This work has been submitted to NECTAR, the Northampton Electronic Collection of Theses and Research.

Article

Title: Towards a higher plane of air transportation security: from hubris to knowledge

Creators: Hills, M. and McFarlane, P.

DOI: 10.1007/s12198-013-0133-z

Example citation: Hills, M. and McFarlane, P. (2014) Towards a higher plane of air transportation security: from hubris to knowledge. *Journal of Transportation Security.* **7**(2), pp. 115-121. 1938-7741.

It is advisable to refer to the publisher's version if you intend to cite from this work.

Version: Accepted version

Official URL: http://link.springer.com/article/10.1007%2Fs12198-013-0133-z#

http://nectar.northampton.ac.uk/7538/

NECTAR

Towards a Higher Plane of Air Transportation Security: from hubris to knowledge

V4.0

Introduction

After the colossal events of the day before—the world awoke on September 12, 2001 thinking about air transportation security in ways never before considered. The aviation industry, the security and intelligence services and scenario planners of the world were caught unaware, and, in seeking to make sense of the world we all now found ourselves in, questions - of how could and how did this happen - , were asked of those responsible for protecting our transportation systems . The crushing impact of the security failure of the day before was starkly captured by American novelist John Updike (2001), who, in an essay for *The New Yorker*, wrote that:

> The nightmare is still on. The bodies are beneath the rubble, the last-minute cell-phone calls—remarkably calm and loving, many of them—are still being reported, the sound of an airplane overhead still bears an unfamiliar menace, the thought of boarding an airplane with our old blasé blitheness keeps receding into the past. Determined men who have transposed their own lives to a martyr's afterlife can still inflict an amount of destruction that defies belief. War is conducted with a fury that requires abstraction—that turns a planeful of peaceful passengers, children included, into a missile the faceless enemy deserves. The other side has the abstractions; we have only the mundane duties of survivors—to pick up the pieces, to bury the dead, to take more precautions, to go on livin".

Air transportation security, if only temporarily—had been given *meaning*. Only two days prior, what was taken-for-granted, featured as an irritating necessity but more or less meaningless to most—was now prominent in the effects on the psyche and behaviour of millions. Yet, in 2013—to use Updike's words, the "survivors" - which includes regulators, scientists, scholars and practitioners - in taking "precautions", are still in a relative state of innocence in terms of their true knowledge that air transportation security is assured and unassailable. As security practitioners and academics, we posit that precautionary acts have, paradoxically—increased complexity and therefore opportunities to exploit already complicated security infrastructures. To fill gaps—the system has become reliant upon autonomous technological solutions and after--the-event patching of vulnerabilities. And, as for the idea that this approach somehow provides a panacea, we suggest that it is in fact part of a much wider problem, where a malevolent confidence constrains our knowledge of the complexity of the security system and therefore may likely deceive us as to its reliability.

Paltry knowledge and crossed-fingers that all's well conceals system vagaries. Revealing these vagaries before they are exploited requires that those charged with designing, managing and operatingsystems are cognisant of what security means. Many have postulated an array of interpretations and practical solutions which seek to define the meaning of air transportation security—yet, there is still no commonly held consensus.

Centuries ago, scholars tackled a similar abstract challenge.

To define the meaning of life, the Greek philosopher Plato, expressed life as the process toward acquisition of the highest form of knowledge, and when applied to aviation security, this Platonic axiom is equally relevant: security and life are mutually dependent. Consequently, without ample knowledge there would not be security—and without security there would not be life.

Practically, this means that for aviation security many lives are dependent on the active generation of knowledge continually making and remaking a system impervious to exploitation by adaptive terrorists and other threat groups (e.g. criminal conspiracies). The purpose of this essay is to provide a novel contribution to the discussion of what security means in commercial air transportation by; (i) considering why our knowledge of the trustworthiness of these crucial systems may be limited, and (ii) how—according to the Platonic axiom - our knowledge can be improved so that vulnerabilities are revealed and mitigated against before they are exploited.

Security: different in meaning and application

A few years ago, , one of the authors (McFarlane) passed through the passenger security system screening system at a London airport. Not for the first time, he was selected to stand and raise his arms while one of the newly installed body scanners determined whether he was concealing any prohibited materials, or anything that which could be used to threaten the safety of the aircraft he was about to board. Whilst standing inside the scanner, McFarlane recalls not being concerned about any risk to his health or a potential intrusion on his civil liberties. Instead, he assumed that this was was just one of the many layers of sophisticated technological security measures in the labyrinth of aviation security that, as a passenger, he would have to successfully overcome before being allowed access to the aircraft.

McFarlane noticed that, in this case, the security process was perfunctory, a well-oiled machine, with observant security operators focused upon their role and task in hand. They appeared to be taking the matter of security seriously, reassuring to a nervous flyer—and ameliorating to McFarlane's frustration that it had taken forty minutes to pass through the system.

