief Scientist, Cyber Assessments at Johns Hopkins University Applied Physics Laboratory

Whether referring to a simple organism, a person, a society, a country, or any other self-aware construct, the achievement of security is not a desirable outcome. While the pursuit of safety is a fundamental and essential component of the survival instinct, the successful completion of that pursuit is actually detrimental. This paper explores this concept from three perspectives, and concludes with an explanation of why the concept, while valuable in its ability to guide our pursuits, can be dangerous when not handled with care.

As a starting place, let us consider this from an abstracted perspective. For any system having needs, its most fundamental need is survival, and it is this need for survival that drives the pursuit of security (the state of being without threat or danger). Going one step further, one can, given enough pages to fully discuss the matter, provide compelling arguments that the process of striving for security in its various forms and dimensions (including factors such as continued genetic survival through procreation) is the primary driver for all significant actions a system undertakes. The examples presented below illustrate the credibility of this claim. But taking the claim as an assumption for the moment, this conclusion follows: successful achievement of security eliminates the need for action on behalf of the system, resulting in a stagnant system.

Accepting that achieved security is antithetical to growth and development, one might question whether this is actually problematic. In a resource-unconstrained system one can envision (albeit requiring a healthy dose of optimism) a successful ecology based on the "live and let live" principle, an ecology where all systems are essentially self-sufficient, or at least symbiotic. However, our world is not so unconstrained. At least within the confines of the prevailing worldview, the Earth is a very resource-limited system, with the result that the survival, whether immediate or generational, of one system is at the cost of others (or, if one is very optimistic, at the very least at the cost of the security and autonomy of other systems). The net consequence is that a non-evolving system (e.g. one that has stagnated through achievement of security) will eventually find itself in an environment to which it is no longer sufficiently well-suited, and hence no longer secure.

The final conclusion: security, as an achievable end-state, is ultimately self-defeating; while the pursuit of security represents a sensible and useful goal, the attainment of security predisposes one towards vulnerability in the longer run.

As previously caveated, this conclusion is based on the necessary assumption that security is the primary driver for self-aware systems. Since a definitive proof of that statement is not practical, the paper will proceed by presenting two examples that hopefully illustrate its credibility and illustrate the basic concept. The first is business systems.

In business, security can be represented as having assurance of continued operations regardless of the actions of the company or changes in the environment for that company. The pursuit of such conditions are the fundamental drivers for every corporate decision – a business diversifies to ensure resiliency against changing markets, and/or focuses to ensure dominance in specific markets. It attempts to take an active role in forming its environment, to absorb competitors, and so forth. Every one of these actions is taken in the pursuit of corporate "security", and those pursuits lead to the company's improved resilience, greater profitability, etc. In a nutshell, pursuit of security provides many desirable outcomes: growth, stability, resilience, better products, better practices, and so forth.

In contrast, consider the situation where a business achieves security, i.e. where it is no longer at risk, regardless of how the environment changes or what the company does. Such a company has no reason to improve its practices or produce better products. Such actions require the expenditure of "energy" (money in this context) without the promise of a return on investment (ROI), and are therefore unjustifiable. In the language of an earlier paragraph, the system is non-evolving.

The history of the airline industry provides an apropos example to consider. Decades ago major airlines became so firmly established and essential, that improved business models were unnecessary. Customer service was minimal, in part because customer satisfaction was simply irrelevant. People had to fly, and they had no choice but to utilize one of the major airlines to do so.

Had the world been resource-unlimited, e.g. all customers had endless supplies of money, this might have enabled a stable equilibrium. Unfortunately (for the major airlines), this was not the case. Newer companies, sporting newer business models and offering new services, came into being and began to siphon away customers from the major airlines. The big airline giants, having become complacent, soon found that their stagnation made them uncompetitive – the environment had changed around them, they were no longer well-suited for it, and the process of mobilizing for change sometimes took so long that many airlines went out of business. Even now, the surviving, "well-established" giants find themselves struggling to stay in business in the face of more agile companies.

