The Power of “the Few”:
A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment

Rodrigo Nieto-Gómez

To a greater degree than at any point in history, individuals and small groups—from nongovernmental organizations (NGOs) on the one hand to criminal networks and terrorist organizations on the other—have the ability to engage the world with far-reaching effects, including those that are disruptive and destructive.


ABSTRACT
This article argues for a new organizational approach to homeland security, designed to confront the challenges of a highly disrupted environment in a more efficient way. Initially, it explains how the accelerating pace of innovation creates a set of homeland security challenges that empower small groups or individuals – “the few” – in new and unpredictable ways. Next, it demonstrates why the current organizational model for homeland security is systemically insufficient to respond to this permanently disrupted environment, despite the best efforts of its members. This is done by dividing the homeland security duties into two distinct missions: an incremental or “systemic mission” and a disruptive or “future shock mission.” The current institutional model is seemingly well adapted to respond to the needs of the first mission but ineffective to address the second. Lastly, the article proposes a new homeland security institutional model, better adapted to confront the negative effects of disruption by fostering and harnessing the positive ones. This is accomplished by adapting Alvin Toffler’s concept of “adhocracy” to homeland security’s needs and using DARPA as an example of a successful “adhocratic” and disruptive security and defense institution.

INTRODUCTION
The task of defining a homeland security environment is tricky. Framing it seems like an invitation to oversimplify its nature as a series of elements that can be fitted into a tightly packaged description that might look elegant, but also provides us with a false sense of linear order and predictability for what it is in reality an interactive, complex, and evolving web of forces, constraints, incentives, and conditions.

This article will first describe how the current pace of technological progress perpetuates the chaotic nature of the homeland security environment and maintains it in a permanent state of disruption. This has given birth to a new phenomenon that I call “the power of the few,” where technology has lowered the barriers to entry for disruption, both positive and negative, thus creating the need for a new kind of security strategy to prevent innovation and freedom being turned against the legitimate users of social and physical infrastructure. I conclude with an exploration of the limits of the current homeland security institutional framework to adapt to this rapidly evolving and unpredictable environment, and propose a new strategic approach to homeland security, based on the different natures of incremental and disruptive threats, to counter more effectively the negative effect of the power of the few.

Whereas the normal approach to describing an environment for strategic purposes is to think of it as a static abstraction of reality, akin to the chessboard where players distribute their pieces and make their moves (think of a battle map, as shown in Figure 1), a social environment for public policy is not a snapshot frozen in time, but a mutating context in which people operate and interact with each other and with
the natural and man-made structures that surround them, and each interaction morphs a little bit the state of the system. It is more an ecosystem than a photograph.

Figure 1. Cartographic representation of Operation Overlord strategic plan.¹

As such, the homeland security environment should be understood as a chaotic system where long term planning is very difficult and forecasting is in reality impossible. As Levy explains it, “chaos systems do not reach a stable equilibrium; indeed, they can never pass through the same exact state more than once.” Therefore, “we cannot learn too much about the future by studying the past: if history is the sum of complex and nonlinear interactions among people and nations, then history does not repeat itself.”² Trend analysis, the basis of most forecasting based planning, is not a useful tool to plan and prepare against future disruptive threats because that previously mentioned metaphorical chessboard will not have the same number of squares twice, and the pieces constantly change the way they move.³

Secretary of Defense Robert Gates described the limitations of forecasting for defense, strategy, and war:

We can’t know with absolute certainty what the future of warfare will hold but we do know it will be exceedingly complex, unpredictable, and – as they say in the staff colleges – “unstructured.” ... And I must tell you, when it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right.⁴

HERACLITUS AND ASIMOV WERE RIGHT

In Cratylus, Plato imagines a dialogue where Heraclitus expresses: “all things are in motion and nothing at rest...[it is] like the stream of a river ... that you cannot go into the same water twice.”⁵ Isaac Asimov, the science fiction writer, updated the quote: “It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any
longer without taking into account not only the world as it is, but the world as it will be.”

That is why trying to describe the current state of the homeland security environment is a flawed approach to developing a strategy, mainly because the current state is just an instant in the evolution of this complex and randomized system. Instead, I will focus on demonstrating how scientific and technological progress (two of the main motivational forces for societal transformations) have accelerated the pace of this evolution, reducing in the process the “shelf life” of some of the security paradigms and doctrines that condition the reactions of our institutions in the homeland security environment. This accelerated pace implies a change of scale that empowers small groups.

Over the last century, radical technological changes have disrupted the human environment in profound and permanent ways. In this very short amount of time, a 100-year-old person alive in 2011 would have witnessed the arrival of the power grid, the telephone grid, the mass produced automobile and the interstate highway system, radio broadcasting, television, the cell phone network (first transmitting only voice and then voice and data), the computer and, of course, the Internet. None of these technologies that shape and sustain the human ecosystem today were generally available the day he was born.

In those same 100 years, new techniques and construction materials have reshaped our urban environment. Reinforced concrete and the steel frame allowed us to build higher, giving birth to the modern skyscraper and opening the door to a new level of urban concentration. Paradoxically, stronger and more flexible infrastructures (dams, pipelines, power plants, the grid, tunnels, bridges, highways, and airports) gave us the capacity to locate people and resources over much greater distances than before, enabling a technological urban sprawl.

This contemporary urban environment is dependent on technological infrastructure operating unceasingly. As Weisman’s provocative narrative describes, it would take less than a week without functioning infrastructure for places like New York City to start a process of rapid decay.  

Because of innovations in transportation and information technologies, the rapport of the individual with space also suffered multiple disruptions and our environment has “shrunk.” Low transportation costs made possible unrestricted and rapid travel to almost anywhere in the world for less than one thousand dollars using the global civilian aviation network, and provided the ability to ship any product anywhere for just a few hundred dollars. This modified our relation with time, as spatial processes that used to take months – like sending a shipment across the world, traveling, or sending a letter – can now be accomplished in days for what used to take months, and instantly for what it used to take days. The grace period that societies used to enjoy to prepare for a disruption coming from overseas no longer exists, or at least it has been greatly reduced. Disruptions not only can travel far and cheap, they can also travel fast.

Lastly, our relationship with the working and productive environment also endured important changes that affect the way we deal with technological innovation. In the last 100 years high tech societies have become postindustrial, and knowledge creation has replaced manufacturing as the main added value for economic growth, with consequences for every production sector.

The food industry operates today in an environment where, thanks to agrotechnology, produce is abundant and easily transported from its source to the consumer. In this high-tech environment, less than 4 percent of the population of any given developed country can grow enough food to feed all its inhabitants and still sell an “exportable surplus.” Furthermore, the primary sector is being disrupted by the recently gained knowledge of how genetics work and how genes can be converted into information and manipulated digitally, freeing genetic scientists from the physical limits of Mendelian inheritance.

