2011-09

Preventing the Next 9/10: The Homeland Security Challenges of Technological Evolution and Convergence in the Next Ten Years

Nieto-Gomez, Rodrigo

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (September 2011), v.7 no.2
https://hdl.handle.net/10945/24988

Preventing the Next 9/10: The Homeland Security Challenges of Technological Evolution and Convergence in the Next Ten Years

Rodrigo Nieto-Gómez

The September 10, 2001 edition of *Time* magazine dedicated its cover story to Colin Powell and his "megastar wattage … curiously dimmed" inside of the Bush administration. Of course, no one knew that at that precise moment all the human and technological components for the worst attack ever committed on United States soil were already in place, and imminent danger existed. Discussing General Powell's role inside the White House was a good cover story for September 10th.

Then came the attacks of September 11, 2001 – 9/11.

The catastrophic event occurred without warning. The attacks seemed like a random and unpredictable occurrence; a black hole in our cognition.

But obviously, 9/11 was a complicated event that required the use of many previous steps, many technologies in concert, and many brains working together to achieve that particular end. What we saw that day was only one more step (not even the culmination) of a very long series of converging processes – a deviant result of the innovation process that also fuels progress inside our technologically dependent civilization.

On September 12, 2001 a still perplexed world asked how was it possible that the terrorists' attacks were not stopped; all the clues were there, the dots were waiting to be connected and al Qaeda had already been active and recognized as a threat by the federal government since the 1990s.

On September 14, 2001 *Time* had a new cover. It featured a collapsing World Trade Center – an avalanche of dust, steel and glass.

But if 9/11 was just the visible part of a longer process, were did it all start?

The historic account of the *9/11 Commission Report* finds the roots of 9/11 in the rise of a national resistance against the communist government of Afghanistan in 1978, which would eventually lead to the formation of al Qaeda[1].

I argue that the patterns that lead to 9/11 are much older, but at the same time they are considerably less linear. Therefore, that direct line that the *9/11 Commission Report* traced is nothing more than an illusion produced by what Nassim Taleb calls the retrospective distortion, "or how we can assess matters only after the fact, as if they were in a rearview mirror (history seems clearer and more organized [linear] in history books than in empirical reality)."[2]

This retrospective distortion creates a security ecosystem where homeland security practitioners feel pressured to try to "connect the dots" every time, instead of adapting to an environment of emerging patterns and mutating dots that cannot be connected.

Moreover, certain technologies have been doubling in capacity every few months for many years now and, as a consequence, technology improvement cycles have also shrunk. We have grown used to having a new and improved version of a product that is twice as powerful in just a few months, and radical disruptive propositions every year or two. Because of technological convergence, it is very hard to predict what unintended consequences all those improvements and new technologies will have once they are recombined with others, and what catastrophic possibilities convergence might have that we will miss on the next 9/10. This is the chaotic security environment where homeland security operates today. For the next ten years, homeland security should embrace it.

9/11/1973: Why Not?

Romance languages, as well as German, have introduced the neologism of "uchronia" (from *uchronie* in French) in their vocabularies to define the subgenre in fiction where reality as we know it is profoundly altered by a change

in the chain of events. They describe a time that does not exist, or a non-time. In an uchronic novel, reality it is indistinguishable to ours until an event – often called a "point of divergence" or a "Jonbar Hinge" – triggers a series of second and third level consequences that end up creating a reality that it is almost unrecognizable from ours, even though initial conditions were identical.

In Turtledove's novel *How Few Remain*, the south won the American Civil War because of an accidental recovery of a document; in *The Man in the High Castle*, by Phillip K. Dick, a successful assassination plot against President Roosevelt creates an environment that ends up being favorable to the axis powers, who end up winning World War II.

Uchronias make interesting readings (or movies, although some people have trouble enjoying the convoluted plots of time paradox films) because they describe contextual patterns that we all recognize and are familiar with. Then, after a fictional "point of divergence", second and third degree consequences create a believable new environment that is almost unrecognizable from reality as we know it, but that we can accept as a plausible "what if." Uchronias confront us with the fragility of reality and the power of the randomized and chaotic forces that surround us. They contradict the linear nature of historic events; show us how precarious and fluid are "the dots" that have to be connected, and how organic is the nature of any threat. If the briefcase bomb would have been a little to the left (or to the right… who knows?), Hitler would have died; if one of many things described in the *9/11 Commission Report* would have happened (or not happened) on 9/10, we would have continued the discussion about Collin Powell on 9/12.