The obvious second example is the biological system, and to facilitate making the point we will consider humans specifically. While it may be personally uncomfortable for some to contemplate that achieving personal security is impossible, it is certainly more readily acknowledged and appreciated. Life experiences have taught us that the world is an unpredictable place, that there is risk in everything we do, and that adoption of a balance in the spectrum of risk acceptance vs. risk avoidance is far healthier than expecting to live at either extreme. Further, there is hopefully no need to expound in any detail regarding the value of pursuing security.

Still, the underlying question is not whether perfect security is achievable, but whether such an achievement is desirable, i.e. in the best interests of a human. Scoping the problem to a single individual, one can toy with the concept of living the perfectly secure life – all needs guaranteed to be met, with only the desire for entertainment or personal enrichment. One could present many arguments for why this might not be as rewarding as it sounds, and why the human psyche will actually generate threat in the absence of external risk. However there can be no concrete, definitive logical argument based on what a human might desire or achieve. Rather, the unavoidable mortality of individual humans suggests that since perfect security is not an option at the individual level anyway, a cross-generational perspective is more valuable to consider.

Examining the idea of achieving security for a group of humans (a family line, a culture, etc.) leads quickly back to a line of reasoning that will differ little, even in terminology, from the first example. Once a group of humans ceases to adapt and evolve, only a very delicately balanced environment with unlimited resources will enable that group to persist indefinitely. In a resource-limited, dynamic environment, competition to survive leads to Darwinian conclusions – only those who are able to evolve will remain competitive for continued survival. And since the presence of any evolving system makes an environment dynamic (for all other systems), evolution becomes a prerequisite for continued survival of all systems in that environment. To summarize, achievement of security creates a dangerous, and ultimately self-defeating, inclination towards stagnation.

Before proceeding to the concluding portion of the paper, it is worth acknowledging that in today's environment, many people's first thought when the term security arises is "cyber security". Why was this not one of the examples used in the preceding paragraphs? The answer is that the premise of this paper and its arguments applies to self-aware systems, and more specifically, systems with needs. While this is a definition in which the homeland of "homeland security" falls, that is not the case for the cyber of "cyber security". In this context, cyber robustness is an aspect of cyber-using systems (e.g. individuals, companies, nations, etc.), a dimension in which to compete with other cyber-utilizing systems. Said differently, there will always be more potent cyber threats, just as there will always be more attack-resilient systems.

At this point, let us restate the idea proposed herein: while the pursuit of security can offer value, the achievement of security is self-defeating. This concept represents both value and danger, and the remainder of the essay will focus on these.

The value in recognizing and understanding this concept comes from its ability to guide our homeland security efforts into greater effectiveness and ROI. Surveying Broad Agency Announcements, Requests for Proposals/Information, and so forth, one sees a disproportionate number that establish metrics of success based on the development of the perfectly secure system or capability. But based on the discussion above, security is not an absolute state, but rather a relative assessment, i.e. the question should not be whether you are secure, but how capable are you relative to your competition. Valuable improvements get overlooked because they cannot promise to deliver the impossible.

Additionally, a poor understanding, or lack, of realistic goals can result in poorly structured research strategies. Underestimating costs is always a concern, but there is a complementary risk from overfunding. When large sums of money are poured into making it secure (whatever that it is) and the effort fails – as it is destined to, since the target is unachievable – the backlash response is to swing in the other direction, substantially underfunding or even eliminating the pursuit entirely. This start-and-stop approach represents one of the most inefficient and ineffective approach to research and development, second only to methods such as "don't try at all" or "wait for a brilliant idea to appear from nowhere".

Recognizing that our goal should be a focus on improvement, rather than achievement, of security, we can realize many benefits. One such gain is having an upfront appreciation that this is a problem that will require a never-ending, sustained effort. Spend sensibly and consistently, rather than solely as knee-jerk reactions to threats of the present that incite public fear.