Regarding the secondary sector, affordable energy, robotics, and outsourced cheap labor made possible by communication and transportation technologies have made dull and repetitive manufacturing tasks unprofitable and undesirable inside the labor environments of most high-income nations, forcing their citizens into more information
driven endeavors. In fact, this labor environment has seen “a huge increase in the number of people paid to think or talk, rather than produce or transport objects.” That is, people are being paid for their capacity to produce and manage information (granted, not all of it creative) and not for their muscles, thus multiplying as a result the amount of knowledge that can be recombined and therefore the potential for disruption (voluntary or involuntary) of the environment in cumulative way.

This takes us to the two main patterns that govern our innovation and security environment and are to blame for the emergence of the phenomenon of the “power of the few.”

The first one has to do with the cumulative, combinatorial, evolving and unpredictable behavior of the system: waves of new technologies lay the foundations for the next technologies with cross-pollination during the same wave. Some new technologies, like the printing press and the combustion engine, have ripple disruptive effects across many domains, and affect security in many ways. Others are just incremental upgrades from previous technologies and security strategies do not need to be altered. Nonetheless, all new technologies inherit some elements from previous generations of scientific discovery and technological advances. While this process can be traced back in time, in what Bryan Arthur denominates “Combinatorial evolution,” he also concluded:

[Modern technology is now] becoming an open language for the creation of structures and functions in the economy... shifting from technologies that produced fixed physical outputs to technologies whose main character is that they can be combined and configured endlessly for fresh purposes. Technology, once a means of production, is becoming a chemistry.”

So, the first pattern exhibited by the system is that technological environments evolve in a combinatorial way, and modern technology has made recombination, including convergence, simpler. For example, when material products are transformed into binary data, they can be manipulated with little to no associated manufacturing cost. As Chris Anderson points out, “once something becomes software, it inevitably becomes free – in cost, certainly, and often in price.” Products that used to be “things” are today binary code: music CDs or LPs, VHS tapes or DVDs, typewriters, solitaire decks, blueprints, calculators, libraries full of books, office files, medical test results, genetic strings, to cite just a few. While this convergence might seem today logical and understandable, just a few years ago (before the computer era) it would have been difficult to find something linking medical research and film distribution.

The second key pattern derivates from the first one. As part of this evolution and the iterative learning process that comes with it, technology gets cheaper and better with time incrementally. Any early adopter of technology has witnessed this phenomenon when, after a few generations, his or her first generation model has become an obsolete object that cost twice as much as the new model. This kind of innovation was baptized “sustaining” by Clayton Christensen. In his words, sustaining technologies “improve the performance of established products.” But he also recognized that sometimes “disruptive” technologies emerge. They bring to “a market [I would say to the security environment] a very different value proposition than had been available previously.”

So, for the purposes of this article, the second important environmental pattern is that innovation brings change to the system either incrementally or disruptively. Incremental improvements of existing mainstream technologies makes them better and cheaper, but disruptive innovation can and often does change the environment in unexpected ways, disrupting (hence the name) the rules that governed what seemed, for a while, a stable ecosystem.

Disruptive technologies are the ones that normally modify the physical qualities of our environment and more importantly, the fabric of our technologically dependent civilization. For example, the combustion engine not only replaced the horse as the main human means of transportation, it also completely disrupted the way humans interact with their urban space, making modern cities and suburban sprawl possible; this created new conditions and constraints.
for spatial planning. It also created new social vulnerabilities and risks, as the thousands of road fatalities per year demonstrate, catapulting accidents – in less than a century – to the fifth leading cause of death in the United States and creating the need for a highway safety and security strategy.\textsuperscript{16}

Technological innovation is a natural consequence of scientific progress. Every time a new phenomenon is understood or, to use Brian Arthur’s words, every time a phenomenon or effect is “harnessed” by science, it can be exploited by technology.\textsuperscript{17} Then, market forces and human behavior normally determine how and if these new technologies will be assimilated and become a permanent part of the environment.\textsuperscript{18}

Each new technology that we adopt creates new structural vulnerabilities. As Ted Lewis points out “highly technological societies are vulnerable because they depend heavily on technology.”\textsuperscript{19} The more technology we use, the more potential vulnerabilities there are. Because technology now has such a high level of combinatorial complexity, it can safely be said that the environment has reached a state where the periods of stability between disruptions are short lived (certainly shorter than before), and we should assume that disruption is the permanent default state.

You cannot go to the same water twice, and when the water reaches the ocean, the shape of its breaking waves cannot be predicted. Change is indeed the main factor of society today. Therefore, the current mutating environment encourages disruptive participation of small groups of new actors that, until recently, had not enough resources to achieve disruption on a global scale. Because of the two previously described environmental patterns (the combinatorial evolution of the technological environment and the intrinsic characteristics of “sustaining” and “disruptive” technologies), the scale has been altered to favor the small groups I refer to as “the few,” and away from big organizations or governments that used to hold a monopoly on system based disruption.

**THE POWER OF THE FEW:**
**A 2001 ‘CELL’ HAS THE SIZE OF A 1941 EMPIRE**

On September 11, 2001, “a few” hijackers were able to bring to a halt the entire nation, cripple the economy, place continuity of government at risk and inflict more than 3000 casualties. The only other occasion when the United States suffered comparable loses from a single attack was during Pearl Harbor, when the combined fleet of six carrier battle groups (the Kido Butai) backed by the full power of the Japanese Empire was deployed to accomplish a similar result.

In 2001, a cell of nineteen hijackers did what only a powerful empire could do in 1941.

How is it possible that a twenty-first century cell has been empowered to provoke the same kind of damage as a twentieth century empire?

The more technologies we integrate incrementally into our society’s environment, the more options or choices for recombination are created, and the more unforeseeable vulnerabilities appear. New technologies have commoditized certain key resources needed to affect the environment on a global scale. In addition, the expensive physical infrastructure that was formerly required to do this has often been replaced by technologies that can be modified and recombined without heavy machinery and big factories.

The *Quadrennial Defense Review* of 2010 explicitly recognized this as one of the key sources for uncertainty in the current security ecosystem:

Globalization has transformed the process of technological innovation while lowering entry barriers for a wider range of actors to acquire advanced technologies. As technological innovation and global information flows accelerate, non-state actors [*the few*] will continue to gain influence and capabilities that, during the past century, remained largely the purview of states.\textsuperscript{20}

It is no longer true that technological innovation requires a heavy investment to manipulate nature and produce a result capable of having an impact in the real world,
as when most technology represented a tangible single-purpose achievement, designed to obtain a specific desired effect. In the past, the pace of disruption was limited by the constraints of the physical world and as such, disruption moved more slowly and was more expensive than it is now. Today, technology is cheaper to create, easier to recombine, and more integrated in our social environment; because of this, the barriers to entry for achieving world wide disruption have been reduced.