The innovation cycle is "pushing" Jonbar Hinges on society faster than ever before. Each new or improved technology adds a new series of combinatorial possibilities that can shape society in unpredictable ways. Many technologies today are nothing other than backbones designed to support spontaneous innovation – touch screen blank slates for others to design their apps, in an emerging cycle that feeds on itself.

Millions of people potentially empowered by those backbone technologies mean millions of potential innovators all thinking and doing things that have not been thought or done before.

But those innovations do not happen in a vacuum. Instead, as Brian Arthur explains:

> New technologies in time become possible components – building blocks – for the construction of further new technologies. Some of these in turn go on to become possible building blocks of yet newer technologies. In this way, slowly, over time, many technologies form from an initial few, and more complex ones form using simpler ones as components. The overall collection of technologies bootstraps itself upward from the few to the many and from the simple to the complex. We can say that technology creates itself out of itself. [3]

Ideas – or memes, as evolutionists like to call them – evolve from the simple to the complex. They progress in the sense that whatever was there before will be constantly improved and recombined with new thoughts and ideas making something better that can then be used again to continue this incessant process.

Unfortunately, innovation has a dark side. The same accelerated combinatorial evolution that empowers entrepreneurs to rapidly improve our high tech environment can, and often is, used to harm the innocent.

In fact, I believe 9/11 was the product of thousands of years of innovation in a radical, deadly, and novel way.

The innovative recombination of technology that made those terrorist attacks possible took advantage not only of the knowledge and imagination of Khalid Sheik Mohammed and Osama Bin Laden, but also of Minory Yamasaki (the WTC architect); the ingenuity of the Wright brothers and all the aviation heroes who made flying machines a reality; the hundreds of engineers from Boeing; and, in general, thousands of years of accumulated human knowledge (material engineering, tube frame design, Le Corbusier modernist philosophy, and thousands more innovations, all the way back to the wheel, language and the invention of tools!).

In Uchronia, 9/11/2001 could have occurred on 9/11/1973, just a few months after the ribbon cutting ceremony of the

World Trade Center. By that time, jumbo jets were flying, the Pentagon had been built, and most of the technology that was materially used during 9/11 existed, ready to be recombined in order to achieve a catastrophic result.

But if the technology already existed in 1973, the "9/11 idea" did not. Creativity does not evolve following a linear path of dots and many things had to happen for this complex adaptive environment to evolve towards a state where 9/11 went from being a possibility that lurked in the dark since 1973, to a sad meme of human innovation [4].

That is the paradox. We can easily imagine "planes as weapons" as the *9/11 Commission Report* asked. The meme requires the recombination of just a few previously known ideas: suicide militants, planes, volatile jet fuel, and skyscrapers. But the same thing can be said for Facebook (it is not hard today to imagine an interconnected personal database), Amazon (an online-only retail store), or Netflix (a mail-based rental model that combined the backbone of the postal service with the Internet). Yes, we can imagine all that, but someone imagined it first, recombined technologies and created huge companies out of it. We can all imagine an iPad, but Steve Jobs and the rest of the Apple designers imagined and successfully implemented it first.

Innovation is innovation not because it is impossible to think of something, but because no one else thought of it before.

WE DON'T REINVENT THE WHEEL – WE APPROPRIATE IT!

Ted Lewis identified the importance of "stigmergy" in the invention-innovation cycle: "invention [works] as the stimulus and innovation as the response. After each cycle, the stimulus-response pattern repeats." [5]

I agree with him that "stigmergic" behavior is one of the patterns that govern the combinatorial evolution process of innovation and the technological environment. Lewis established the reciprocal need inventors and innovators have for each other in a stimulus-response cycle loop, but I believe that there is a third key actor in the invention-innovation cycle: the adopter of the technology. Inventors, innovators, and adopters stimulate each other. Although most adopters will be fairly passive actors, some will adapt the technology to be used as something that neither the inventor nor the innovator thought it could be used for, in a process that Dix refers to as appropriation. [6]

I am convinced that all innovators are also active appropriators – they appropriate existing technologies for their new designs, using them in unanticipated ways.