Another benefit is to motivate investment strategies that emphasize building a scientific base that aims to serve future efforts as much as current engineering solutions. To date, comparatively little emphasis has been placed on understanding security at a fundamental level, and the investments made towards one solution are rarely captured to inform and augment investments made towards another. Like novice software developers who can't be bothered to document their code, we are easily deceived into thinking that this will be the one and final solution that will never be built upon or amended. We also presume that an effort not resulting in an improvement to security is a failure with no redeemable value. If we learn to document and understand our failures alongside our successes, we will greatly increase our effectiveness at improving homeland security.

So where is the danger?

First, while in this paper the nature of the dangerous idea has been carefully phrased to minimize the risk of misunderstanding, this is not typical of casual conversation. A more cavalier expression of the same concept, such as "achieving security is a bad thing," can lead to unfortunate consequences. In the case where the statement is accepted as true, it could easily be (mis)interpreted to mean that we should not be investing in, or otherwise striving for, improved security (homeland or otherwise). Such an attitude would clearly be detrimental (to say the least).

The opposite (i.e. when one does not recognize that security is about continual improvement, not solving a finite, static problem) is similarly dangerous in that it leads to the establishment of "achieved security" as a Boolean metric of success. Not only does setting unrealistic expectations for determining whether an investment is providing an acceptable return lead to inappropriate funding strategies, it is disheartening; that, in and of itself, can result in poorer progress.

Another important factor, related in part to the previous point, is that realism is a core component of human motivation. Most people find it difficult to enthusiastically pursue a goal that they believe to be unachievable. In recognizing the impossibility/undesirability of perfect security as a viable option, there is a danger of sabotaging our own efforts in moving towards that (unachievable) goal efficiently, and limiting the gains that the effort can provide. Alternately stated, active recognition of the fallacy of the goal introduces the risk of forgetting that while the goal itself may represent an undesirable state, the journey towards that state is the important part, and that it offers substantial – one might even say essential – benefits.

This idea is not new, of course. There are numerous philosophies that promote the concept that a destination is valuable only as a motivation for making a journey. However, it is recognized that perhaps the greatest challenge for people, even those who subscribe deeply and thoroughly to such philosophies, is to overcome the instinctive human behavior to fixate on the wrong thing (in this case the destination) despite "knowing better".

Although the concept is dangerous in its susceptibility for misunderstanding and the ease with which superficial consideration can lead to poor decisions and planning, it is the opinion of the author that the risk is worthwhile if recognition of the concept results in more realistic expectations, better pursuit strategies, and a more informed approach to gauging a sensible balance between security and personal freedom.

HOMELAND SECURITY: TRUSTING THE PUBLIC

Erik Archibald
Research Assistant, University of Delaware: Disaster Research Center

On the morning of September 11th 2001, four commercial airliners were hijacked and used like missiles to attack the World Trade Center and the Pentagon. Such a devastating terrorist attack on American soil was unprecedented and largely unforeseen by the American public and government. Although in the summer of 2001, the Whitehouse, CIA, FBI, DoD and even the FAA were aware of a high profile threat from Al Qaeda, there was not enough information for any government agency to prevent the attacks. In the minutes between the first reports of hijacking at about 8:25 AM and the last airliner crash at 10:03, no government agency was able to take action to stop the attacks. This short time period was, however, just long enough for the passengers on United Airlines Flight 93 to perceive the suicide hijacking threat, and act on that information to disrupt the terrorists' plot. Their heroic actions likely spared the U.S. Capitol Building or Whitehouse from destruction[1]. Although the government wasn't well prepared to stop such an attack, the randomly assembled group of complete strangers with little counter-terrorism experience flying on board Flight 93 had both the motivation and capacity to thwart a terrorist plot.

A dangerous idea for homeland security would be to actually enable, empower, encourage and expect the public to be the principal actor in protecting our nation from terrorism and disaster. This idea is dangerous because many see homeland security as largely a government function and don't trust the public to fulfill this role. Despite this danger, there are many advantages to empowering the public to do the work of homeland security.