The price of the transistor, backbone of the current computing paradigm and essential to recombining technology, has shrunk exponentially since the 1960s, and computing power has become accessible to everybody for many purposes. As a consequence, digital technology has invaded our environment, replacing in many instances the single purpose “moving parts” that existed before. The digital world serves as a common denominator for an enormous number of social and natural phenomena and directly affects the analog (i.e. the “real”) world: anything that can be transformed into binary data can be processed digitally and recombined with other seemingly unrelated phenomena, all for a marginal cost that quickly approaches zero.

We have assimilated into our innovation landscape some of the positive consequences of this new phenomenon. Nowadays, some independent blogs have a readership as large (or larger) than established newspapers with more editorial influence and without the need for expensive presses or distribution channels. Small groups of entrepreneurs were capable of creating “garage startups” that became big multibillion household names like Apple, Microsoft or Google, mainly selling a programmable idea without the initial requirement of large industrial capacity. The original capital needed to jumpstart these companies was in the hundreds of thousands rather than millions of dollars.

Grassroots movements of loosely interconnected individuals (at the left and right of the political spectrum) have been emerging around the world, using Web 2.0 tools to transform political landscapes without the need for cumbersome party bureaucracies, but also with new vulnerabilities hardwired into their structure because of their need to communicate online.

Aggregators like Wikipedia have started to take advantage of the fragmented knowledge and the free unstructured time of millions of individuals, who are willing to donate this time “just for fun,” capitalizing on what Clay Shirky calls an enormous and yet unexploited cognitive surplus. This effort has created a source of information many times bigger than any physical library, accessible from anywhere where there is an Internet connection. This dematerialized knowledge distribution is leveling the information field, independently of how far people are from the cultural centers. It might be true that Wikipedia is the result of the work of many thousands of volunteers working together, but thanks to aggregation and crowd sourcing technology, this is done at the individual level (the scale of the few) replacing big centralized teams.

As all the previous examples demonstrate, global consequences for the actions of small groups of individuals have been commoditized to the extreme. There is one last example that is more dramatic than any other: Thanks to computer modeling, geo-engineering projects to alter weather patterns are now within reach of wealthy individuals like former Microsoft CEO William Gates. In 2008 (well before Gates announced that he had any interest in funding this kind of projects) David Victor wrote “a lone Greenfinger, self-appointed protector of the planet and working with a small fraction of Gates bank account, could force a lot of geo-engineering on his own. Bond films of the future might struggle with the dilemma of unilateral planetary engineering.”

Current technologies make it possible for small groups of individuals (“the few” or “the one”) to alter Earth’s weather patterns. This is the degree of change in the scale of disruption: one person, financing a “few”, can change the planet, and not only in a metaphorical way. In less than fifty years, individual disruption potential has reached a global scale.

In the 1970s, Alvin Toffler coined the term “future shock” to describe the effects of rapid and accelerating changes in society. In his words,
The rate of change has implications quite apart from, and sometimes more important than, the directions of change. No attempt to understand adaptivity can succeed until this fact is grasped. Any attempt to define the “content” of change must include the consequences of pace itself as part of that content.\textsuperscript{28}

In this rapidly changing environment, where consecutive waves of disruptive technologies are reshaping society faster than it can adapt to the last wave, the small and unstructured “few” are capable of adapting to the pace of change faster than vertical organizations or big governments. As this is a tool-based phenomenon, and tools have no morals or ethics, the “power of the few” can be moral or immoral, legal or illegal.

Without the proper countermeasures, small groups (i.e., terrorist cells, gangs or cartels) or even just lone individuals (e.g., skilled hackers), have a new capacity to inflict damage, fear, and death due to potential access to the same tools that also empower positive behavior and sustain our technologically dependent environment.

The implications of this are fundamental for homeland security’s strategic culture. New technologies, especially disruptive technologies, come with new recombining potential. Because “the few” have better adaptivity than “the many,” small groups can take advantage of unforeseen consequences of the new altered environment more rapidly than authorities can identify a new potential threat and react to it. Convergence of different technologies makes this a multi-layered vulnerability, beyond just information technology risks. For example: human beings outfitted with Life Critical Implantable Medical Devices, (e.g., pacemakers, defibrillators or neurostimulators) have potentially become “hackable” targets. Most of the new versions of these lifesaving devices are activated and deactivated via wireless protocols and “the lack of authentication and integrity mechanisms put patients at risk from attack by anyone with a transmitter.”\textsuperscript{29} Without the proper countermeasure, “the few” might conceivably be empowered to literally stop a heart or a mind by just thinking about it (and programming the proper code).

The permanently disrupted environment cannot and should not be reversed, as its positive effects far outweigh its negative implications. In those places where, in the last 200 years, science and technology have become permanent fixtures of the social landscape, quality of life and security are greater than ever. As Indur Goklany explains in his thoroughly researched book, meaningful indicators like hunger, infant mortality, life expectancy, education, political rights and the UN “human development index” are all positively affected by the presence of “unparalleled technological change, which has transformed the world more in the past two centuries than all the other events put together since the beginning of agriculture 10 millennia ago.” He then points out: “Economic growth and technological change have redefined the role of women and children, restructured the workplace, undermined age-old arrangements of caste and class, expanded the middle class, and developed new institutions and organizations.”\textsuperscript{30}

A policy that would try to stop innovation and progress in the name of security would also be immoral, as it would do more harm than good by denying solutions to some of our most pressing problems. It would also would be Orwellian, as it would transform the creativity and imagination of innovators into “thoughtcrimes” punishable by law. The suppression of technology has rarely if ever been proved to be an effective strategy.\textsuperscript{31} Instead, we need a security strategy designed to protect the safety of “the many” from this recently acquired power of “the few,” while at the same time preserving the technological tools needed to unleash innovation and entrepreneurial creativity.

A high-tech environment is also a target-rich environment, where society’s infrastructure is not only vulnerable to sabotage – it can even be “illicitly appropriated,”\textsuperscript{32} by clandestine actors, and turned against its legitimate users. Even the consequences of natural disasters are worse today because of our social dependency on technological infrastructure in dense population centers.\textsuperscript{33} As Mitchell and Townsend observe:
By bringing down the networks it depends upon, a city can be killed. Those networks can also be hijacked and turned against their creators delivering destruction by appropriating the very transfer and distribution capability that motivated their construction … for an attacker it can be a better strategy to exploit, rather than destroy, an enemy’s networks. If access to large-scale network can be gained, it eliminates the need to expend a lot of effort and energy to get to them. It isn’t even necessary to possess comparable forces. Violence and destruction can be delivered with modest means but pinpoint accuracy, by infiltrating or hijacking those networks.\(^{34}\)

Furthermore, complex networked environments like the ones previously described tend to self-organize critically, injecting a degree of randomness into the security landscape in which, as Lewis points out, catastrophe is hard to avoid: “A small (random) perturbation in these systems can trip a major collapse, unexpectedly, dramatically, and resounding. Because the cause is not obvious (until after the fact), and it is often a very minor perturbation, the collapse comes as a shock.”\(^{35}\)

On 9/11, the illicit appropriation of the civilian aviation network was catastrophically recombined with the steel frame of the skyscrapers in a very disruptive way, to circumvent the security systems of the continental United States. Basically, on that day, the United States of America was hacked by a terrorist cell.