By way of contrast, when boarding a commercial flight from a country on the African continent, the nervous traveller - that McFalane was — became alarmed. He encountered a very disorganised system of passengers being hurried through a screening checkpoint by distracted staff engaged in conversation—rather than being attentive to the images on the baggage screening device. McFarlanewas stopped and searched by hand. The search stopped when the security guard found some loose change in his pocket. Expecting to be asked to put it into a plastic tray — the guard directed that the coins be placed in his hand, which McFarlane did. To the latter's surprise, the guard put the oney in his pocket, smiled and waved him through – all the time wishing him a safe journey.

An obvious problem with security is that, and particularly so with air transportation security - —is that it generates different meanings for different people. For example—consider for yourself: travelling through both of those airports. Two entirely different experiences. Each a real world example of the disparity in the application of security. How safe would you feel? Which of the two experiences would make you feel most secure? And, which one, in your view, defines what security means? Was it, as we expect, the one at London? Why, then, is this the case? And, why is it—notwithstanding that there have been attempts, by hostile adversaries, to breach security system using airports in Africa—when we look back on the last decade, most interestingly, almost all the attempts to cause explosions on commercial transportation aircraft have been through vulnerabilities exploited in ***airports in the Western hemisphere and Europe in particular***? Arguably—these are the most secure in the world, and yet have been the source of significant, viable attacks (cf. Richard Reed; the liquid bomb plot).

To a lesser extent, an answer lies in the fact that - for terrorists - security also has its own meaning. They do not make decisions based upon gut feeling or instinct—their calculus is methodological, analytical and, as we know, potentially extremely effective in execution. In addition, for them, utility exists despite failure. Ordinarily, if devices fail to detonate or if terrorist operatives are captured or killed, then their efforts are deemed to have failed (Silke, 2010: 52) or been an embarrassment. However, the short term amplification of the reaction by the travelling and commenting public and security regulators to these, theoretically failed attacks, paradoxically, still render the terrorists' efforts successful and explains, to a point, why they have not been deterred, and rather have purposively sought to breach the highest levels of physical and technological security measures in the most defended systems in the wold.

Moreover, and to a greater extent—in air transportation security there is a paucity of knowledge. The system, remarkably, is *perceived* to be highly defended, rather than acknowledged as being permeated with latent, exploitable vulnerabilities and risk. Susceptible lawmakers, regulators—and even practitioners - have unwittingly contributed to the creation of a malign system condition where air transportation security is now far too complex. Each mode of failure (security event) has led to constant readjustment—and the creation of further (unnecessary) layers of technological defences. Erroneously, and ironically, rather than reducing the risk of future system failure—new "vulnerabilities" and "error opportunities" are unavoidably created (Dekker 2005, p.152) and become deeply buried within the intricate layers of the security system, and as such will only be discovered in *extremis*—when it is too late to act on the findings (McFarlane and Hills, 2013, p.xx).

All things considered, what is remarkable is that we know from brutal evidence (successful, thwarted and planned attacks) of this malign condition—yet our confidence remains with the very system which, at some point in the future, will again be exploited through the new vulnerabilities which have been created. The Nobel Laureate Daniel Kahneman describes this dangerous condition as *the illusion of validity*—where in our case the security system is perceived to be effective, even though we know that it is not. This condition, according to Kahneman (2011), is extremely pervasive.

There are many examples of this condition, especially, in the financial markets where people know that in principle one cannot do better than the market; but nevertheless; are confident that they are uniquely able to do so. They truly feel that they can do something which they know cannot be done, and are ambivalent to the reality that their knowledge and expertise does and can not extend to predicting the future. In aviation security, since 2001, our exposure to real world events does not appear to affect our *mis-placed* confidence in the capability of the system to prevent further attacks.

Why is this? Well, we suggest that this is because the human factor in complex systems is inherently susceptible to hubris. Hubris is dangerously parasitic—and can blind most about the true state of the condition of any system. As an example, in the 2008 financial market crash, hubris concealed a culture of reckless risk taking—which, when combined with the non-linearity and randomness of the system, fooled the powerful institutions (Taleb 2005) into believing that they were operating safely in a state of unchanged equilibrium. In hindsight, however, there is no doubt that hidden behind the *hubristic curtain* there were numerous warning signs and signals that the financial system had, over many years, become more complex and risk-laden. The overuse and reliance upon Byzantine financial instruments, and their mathematical sophistication led the financial institutions to believe that they were operating safely (Adams 2008), rather than, as was the case, recognising the danger that was fermenting within. This created an illusion which concealed latent risk, vulnerability and—a system that was not in equilibrium, but in a critical condition. The curtain enabled institutions to effectively deafen and blind themselves even to evidence that would be both compelling and comprehensible – presented, for example, by senior whistleblowers.

Sharing many characteristics - we argue that in air transportation security systems a similar pathological condition now exists. The asymmetric reliance upon complex and sophisticated technological solutions has, actuarially, determined that the security of the system has reached the point of diminishing return. The hard-wired human instinct of fear has perpetuated the increasing complexity of the system, which – akin to the example of the financial systems—has now moved toward a critical condition. This, unfortunately is only visible to some, because for the millions of people, who one way or another, are associated with the air transportation system—each of those will apply a different meaning to security and risk. Whether individually fatalists or cautious egalitarians, their meaning will be subjective in construction, drawing upon heuristic experience to delineate the threshold between fear and security. This threshold, however, is not static—it is moving and when lawmakers and regulators take snapshots—their picture is blurred.