THE DANGERS OF RELYING ON THE PUBLIC

Trusting the public to play a key role in homeland security could be very dangerous. For the most part homeland security is currently done by trained professionals with decades of experience and structured organizations to manage the work. Expecting the public to be the principal player in homeland security would be a large shift and could be dangerous for a number of reasons. The public could hinder the work of professionals, and may provide inconsistent or poor quality work.

[1] 9/11 Commission Report

IMPEDING THE WORK

One danger of allowing the public into the intimate details of homeland security is the possibility of them getting in the way and impeding the work of professionals in the field. For firefighters or EMT's responding to car accidents or house fires it can be frustrating to have to deal with people who want to help, but have little emergency expertise to contribute. Ironically, these same people getting in the way are also those who provide the first and most critical care to a patient. In intelligence, law enforcement and other areas, information is classified and restricted from the public to prevent the leak of sensitive information to potential adversaries. While well-meaning citizens have appealed to internet service providers to take down numerous websites that recruit and inform terrorists, members of the intelligence community see this as a nuisance that only makes it harder for professionals to gather intelligence on terrorist activity[2]. Having the public intimately involved in homeland security can impede the work of professionals.

INCONSISTENT EXPECTATIONS

Expecting the public to do much of the work in homeland security could be dangerous because nobody would really know exactly what the public would do. Unlike government organizations which are governed by law, policy and procedures, the public isn't bound to act in one way or another. This could lead to very inconsistent performance. A greater reliance on the public may leave unanticipated gaps in the service provided. While in some communities, the public may excel at performing homeland security tasks, others may provide unfair, poor, inconsistent or even unlawful service, if any at all.

THE DANGERS OF NOT TRUSTING THE PUBLIC

While it may be dangerous to trust the public in homeland security, the failure to trust the public to play a large role in homeland security is even more dangerous. The task of homeland security is far too big for governments to face alone. Not only does homeland security require more resources than government can offer, government organization is in many cases not well-suited to address the many challenges at hand.

Homeland security is too large of a challenge to address without fully accepting the public as a key player. In current homeland security practice, we try to manage or control things that in many cases

[2] Fox News. *Cyber Vigilantes Track Extremist Web Sites, Intelligence Experts Balk at Effort* http://www.foxnews.com/story/0,2933,340613,00.html

are entirely impossible to control. We cannot expect a few thousand government agents to maintain complete control over 6000 miles of land border and 95,000 miles of sea border, stopping all illegal entries, finding every weapon and enforcing hundreds of laws regarding international trade. In a disaster where millions of people are affected and have diverse needs, we can't expect any level of government or even all of them combined to manage, control or lead an effective response to meet everyone's needs. Homeland security is a big task. We all know that government cannot and does not expect to do it alone. Beyond not being able to do it alone, government can't control, organize, lead or even coordinate it all.

Traditional bureaucratic government is poorly suited to meet the challenges of homeland security[3]. Our nation faces asymmetric threats. Although in many ways a large well-organized government is well setup to face these threats, in other ways a large bureaucratic government makes it more difficult for us to rapidly adapt to changing threats and dynamic situations.

BENEFITS OF TRUSTING THE PUBLIC

There are many benefits to enabling and empowering the public to become the key player in homeland security. The public is readily available and can be found everywhere. They offer skilled and unskilled labor at very little cost. In many cases they can organize and adapt more rapidly than government. An involved public also extends the reach of homeland security efforts into realms that government may not penetrate.

EVERYWHERE

A key benefit of relying on the public is that they are everywhere. In many cases when homeland security professionals are unable identify and stop a terrorist plot before it happens, ordinary people step in and respond. In 2010 a car bombing attempt in Times Square was noticed by street vendors which reported the incident to an NYPD patrolman. On Christmas day 2009, Umar Farouk Abdulmutallab attempted to bomb his flight by igniting explosives sewn into his underwear. He was apprehended by a Dutch movie director and flight attendants that restrained the bomber and put out the fire. Despite intelligence about Abdulmutallab's involvement with extremists, he was able to obtain a valid U.S. visa and board the flight which he would later bomb[4]. Although the federal government failed to prevent the attack, ordinary people were able to respond to it in the moment.