While homeland security has been redefining the role of the state in the fight against asymmetrical attacks, the current strategy has structural limitations in its capacity to deal with “out of the box” vulnerabilities created by our dependence on new technologies and the accelerated pace of technological change. A new strategy capable of taking advantage of this disrupted environment is urgently needed for our era, as the acceleration changes in new technologies – like bio or nanotechnology, robotics and geo-engineering – means the clandestine “few” can find new possibilities every day to appropriate more systems, recombining them in unforeseeable ways.

No traditional, slow reacting bureaucracy is agile enough to respond to this challenge, and the current homeland security institutional model is no exception. Therefore, I argue here that a new organizational change to America’s homeland security institutions is needed to prepare them to be proactive actors in this disrupted high-tech environment.

**The Limits of Current Homeland Security’s Adaptability to Disruption**

How can a traditional security bureaucracy react to this permanently disrupted environment of innovation and fast paced technological evolution? How can a big enterprise made of bureaucratic institutions composed in their turn of hundreds of thousands of individuals, respond to the new vulnerabilities and threats posed by disruptive multipurpose technologies that raise, recombine and fall in cycles measured in months and not years, empowering the adaptable few in unexpected ways?

The answer is that it simply cannot.

To understand why and what choices are available to defend society’s freedoms in this innovative but unstable landscape, it is essential to consider two key determinants regarding the current nature of the threat and how homeland security institutions are expected to confront this threat with a two-pronged approach.

The first essential determinant is that while terrorism should be a big part of any current asymmetrical threat assessment – if only because it is the tactic of choice not just of the weak, but also of the clandestine few (while they are more adaptable than the many, they are not always weaker) – the narrow framework of terrorist conduct does not suffice to describe the homeland security threat posed by the few. Most institutional definitions of terrorism concur that one of the main elements of any terrorist’s conduct is the motivation behind the calculated use of violence.\(^{36}\) Whether this motivation is political, religious, or ideological, the terrorist act has to be oriented to modify the conduct or policy of a government. Yet, in a permanently disrupted environment, what defines the threat posed by the few has less to
The new vulnerabilities of this high tech society make motivation irrelevant. Whether a critical infrastructure is sabotaged or illicitly appropriated to pursue a political or religious agenda, to look for personal gain, to just prove that it can be hacked, or even by accident, the catastrophic consequences for “the many” are the same.

In that sense, homeland security’s response to the power of “the few” has to shift its focus beyond motivation to the means. To phrase it differently, not all homeland security threats will be terrorist attacks per se (i.e. politically, religiously or ideologically motivated acts designed to affect the government’s policies), nor will all homeland security adversaries will be traditional terrorists. Nevertheless, understanding how a technology can be sabotaged, penetrated, or illicitly appropriated to harm society’s interests can be achieved independently of the motivations of the adversarial actor, and a “homeland security response” can be preemptively deployed to address this technological risk.

Without question, confronting the underlying causes which incite a particular group of “the few” to try to do harm to “the many” must be an important and permanent objective of the entire nation and not just of the homeland security enterprise. These causes can be diverse and are often beyond the reach of any security policy. Issues like international Islamist radicalization, domestic racism and xenophobia, organized crime, radical rejection of the federal authority, bullying and social rejection in American schools and colleges, to name just a few, are all social problems for which a solution has to be actively pursued. However, a security and defense policy that would try to address all underlying causes would be diluted in its diversity and faulty in its means, since these and other asymmetrical sources of conflict, almost with the only exception of international state sponsored terrorism, are not at the outset a security or defense problem, but a social one. Consequently, responding to these sources of conflict is a mission for a nation, not for a security strategy.

The second determinant is that we demand from homeland security institutions (composed of more than just the Department of Homeland Security) a two-pronged approach, shaped by two seemingly opposing missions. On the one hand, these agencies are supposed to manage an organizational system of systems using standardized procedures and best practices to prevent known kinds of vulnerabilities in our high tech environment. When a traveler removes his or her shoes to be x-rayed by the Transportation Security Administration (TSA) before boarding a plane, this bureaucracy is applying a continuous security layer designed to counteract a known security vulnerability. On the other hand, homeland security institutions are supposed to “connect” the proverbial dots to anticipate all the threats and vulnerability scenarios that have not yet happened, might never happen, but are morphing rapidly because of the complex nature of the recombining technologies (old and new), and then patch the security holes, before clandestine actors can exploit them.

Both missions are critically important, but their relation to innovation and therefore to the power of the few is very different. The difference resides in the previously explained distinction between sustaining or incremental technologies and disruptive technologies. The first mission, that I will call here the “systemic mission,” deals with sustaining threats. In contrast, the second one, the “future shock mission,” is supposed to neutralize disruptive – almost random – threats posed by the rapid pace of technological evolution. These differences are key to understanding homeland security’s successes and “failures,” and to establishing an alternative strategy to adapt to this complex ecosystem.

Contrary to what one might think, the majority of potential threats against our high tech society are incremental and not disruptive in nature. A bomb used against a soft transportation target like a subway train or a bus (Madrid 2004 or London 2005), for example, is a well-rehearsed and well-proven method. It has happened many times before and it will probably be tried again with just small incremental innovations to adapt it to the precise conditions of the chosen scenario.
(i.e., size of the bomb depending on the target, method of concealment, etc.). The same thing can be said about the suicide bomber in a highly dense urban setting, the Columbine copycats, the car bombing of public buildings, and airplane bombings (such as the Pan-Am 103 bombing of 1988, the failed attempts of the so-called shoe bomber in 2001, and the Christmas bomber in 2009).

From the point of view of technology, these are all sustaining threats made possible by the sabotage or destruction of critical infrastructure, exploiting known security holes that are difficult to close in open and technologically dependent societies. It is for these kinds of hazards that a bureaucracy is needed to manage, maintain, and ameliorate a system designed to neutralize incremental, known threats. An organizational approach is essential for this systemic mission, as most of the known security deficiencies can be corrected through standardized measures and “best practices,” which create a more secure process for the technology user and ultimately for society. While in some cases budget constraints or civil liberties issues might limit the full spectrum of choices for the policymaker, forcing him or her to imagine disruptive alternatives to solve an otherwise incremental problem, in general the mission can be handled well by an efficient security bureaucracy.

As Henry Mintzberg and others point out: “the key to strategic management, therefore, is to sustain stability or at least adaptable strategic change most of the time, but periodically to recognize the need for transformation and be able to manage that disruptive process without destroying the organization.”