For example, the designers of the Chevy Volt did not have to reinvent the wheel or velour interiors. On the other hand, I am sure that the inventors of the wheel or the so-called "faux velvet" did not envision an electric car as one of the applications of their technological innovations (none of them knew what electricity or cars would be!). Progressive innovation requires the appropriation of previous technologies to be used differently from what the original designer anticipated.

When a clandestine actor uses infrastructure to do harm, he or she illicitly appropriates the technology to achieve a goal different from what the designers intended. In the online world, we give the name of hacking to that behavior. In the real world, terrorists hack our high tech society every time they are successful and the acceleration of technological development provides the illicit appropriator more building blocks and more possibilities to combine them every day. Combinatorial evolution creates unforeseen convergence that gives to the inventor-innovator-appropriator cycle more uchronic choices.

Terrorism is a technological artifact that results from the appropriation of systems through combinatorial evolution. Forecasting every possible innovation in this context is impossible.

Consequently, while it seems like an easy challenge to imagine planes as weapons (in fact Tom Clancy wrote an almost uchronic novel out of this exact idea), Taleb reminds us "had the risk been reasonably conceivable on September 10, it should not have happened. If such a possibility were deemed worthy of attention, fighter planes would have circled the sky above the twin towers, airplanes would have had locked bulletproof

doors, and the attack would not have taken place, period." He then continues: "something else might have taken place. What? I don't know."[7]

At this precise point, I am sure, many patterns are forming that will create appropriation opportunities in the future, and some of them will be harmful. Which ones will turn out to be relevant? I don't know either.

In this complex adaptive environment of accelerated high tech innovation, the "connect-the-dots" game seems to be the worst possible metaphor. If one has to be found, I would like to offer an "Encrypted letter soup" as a replacement, where all the relevant information of a catastrophic event becomes relevant only after the pattern has been recognized. That is, after the fact.

In this primordial letter soup of catastrophes, the proverbial dots to be connected are encrypted in noise. Worse, because there is no preconceived pattern, the "dots" evolve and change in randomized ways, until one day they acquire meaning.

Connecting every dot is called paranoia. In the case of nation states, institutional paranoia is quite often the foundation of totalitarian regimes that thrive in the waters of the politics of fear.

We cannot anticipate all innovations, and imagination understood as anticipatory forecasting of new threats cannot be bureaucratized.

CONCLUSION: HOMELAND SECURITY: THE EARLY ADOPTER DISCIPLINE

Combinatorial evolution of technology does not have to favor the illicit appropriator. This randomized environment created by the accelerated pace of technology cycles will favor those who can produce more ideas, and ride the wave of uncertainty instead of opposing it.

While studying the origins of the so-called geniuses, Dean Simonton found that "The more ideas a mind can produce, the higher the odds that those ideas will be original and varied.... Flexibility and originality are both to a very large extent mere consequences of fluency."

His research conclusively demonstrated that:

> The creative process is to a certain extent blind. Even the greatest creators possess no direct and secure path to truth or beauty. They cannot guarantee that every published idea will survive further evaluation and testing at the hands of audiences or colleagues. The best the creative genius can do is to be as prolific as possible in generating products in the hope that at least some subset will survive the test of time.[8]

The homeland security effort for the next ten years must encourage public and private inventors, innovators, and appropriators of new disruptive security ideas to be prolific and then aggregate those efforts. This would allow us to surpass – by a few orders of magnitude – the number of disruptive ideas produced by the clandestine actors.

In the next ten years, the Department of Homeland Security (DHS) should embrace and become the early adopter of almost all new technologies, appropriating them, generating knowledge about them, and proactively thinking how to recombine them with other building blocks in order to make civilization more resilient.

Ten years from now, DHS must be the gold standard of usability labs in order to understand, appropriate, and improve as many new technologies as possible.

We cannot control the complex adaptive environment of technological evolution nor should we try, as positive innovation requires – in Schumpeter's words – creative destruction and chaos.[9] Nevertheless, we can control the government's own pace of innovation, and its rate of technological understanding and adoption.