[3] Kamarck, Elaine. *Applying 21st Century Government to the Challenge of Homeland Security* in The Forum Vol 1 2002.

[4] U.S. Senate Report 111-199. *Attempted Terrorist Attack on Northwest Airlines Flight 253*

Skilled and Affordable

Collectively the public has every skill that could ever be needed. When given sufficient motivation and the opportunity to serve, the public can contribute many specialized skills at practically no cost to the taxpayer.

Online communities in response to Hurricane Sandy provided a great deal of free skilled labor. FEMA relied on a crowd-sourced damage assessment, in which aerial imagery was given damage classifications by regular people looking at the images on a web page[5]. Online communities of software developers from all across the U.S, as well as in Ireland and New Zealand got together to develop software to aid in Hurricane Sandy response. They developed software for FEMA, the Red Cross and the general community to monitor hospital status, identify operating gas stations and help people find temporary housing and carpooling arrangements[6]. One group even put together an IT (information technology) help desk to help affected businesses recover by providing free help with websites, servers and networking[7].

A more dangerous way in which members of the public contribute their skills for free is through cyber vigilantism. Cyber vigilantes take down websites, flag terrorist material for removal on sites like YouTube, find and report terrorists online, and collect and share intelligence. These activities have the potential to do both great harm and great good in furthering counter-terrorism efforts[8]. While some argue that federal officials are already so busy tracking terrorists online that they do not have any time to mess with members of the public who may interfere, others argue that federal officials are so busy following terrorists online that involvement by the public could only help. Either way, these citizens' actions have resulted in the shutting down of dozens of sites that recruit terrorists[9] and have resulted in a number of arrests[10]. Many members of the public are both willing and able to further the mission of homeland security.

[5] FEMA. *FCO Thanks people who have been helping*. http://www.fema.gov/medialibrary/media_records/10369

[6] Crisis Commons Wiki. http://wiki.crisiscommons.org/wiki/Hurricane_Sandy_2012

[7] Operation Sandy Support. http://operationsandysupport.tumblr.com/

[8] The Counter Terrorist. *Cyber vigilantes: Citizen hackers go to war against terrorists* http://www.homeland1.com/domestic-international-terrorism/articles/873689-Cyber-vigilantes-Citizen-hackers-go-to-war-against-terrorists/

[9] Washintgon Times. *Blogs Target Jihadis Online* http://www.washingtontimes.com/news/2007/oct/10/blogs-target-jihadis-online/?page=1

[10] Shannen Rossmilller. *My Cyber Counter- jihad.* http://www.meforum.org/1711/my-cyber-counter-jihad

FLEXIBILITY IN ORGANIZING

Another benefit of public involvement is their incredible flexibility in organizing. After a disaster, many people organize themselves to respond. Without any pre-existing plans, command structure or government direction whatsoever, thousands of volunteers decided to contribute their skills to help after Hurricane Sandy. While many volunteers were deployed by government or non-profits, many others started their own relief operations. They grabbed their gas grills, loaded up trucks full of donated materials or grabbed their gloves and tools and headed into the disaster zone. In person and on the internet they began to build situational awareness of what the needs were and adjusted accordingly. Although, these efforts may not be as efficient as a well-organized effort, their effort is effective in that collectively the needs are better met even though resources may not be used in the most efficient manner possible.

An impressive example of rapid organizing and adaptation to change is the Occupy Sandy relief effort. Although the Occupy movement previously played no role in disaster relief, Occupy Sandy quickly became one of the largest relief operations. Within a few days Occupy Sandy had a command post, two warehouses, a dozen distribution points and hundreds of volunteers going door to door finding out needs and then organizing donated labor, supplies and food to meet those needs. Despite some chaos, rapid growth and change, Occupy Sandy volunteers signed up online, received brief orientations and training. Occupy Sandy rapidly built up communications capability via its website, Twitter, Facebook, email lists, a text message loop and regular phone calls[11]. Occupy Sandy is an excellent example of how ordinary citizens can rapidly organize an effort to respond to disaster.