Bureaucracies are good organizations for managing iterative processes that are subject to continuous improvement loops and must be executed every time in the same way, independently of the specific individual who takes care of the task any given day. They are the best solution to the problem of maintaining the same level of quality in a repetitive process.

![Figure 2. Iterative feedback loop of the homeland security Risk Management Framework.](image)

In fact, because of the iterative nature of the bureaucratic processes, this organizational model embraces sustaining change. James Wilson explains, “changes that are consistent with existing task definitions [i.e., incremental innovation] will be accepted ... [and] only those changes that require a redefinition of those tasks [i.e. disruptive innovation] will be resisted.” Mintzberg goes one step further when he suggests: [Traditional planning] usually institutionalized a form of incrementalism [with relation to planned change] ... because incremental change – change at the margin, with limited scope – is consistent with the established orientation of the organization, and is planning itself. In contrast, quantum change – which means comprehensive reorientation ... disrupts all the established categories of the organization, on which planning depends. As a result, such change tends to be resisted, or more commonly, ignored, in the planning process.
For Mintzberg, an organization pays the price of having an enunciated strategy with their "ability to change when it must."

The "systemic" homeland security mission appears to be executed in an acceptable way. Most of the time there are no casualties linked to acts of sabotage against or appropriation of the critical infrastructure of the United States; since the establishment of the homeland security policy, only one plane has been used to perpetrate an attack. In 2010, a single-engine plane was deliberately directed against a government building in Austin, Texas, killing one person besides the pilot and prompting a vivid debate about as to whether or not this incident qualified as an act of terrorism, given the sui generis motivations of the perpetrator (an IRS audit).

If I suggest that the systemic mission appears to be well executed, it is because measuring the success of the homeland security deterrence strategy takes us into the difficult realm of measuring the success of a negative. How do we "tally the score" of events that did not happen because they were deterred by a systemic approach? What statistical indicators are available to determine if the homeland security institutions are doing a better job today than yesterday and a worse one than tomorrow (the basis of continuous improvement)? And, what is more important, how do we know that we are safer and more secure today – because of all this organizational effort – than before 9/11, our baseline?

Answering these questions is essential for both, the "incremental" and the "future shock" missions, albeit even more complicated for the second, as I will later demonstrate.

There is, of course, a simple methodology to prove the effectiveness of most homeland security measures to protect our security environment. A controlled experiment could, for example, shut down all iterative security measures at the airports of one state, while maintaining them at all the other airports in the United States. Once all the protections and security protocols in that state were removed, we would just have to measure the difference between the amount of security incidents originating from those airports (even when flights crossed state lines), and compare them with the control group (the rest of the US) to see if there was a positive difference (i.e., the airports of that state were more secure) or a negative difference (i.e., the airports of that state where less secure). This is the underlying logic of the tests used by the pharmaceutical industry and the FDA to determine the safety of a drug, or by the computing industry to test the effectiveness of the security architecture of their networks.

A homemade version of this test can be tried by anyone: it would just be necessary to take a personal computer and install a version of Windows XP without Service Pack 1 and 2, no firewall and no antivirus program, and then start using the web with Explorer 6. Then, the experimenter will have to wait and see how long it takes for the computer to get hacked or infected by a virus. After this test, he or she will now know with certainty how effective the previous security measures were. (For my computer, it never took more than three minutes for the OS kernel to be corrupted).

The moral, legal, and political implications of such an experimental and controlled approach to measure the effectiveness of a deterrence strategy for homeland security are evident.

A seemingly less effective, but certainly more humane alternative to address the task of assessing effectiveness has been developed in the form of vulnerability analysis methodology for critical infrastructure protection, designed to study and determine the best way to "allocate limited funding in such a way as to minimize overall risk.”

While this methodology creates a more efficient resource allocation system for homeland security funding, the nature of the bureaucratic culture signifies that risk reduction will be perceived through the lens of the continuous improvement process and hence always as an incremental movement. As Christensen points out:

One of the dilemmas of management is that, by their very nature, processes are established so that employees perform recurrent tasks in a consistent way, time after time. To ensure consistency, they are meant not to change or if they must change, to change through tightly controlled procedures. This means that the very mechanisms through which organizations...
create value are intrinsically inimical to change.\textsuperscript{44}

Therefore, homeland security organizations will tend to evaluate critical infrastructure protection countermeasures, even the disruptive ones, within the current continuous improvement paradigm. This is fine for the systemic mission, but everything related to the second mission, the “future shock mission,” will most probably be discarded, because disruptive and unpredictable threats posed by the recombining nature of new technologies cannot be confronted by incremental methodologies. They are by definition outside of the feedback loop.

In other words, for the yet to be planned homeland security incident that will use a new combination of technologies never tried before, the current homeland security institutional framework cannot connect the dots, because there are no dots to be connected. What makes Christensen’s concept of disruptive technology so troubling for administrators all over the world is that he clearly demonstrated that good planning, and not the opposite, was in fact one of the main reasons why big companies failed and were crushed by new disruptive technologies. In the context of homeland security policy, this means that with the current organizational model, the bureaucracy might get as good as it can possibly be and still miss the next threat precisely because it has learned to be very efficient in its normal operation, thus resisting any change outside its sustaining processes. Hierarchical iterative bureaucracies are precisely the worst kind of organizations to confront “out-of-the-process” threats.

This is why I stated earlier that a traditional bureaucracy cannot be the one reacting to disruptive threats. Instead, to fight this bureaucratic hysteresis the current homeland security institutional design (indispensable for the “systemic mission”) has to be complemented with another very different approach to security to confront the recombining threats of the permanently disrupted environment. A new ad-hocatory organization, with no direct involvement in the fight against incremental threats or the day-to-day operation of homeland security institutions, should concentrate its efforts on producing positive homeland security disruption to counteract the negative effects of the power of “the few.”

**PUSHING THE BORDERS OF THE IMPOSSIBLE: DISRUPTING POSITIVELY THE HOMELAND SECURITY ENVIRONMENT**

While the first homeland security “systemic mission” of neutralizing incremental threats seems to be fulfilled in an acceptable way by the current homeland security institutional model, the second “future shock mission” focusing on counteracting the threat posed by the recombining of disruptive technologies is almost nonexistent. In fact, the relative success of the first mission is one of the biggest obstacles to accomplishing effectively the second one. As the homeland security bureaucracy becomes more effective in limiting the success ratio of incremental threats, it creates a political environment where it is very difficult for the policymaker not to keep allocating more resources to the same programs that appear to be working, therefore sustaining the investment cycle. This makes it very challenging for the few to repeat the last attack, but it also focuses the limited organizational resources and attention span on the last incremental scenario and away from the next (unforeseeable) disruptive attack. Hence, the strategic truism, which states that successful armies and navies are always preparing to fight the last war, has, in this case, metaphorical and literal significance.