For the next ten years, the homeland security community should become the most tech-enthusiastic community inside of government. No one – with the probable exception of DARPA – should be more innovative and more "tech savvy" regarding what makes technology usable, why people use a particular technology, and how security can be improved while also improving usability.

In 2021, homeland security should be perceived as a project that has helped

maintain, or even accelerated, the pace of the innovation cycle and not the opposite. A project that has made the backbone of American innovation stronger, more open for positive appropriation, and more resilient for when the unavoidable illicit appropriation does take place.

Homeland security as a doctrine should embrace combinatorial evolution and plan for it. Government projects should be innovative, but also scalable, so they can be adapted to the unexpected, and they should prefer social to centralized deployment of technology. When possible, government should prefer software instead of hardware and off-the-shelf to proprietary. It should also design policy and infrastructure for openness instead of secrecy; there are more good people than bad people, so policies should take advantage of this superiority of numbers and aggregate their knowledge and effort.

Homeland Security technology and strategies (also a social technology) should be easily upgradable. If not, many of them will be will be legacy technology by the time they reach the public. Homeland security decision makers should avoid bloated solutions and examine constantly old security measures to avoid petrifaction. It might even be worthwhile to consider "sunset" security laws and regulations, in order to permanently question if old security layers are still needed in the ever-evolving security environment (we might be able to finally leave our cell phone on during take off…as many iOS users already do, without knowing it![10])

Finally, instead of official futures (we will get them wrong anyway), the homeland security planning process should plan for Uchronia and serendipity. Current scenario planning methodologies are a good starting point, although homeland security practitioners should create their own.

Technological evolution is part of our instinct to explore. It is who we are, and it is part of what makes us better than our previous selves. In 2021, the homeland security project should be the reason why the creative backbone of civilization is stronger and more resilient, so the explorers of tomorrow can perpetuate the very American tradition of thriving in the unknown, pushing the last frontier – the knowledge frontier – further, one innovation at a time.

ABOUT THE AUTHOR

Rodrigo Nieto-Gómez *is a research professor at the department of National Security Affairs and the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, California. His fields of research include border security, the implications of new technologies for security and defense and the geopolitical and strategic implications of homeland security and defense policies.*

---

[1] The National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report* (July 22, 2004), 47. http://www.9-11commission.gov/.

[2] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (Kindle version, 2010).

[3] Bryan Arthur, *The Nature of Technology: What It Is and How It Evolves* (Kindle version, 2009).

[4] The history of aircraft hijacks is the history of a threat evolving from the first hijackings that were conducted by pilots trying to escape from authoritarian communist regimes, to hijacking as an extortion tool, to the first incidents of terrorist sabotage. See: http://fcafa.wordpress.com/2011/03/12/they-flew-to-exile-1950/.

[5] Ted Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World* (Monterey, CA: Agile Press, 2011), 259.

[6] Alan Dix, "Designing for Appropriation," *Proceedings of the BCS HCI 2007 Conference, People and Computers XXI* (London, UK: BCS-eWik), 2, http://www.comp.lancs.ac.uk/~dixa/publist-2007.html.

[7] Taleb, *The Black Swan*.

[8] Dean Keith Simonton, *Origins of Genius: Darwinian Perspectives on Creativity* (Kindle version, 1999).

[9] Joseph Schumpeter might be, from among all the classical economists, the one who best understood the nature of innovation and change. In Schumpeterian terms: "Industrial mutation – if I might use that biological term – that incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one. The process of Creative Destruction is the essential fact about capitalism." From: Joseph Alois Schumpeter, *Capitalism, Socialism and Democracy* (Google books version, 2003).

[10] iOS is the operating system that powers most Apple mobile devices, including the iPhone, iPad and iPod Touch. Turning the device off is a two step process that requires that the user hold the off button for four seconds, and then move a virtual button from left to right in the touch screen. I have noticed many times that during take off or landing, when supposedly all electronic devices should be off for the security of the plane, what many iOS users do is to press the off button once. While this behavior darkens the screen, the Apple device is still fully powered. Nevertheless, no accidents have occurred after many years of unintentional violations of the "turn off all electronic equipment" security rule.