EXTENDED REACH

An involved and empowered public can extend the reach of homeland security. The internet has made it easier than ever for citizens to participate in homeland security. Thanks to the public, during and after a disaster, Twitter feeds are full of brief text descriptions, pictures and sometimes even links to video showing what has happened. After a disaster, Facebook groups form for community members to share information on how to get help and how to help others. These groups

[11] Field work by Author in the Rockaways, Brooklyn and Staten Island after Hurricane Sandy.
See also November 9, 2012 New York Times Article. *Occupy Sandy: A Movement Moves to Relief*
http://www.nytimes.com/2012/11/11/nyregion/where-fema-fell-short-occupy-sandy-was-there.html?pagewanted=2&_r=1&adxnnl=1&smid=tw-nytmetro&partner=socialflow&adxnnlx=1360934433-2q8dBchZ0yzWR4ArtieuIw

can be incredibly powerful. A Facebook site put together by citizens of Joplin after the Tornado has more than 171,000 likes. This is more than the city of Joplin, the local newspaper, the state of Missouri and FEMA combined[12]. After Hurricane Sandy, dozens and dozens of Facebook sites and other websites were active providing information, and coordinating volunteers and donations[13]. For law enforcement, Philadelphia has recently begun using the social networking site Pinterest to post photos of wanted persons. In one month, they posted 200 videos of wanted persons and made 112 arrests[14]. Internet information gathering, coordination and collaboration can greatly increase the reach of homeland security.

TRUSTING THE PUBLIC

Empowering the public to play the principal role in homeland security is dangerous. It means the role of government will need to change. There will be gaps. There will be mistakes. There will be confusion. No one will be able to completely control or coordinate it. Regardless, the public's role in homeland security is indispensable. The public is everywhere, they are talented, they are dedicated. They are willing to work just to be able to help protect themselves and their neighbors. They can rapidly organize and adjust to dynamic environments. They have the potential to greatly increase the reach of homeland security.

Governments will always play an important role. Beyond doing that which cannot be done by the public, they need to partner with the public and empower them to play their important role. A good example of this occurred during the 2013 winter storm Nemo. The mayor of Boston set the direction for the public by using Twitter to encourage people to help their elderly and disabled neighbors[15]. Some responded by individually helping their neighbors. Others formed groups. Others used websites to map aid requests so that volunteers could find those who needed help nearby[16]. In less than 200 characters of text, the mayor of Boston got more done for the elderly than any special needs emergency plan could have ever accomplished. This is the power of the public.

[12] See https://www.facebook.com/joplinmo ; https://www.facebook.com/mogov ; https://www.facebook.com/CityofJoplin ; https://www.facebook.com/FEMA

[13] See https://docs.google.com/spreadsheet/ccc?key=0AlVkJ9AAruYBdF93SllVN2UxT1Zxejl6Z2ZubGhXSFE#gid=0 for a listing of Facebook sites, web sites and other resources developed by the internet community for Sandy response.

[14] Knell, Noelle. *Catching Criminals on Pinterest.* http://www.govtech.com/public-safety/Catching-Criminals-on-Pinterest.html

[15] Stephens, Kim. *Social Media and #NEMO in Massachusetts: Some observations* http://idisaster.wordpress.com/2013/02/11/social-media-and-nemo-in-massachusetts-some-observations/

[16] http://neighborsforneighbors.org/page/snowcrew

For creative and innovative governments there are countless ways in which government can empower the public to participate in homeland security.

At 10:03 AM 9/11/2001, Flight 93 crashed into a field. Without access to intelligence or thousands of hours training, without weapons, tools or massive amounts of data, an ordinary group of passengers on Flight 93 were successful in thwarting a major terrorist attack. This is the power of the American people. How dangerous could it be?