In this security ecosystem defined by the accelerated pace of disruptive technological recombination, “connecting the dots” is not an acceptable strategy to avoid the next threat. Intelligence gathering is not possible for attacks that have not yet been planned or even conceived, combining technologies that are or will be available, but were conceived for other purposes. Also, while focused intelligence plays a central role for avoiding specific threat scenarios, once these scenarios are identified and hopefully neutralized they become, by definition, part of the systemic mission and an incremental threat.
Instead, homeland security institutions addressing the “future shock mission” have to be able to be proactive and become disruptive agents themselves. In this way, the state would reclaim the initiative with innovation (instead of fighting against it), provoking positive environmental changes through a sustained research and development effort. Doing this requires an organization shielded from the “systemic mission,” designed to avoid the same things that make other bureaucracies so successful: iteration and incremental processes.

Administrative reforms have a bad name in homeland security, probably because there have been so many of them in a very short amount of time. Wood and Waterman established that political reorganizations might not be enough to break bureaucratic resistance to change when more than one organizational culture exists inside the bureaucratic bodies. That is the case of the Department of Homeland Security, where the so-called department components (TSA, CBP, the Coast Guard, FEMA, Secret Service, etc.) have strong organizational cultures that precede the merger that created the department in 2002.

It is precisely for this reason that a new partial reorganization is necessary, addressing the limitations of the current structure to confront the “future shock mission.” The current competing organizational cultures of the homeland security bureaucracy are oriented to accomplish the old missions of the department’s individual components, fighting threats in an incremental way. Any new task given to this existing structure will be watered down by an older, more successful, more proven and more consolidated organizational ethos. Wilson explains it:

Tasks that are not part of the culture will not be attended to with the same energy and resources as are devoted to tasks that are part of it. Second, organizations in which two or more cultures struggle for supremacy will experience serious conflict as defenders of one seek to dominate representatives of the others. Third, organizations will resist taking on new tasks that seem incompatible with its dominant culture. The stronger and more uniform the culture – that is, the more the culture approximates a sense of mission – the more obvious these consequences.

In the current homeland security administration model, research and development efforts are embedded in the “systemic mission” and most if not all of its current results are incremental and not disruptive in nature. Therefore, there is no incentive to look for solutions to problems that are not considered part of the operational objectives of the current homeland security environment. That is why there is so much interest and debate regarding, for example, the development and implementation of the controversial full body scanners (an incremental innovation useful to the current operational mission of DHS), and so little interest in countermeasures for security risks that have never been exploited.

In fact, Michael Greenberger demonstrated that under the current organizational model, homeland security’s institutions are unresponsive even to technology solutions that are widely available. He found that because of organizational limits, the Department of Homeland Security was incapable of recognizing widely available technology solutions to security threats in at least two cases: efficient “see through” technology to screen cargo, and liquid explosive detection for airplane passengers. To combat this resistance, he proposed an institutional reform to create inside DHS a “Department of Homeland Security Technology Mobilization Board” based on the successful mobilizations boards used during World War II to “review and search out antiterrorism technology and quickly decide whether the new technology should be used and promoted in the homeland security effort.” I would like to take this good proactive approach a step further, using as a model the most disruptive institution for military research and development in the history of mankind: the Defense Advanced Research Projects Agency (DARPA).

Created in 1958 after the so-called “Sputnik Crisis,” when the American government was taken by surprise by the successful launching of the Soviet satellite Sputnik, DARPA’s mission is “to maintain the technological superiority of the U.S. military
and prevent technological surprise from harming our national security by sponsoring revolutionary, high-payoff research.” It is a highly disruptive organization “with no operational mission, no service requirements and designed to protect fragile ephemeral projects.” It doesn’t avoid future shocks surprises in itself, but tries to create its own surprises faster than its adversaries, thus controlling the pace of military innovation.

An organization like DARPA succeeds in managing a disrupted environment because it does not negate its disrupted or disruptive-prone nature, but instead uses it to its advantage. This means that it fights surprise by creating surprise, consciously producing as many environmental disruptions as it can. When DARPA succeeds, it forces American adversaries into the uncomfortable position of being the ones reacting to American military disruption and trying to guess the next move, robbing those adversaries of the initiative that the few naturally tend to enjoy. By doing this, DARPA does not counter specific future shock surprises, but it creates a security environment where US Armed Forces have the upper hand.

As any investor knows, high return and high risk are directly correlated. Therefore, high payoff research and development need a higher institutional tolerance for risk and failure. Christensen points out that because “the ultimate uses or applications for disruptive technologies are unknowable in advance … Failure is an intrinsic step toward success.” DARPA’s creative process aims to “find an area of technology that could go a long way toward serving the needs of the country if improved but that wasn’t getting much attention in the private sector, put some well-considered research and development money into it to get it on its feet, and then cut it loose.” Because of this high-risk approach, some of its projects fail in a way that would put in danger the career of the project manager in any other organization, while others, like the Advanced Research Projects Agency Network (ARPANET), succeed in forever transforming the human environment.

For this approach to work in the context of homeland security, it is essential to create an agency isolated from the core requirements of the “systemic mission.” It would have to be a task oriented research and development organization designed to positively disrupt the security environment with technology solutions for problems not yet identified by “the few.”

Some, like Joshua Cooper, have used the metaphor of an institutional immune system to describe such an approach to defend society against the negative effect of the accelerating pace of change. For him, “this constant surprise, and the demand it makes for an ‘always-on’ defense, is one of the reasons we need a deep-security immune system instead of an old-style Grand Strategy.” An evolving homeland security immune system requires a risk management approach to identify vulnerabilities with low investment-high rewards opportunities to close a technological security hole while at the same time the usability of the concerned technology is preserved and, if possible, enhanced.

DARPA’s success as the proactive component of the Department of Defense immune system is due to the fact that it is structured as an adhocracy, a term coined by Toffler to describe an organizational model where organic temporary relations are established (hence the ad hoc part of the name) to respond to a particular task (or threat) with very little or no formal hierarchy or standardized behavior. An adhocracy is a “fast-moving, information-rich, kinetic organization of the future, filled with transient cells and extremely mobile individuals.” Such a model for homeland security would create ephemeral teams of experts used to close high risk security holes that would then be disbanded to make place to another team formed to tackle another disruptive challenge.

In fact, as Christopher Ford identified, some of DARPA’s most recent projects have already some unambiguous homeland security implications. The “DARPA network challenge,” for example, showed how social networking web tools and aggregators can be engaged to gather data, mobilize participants, foster collaboration, and build trust in the context of multiple homeland security missions.

For the homeland security “future shock” mission, the challenge is not only to pair a disruptive solution with a disruptive
problem; even the problem definitions themselves should be disruptive in nature: How to neutralize a threat that no one has yet identified as a threat? Thus, the “future shock” prevention effort must identify proactively security threats to the human environment provoked by the recombining of technology and human social and cultural behavior.

Consequently, this new homeland security institution would have to invest an important part of its resources probing disruptive security scenarios, using a “red team” methodology to identify security shortcomings. These “white hat” hackers would try to hack the whole United States of America technology environment, establishing the mission requirements for the new agency. Only then, after a critical technology has failed this highly classified penetration test or a scenario that recombines multiple technologies in a novel way has been identified, research and development could begin to find a minimum sufficient response that permits the technology to operate as efficiently as before but closes preventively the security hole. While this proactive approach will not identify every recombining threat, it will add a new layer of disruption and innovation to the human ecosystem on top of the ones that are already in place, but this time under the direct control of the homeland security institutions.

Because there is no bigger threat to America’s interests than the loss of competitiveness caused by crippling its critical sectors in the name of pointless security measures – something akin to an autoimmune disease if we extend the metaphor a little bit more – the concept of a “Minimum Sufficient Response” is essential. In fact, for the effort to be successful and sustainable, most of the tasks should be dual-purpose, enhancing (rather than the opposite) the usability of the concerned technology. This would also have a protective effect on American civil liberties and human rights, by limiting the scope of the security procedures. If done properly, this new actor in the homeland security environment would identify unproductive and bloated security solutions where a risk management approach is absent (i.e. a layer of security that does nothing to enhance the resilience of a technology), and could propose the necessary changes to improve the usability of the system.

While incremental research and development is an essential part of the systemic mission,” this new organization should be isolated from them. If an attack by the few does occur, the technological solution needed to avoid such an event in the future should not be the responsibility of this new institution. Once a real “red team” has made explicit the exploitable vulnerability, fixing it has become an incremental and not a disruptive challenge.

Proving the effectiveness of this new institutional approach will be difficult and will require “out of the box” managerial and political skills. To demonstrate this, I offer to the reader a thought experiment: Imagine that an organization like the one I am describing existed in 1997. In 1998, the organization’s red teams identified the cockpit doors of commercial airplanes as weak links in the security environment of the transportation sector for many scenarios, none of which looked like the 9/11 terrorist attacks. Then, multidisciplinary research and development teams identified a Minimum Sufficient Response technology solution: by armoring the cockpit doors and making it impossible for the pilot to open them while airborne – even if he or she wants to (in case the criminal actors try to blackmail him or her by holding hostage a passenger or a flight attendant) – no asymmetrical actor would be able to gain control of the airliner, closing the security hole.

If such a process would have taken place, we would never know that something as costly as 9/11 was deterred, but we would have taken advantage of a low investment-high reward opportunity to “upgrade” the United States security ecosystem in a disruptive way, leaving mostly unaffected the usability of the technology. I use the 9/11 example because it is a disruptive threat that has already been identified and mostly neutralized by precisely this kind of solution (the most cost effective measure of all the preventive solutions identified by the 9/11 commission report). It also shows how hard it would it be to measure the effectiveness of a procedure that might deter a catastrophic
event if that event never takes place because of our actions.

Finally, because what I am proposing here is a DARPA inspired model for the problem of adapting the homeland security organizational framework to respond to the power of “the few,” it is necessary to explain why I do not consider the existing HSARPA a sufficient solution. First, HSARPA lacks the proper funding needed to have the same positive effect that DARPA has had for research and development. Second, HSARPA is devoting most of those resources to research incremental solutions to incremental problems. The HSARPA mission specifically states that it was created to “enhance departmental operations.”60 Because of this, HSARPA is not capable of addressing the “future shock mission.” One employee of the science and technology directorate at DHS described HSARPA to me as an agency “suffocating” inside of the Department of Homeland Security bureaucratic structure. For an organization to be successful at confronting disruptive technologies, strong evidence suggests that an independent small organization is needed to escape the gravitational field of the incremental mission of the bigger institution and its organizational culture.61 Currently, most if not all of the HSARPA projects are sustaining research and development programs pivoting around the operational missions of the Department of Homeland Security.

CONCLUSION

The expressed objective of this article was to define the rapid pace of technology’s evolution and its recombining nature as two primal forces that shape the homeland security environment in a way that has lowered the barriers to entry for disruption by small groups of actors that I called here “the few.” Because of this recent phenomenon, high tech societies require a security strategy to react to the threats that arise from this amoral phenomenon, and to preserve innovation opportunities and freedom of usability for new technologies. In the United States, this mission stands on the shoulders of the homeland security institutional framework, which is a consequence of a catastrophic “power of the few” attack.

It was also my intention to demonstrate how the dual nature of innovation (incremental and disruptive) creates very different challenges to the security environment. While homeland security institutions seem to be dealing effectively with the incremental threats, the current model offers no real response to the disruptive ones. This has a clear and dangerous negative effect on the American strategic process, penalizing disruptive solutions to disruptive threats, and privileging an incremental approach to security planning. Because both are needed, a new institutional framework should be instituted to take advantage of the proven superiority of adhocratic adaptive organizations to deal with unpredictable, chaotic environments. By adding a new layer of positive disruption to the environment, positive and unpredictable innovation would provide the best possible antidote to negative innovation and the illicit appropriation of technology.

America has been built on the belief that the future will be better than the past and that the best way to harness progress is to allow people to experiment and think freely. Protecting the homeland must become a synonym for protecting those foundational values, by making sure that positive technological recombination is available for all, and people can embrace and not be afraid of this permanently disrupted human environment.

ABOUT THE AUTHOR

Rodrigo Nieto-Gomez is an instructor at the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, CA. His fields of research include the geopolitical effects of homeland security/defense and national security with a regional focus on North America, border security, discourse analysis, and the implications of new technologies for security and defense policies. Dr. Nieto-Gomez obtained his PhD in geopolitics at the Institut Francais de Geopolitique of the University of Paris. More information and contact information can be found at: www.rodrigonietogomez.com.
Available as a Wikipedia commons at: http://upload.wikimedia.org/wikipedia/commons/1/1e/Allied_Invasion_Force.jpg.


3 Also, the pieces move all together and at the same time, instead of in alternating turns; their intentions and incentives are not always shared with the chess player and one piece, coming from outside the chessboard can disrupt the whole game! The more one explores the metaphor, the least chess seems like a good analogy for strategy.

4 Available at: http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1539

5 Plato, Cratylus [Gutenberg project edition]. Available at: http://www.gutenberg.org/ebooks/1616


8 The term itself was coined by Daniel Bell in his now classical exercise of “social forecasting,” one of the first works of social science that tried to introduce social chaos to the domain of trend studies, albeit still emphasizing the notion of forecasting. See: Daniel Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting (New York: Perseus Books Group, 1976).

9 See: CIA, World Factbook Labor Force by Occupation. USA: 0.7%, Japan: 4%, Germany: 0.9%, France 1.8%, United Kingdom 1.2%. Available at: https://www.cia.gov/library/publications/the-world-factbook/

10 In economics, the primary sector is formed by all those activities that involve the process of growing food and obtaining raw materials. The secondary sector is composed of heavy industry and manufacturing. The tertiary sector is made up of the service industry. While there is no controversy surrounding the fact that the knowledge economy has transformed the tertiary sector, the environments for the primary and secondary sectors have also been reshaped by technological transformations.

11 Gregor Mendel is one of the founding fathers of modern genetics. Mendel inheritance laws explain how the process of hybridization can be used to reinforce desired traits in plants and animals.


This phenomenon of the exponential growth of computing power is called “Moore’s Law,” and it is one example of trend forecasting that has proven to be accurate, in part because it became a self-fulfilling prophecy. It assumed the form of the gold standard for the semiconductor industry’s long term planning and benchmarking, and it is based in the knowable physical characteristics of semiconductors. In a way, it is like forecasting what the population will look like in 20 years, when you already know the current birth rate. What will happen with Moore’s Law after we reach the physical limits of those materials is less clear. See: Gordon Moore “Cramming more components onto integrated circuits,” *Electronics* 38, no. 8 (April 1965). [https://docs.google.com/viewer?hl=en&url=http://download.intel.com/museum/Moore_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf&pli=1](https://docs.google.com/viewer?hl=en&url=http://download.intel.com/museum/Moore_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf&pli=1).

For example, the Huffington post, “the Internet newspaper” and technically a blog, was bought in 2011 by America Online for $315 million. At that moment, the blog/newspaper was attracting more than 25 million visitors every month and more importantly, had become a strong liberal voice in American politics.

Evgeny Morozov has demonstrated that social movements based on web 2.0 technologies are in fact more vulnerable to repression because of their dependency on these technologies. See: Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, [Kindle Edition] Retrieved from [www.amazon.com](http://www.amazon.com).

Clay Shirky, *Cognitive Surplus*. Both, Morozov and Shirky have been engaged in a very public and rich debate about the virtues and shortcomings of the internet as a tool for democracy. For Morozov’s criticism of Shirky’s position see: [http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/](http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/)

For Shirky’s response, see: [http://www.prospectmagazine.co.uk/2009/12/the-net-advantage/](http://www.prospectmagazine.co.uk/2009/12/the-net-advantage/)


Ray Kurzweil upgraded the term in 2003 with his “law of accelerating returns,” forecasting a technological “singularity,” a scenario where biological evolution would be replaced by a technological one. The term has been gaining adherents and antagonists inside and outside of academia since it was proposed. Nevertheless, Toffler’s acceleration of change hypothesis is discussed here independently of the singularity prediction, as this last one is irrelevant for the objectives and proposals of this paper. The arguments exposed here are valid if the forecasted singularity scenario is correct or not. For more information on the singularity concept see: [http://www.kurzweilai.net/meme/frame.html?main=articles/art0610.html](http://www.kurzweilai.net/meme/frame.html?main=articles/art0610.html)


For a frightening and interesting analysis on the limits of nuclear control and suppression and the technological challenges ahead, see:


Dr. Calvillo Gámez and I introduced this term to describe the process when a user appropriates a technology thwarting the designer’s intentions and breaking the law. 9/11 is a clear example of a successful illicit appropriation of the transportation sector. See Rodrigo Nieto-Gomez and Eduardo Calvillo Gámez, “The Case of ‘Illicit Appropriation’ in the Use of Technology,” in M. Vargas, and A. Edwards, eds., *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives* (Hershey, Pennsylvania: IGI Global, 2010).


36 For example, the dictionary of military terms of the DoD defines terrorism as: “The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.” Available at: http://www.dtic.mil/doctrine/dod_dictionary/.

37 In a “classical” behavioral profile for hackers published by the Cyberpunk project in 2003, using supposedly (no methodological appendix is presented) a trial balloon approach with 100 USENET hackers, it was established that “Hackers are generally only very weakly motivated by conventional rewards such as social approval or money. They tend to be attracted by challenges and excited by interesting toys, and to judge the interest of work or other activities in terms of the challenges offered and the toys they get to play with”. Available at: http://project.cyberpunk.ru/idb/portrait_of_j_random_hacker.html.

38 Or even with no adversarial actor at all.


44 Clayton Christensen. The Innovator’s Dilemma.


46 James Wilson, Bureaucracy.

47 See: http://www.tsa.gov/ approach/tech/imaging_ technology.shtml


49 Available at: http://www.darpa.mil/ mission.html

50 Mr. Ryan Paterson Deputy Director for the Adaptive Execution Office (AEO), DARPA Adaptive Execution Office Conference, Naval Postgraduate School, 23 March 2010.

51 Clayton Christensen. The Innovator’s Dilemma.


53 For a list of some of some of DARPA’s high profile hits and misses see: “Fifty years of DARPA: Hits, misses and ones to watch” http://www.newscientist.com/article/dn13907-fifty-years-of-darpa-hits-misses-and-ones-to-watch.html


55 Alvin Toffler. Future Shock.


58 In fact, it is very probable that such a team would have identified something resembling the 9/11 scenario, finding it very plausible. In 1994, the Groupe d’Intervention de la Gendarmerie Nationale of the French government stopped four members of the Algerian “Groupe Islamique Armé” from using a hijacked airplane against the Eiffel Tower. Tom Clancy’s fictional novel Debt of Honor (1994) identified some of the same key technological vulnerabilities that made 9/11 possible, proving that they were publicly known. The author explained to the BBC how he came with the scenario: “Well first you identify the point of vulnerability and then you try to see how you can address that particular problem.” Interview retrieved from: http://news.bbc.co.uk/hi/english/static/audio_video/programmes/panorama/transcripts/transcript_24_03_02.txt

Nevertheless, for the sake of the thought experiment, let assume that a 9/11-like scenario does go unnoticed.

59 The capabilities analysis done by the 9/11 commission expressed that: “Any serious policy examination of a suicide hijacking scenario, critiquing each of the layers of the security system, could have suggested changes to fix glaring vulnerabilities—expanding no-fly lists, searching passengers identified by the CAPPS screening system, deploying Federal Air Marshals domestically, hardening cockpit doors, alerting air crew to a different kind of hijacking than what they had been trained to expect, or adjusting the training of controllers and managers in the FAA and NORAD”. Available at: http://www.9-11commission.gov/report/911Report_Ch11.htm

60 DARPA’s allocated budget might well be the most cost-efficient use of taxpayer’s money in the entire US government. Its annual $3 billion has given us the Internet and GPS navigation, just to name the two most visible and successful projects of the agency. GPS technology is today a multibillion market and the Internet created a whole new economy.

61 Available at: http://www.dhs.gov/xabout/structure/editorial_0530.shtml

62 Clayton Christensen. The Innovator’s Dilemma.