Immediately in view is the short term fixing and repairing of the system problems that have been revealed through their exploitation. Looking further into the system, the depth of field is blurred and the security industry has not adjusted its lens to concentrate upon those technologies, decisions and processes, as we have argued, are causal to the creation of future pathogens and systems weaknesses.

Aviation security: A falsifiable proposition

The idea of falsification neatly explains the present situation which can be found in air transportation security. It is only when the system is engaged and exploited by the actions of terrorists or other threat groups—that the meaning of security cease to be merely theoretical and abstract. Equally it is only when this occurs—even if only for a short time - that the true extent (and limitations) of our knowledge concerninng the effectiveness of the system is revealed. The philosopher Karl Popper was one of the most influential thinkers of the twentieth century, and in his book—*The Logic of Scientific Discovery*, distills the deductive notion of "falsifiability" (2002, p.57). Scientists, in seeking to understand particular phenomena, hypothesise theoretical explanations which are subject to the test of falsifiability. If, by empirical observation (reality), the hypothesis cannot be falsified then the proposition remains valid. Conversely, if it is rebutted, then the explanation provided by the proposition is dispatched into obscurity.

For this reason, the development of our knowledge of security is limited to this deductive principle. *Unnecessarily, we wait until the system has been breached, and only then accept that the proposition that that the system is secure has been falsified.* The system designers then have to quickly adapt the existing or develop a further system which is once again then made subject to this test. Something that the industry is yet to fully embrace is the concept of constant testing – in the same way that a critical computer system is protected by the challenge of robust (but ultimately friendly) attack and the immune system by exposure to pathogens. Without doing this, air transportation security will continue to be nothing more than ephemeral in meaning—an abstract concept—a Kahneman type illusion—a hypothesis of a system condition, which reinforces belief of the effectiveness of the system. Nevertheless, there is an advantage to be gained by considering air transportation security from this perspective because we are forced to think about it within the realm of empirical science. And, by doing so we can benefit from the appreciations of this approach to develop knowledge—in advance of waiting for the system to be tested by falsification.

Final Thoughts

By adopting the credo that systems such as those that comprise air transportation security should not be allowed to have their vulnerabilities demonstrated by exploitation, the answer, therefore, as to whether our knowledge of air transportation security is of the highest form—is for us, as practitioners and academics, clear cut. In tackling a similar challenge, it was the famous scientist, Peter Medawar (1967, p.97) who observed that:

> No scientist is admired for failing in the attempt to solve problems that lie beyond his competence. If politics is the art of the possible, research is the art of the soluble. Both are immensely practical minded affairs. Good scientists study the most important problems they think they can solve. It is after all, their professional business to solve problems, not merely to grapple with them.

This dictum compliments that of the terrorism analysts Schmid and Jongman (2005: 179) who said that: “The researcher should not confuse his roles. His role is not to fight the terrorist fire; rather than a fire-fighter; he should become a student of combustion". In air transportation security—we have yet to become students of combustion: in order for there to be fire, what components are required? As well as intent, for example, there needs to be opportunity to effect an aviation transportation security breach. Opportunities can be latent as well as generated, but both can and should be detectable as either will leave traces of some kind of change. We are still distracted—grappling with perceived problems that are not the real problems: plugging a revealed gap with policies and their technical solutions does nothing more than (at best) divert attention to a less hardened target.. We should instead be solving the very problems that are being sought by terrorists, to use existing scientific knowledge and method to mitigate system criticality, weakness and vulnerability. These problems are not insurmountable. They are not "Black Swan" (Taleb xxxx) improbable occurrences, but are a failure of security systems to identify that it (now) has ineffective countermeasures to mitigate vulnerability and weakness (Woods 2006, p.24; McFarlane and Hills, 2013). For the time being—this provides an advantage because terrorists have the knowledge to exploit vulnerabilities and weakness before we are able to identify, design and mitigate them out of the system. However, this is not entirely a reason to be pessimistic, s the challenge is one of working with systems designers, intelligence analysts, grassroots employees, network administratrs and others in order to acquire and make sense of actually available knowledge. We do not have to wait for greater scientific understanding or new theories - these problems are all potentially soluble by existing theoretical paradigms.

Adams (xxxx) Emeritus Professor of Geography at University College London, and a world expert in the study of risk -aking behaviour, makes a similar connection between an identical risk that is known and visible to some—and concealed by uncertainty and complexity others. To do so, he describes the unfortunate drunk who searches for his keys, not in the dark where he actually dropped them, but only under the lamppost where he can see. Presently, lawmakers, regulators and system designers only look in the well-lit areas—in front of the illusory and hubristic curtain. The risk is actually behind—concealed in darkness amongst the intricacies and vagaries of the system where we need to look. It is this area which conceals the ongoing active (purposive) and passive (accidental) creation and incubation of system vulnerabilities and weakness. It is only when we change where we look that (i) we will attain the higher forms of knowledge, and (ii) then understand what security in air transportation really means. We can then apply this knowledge scientifically and, in the words of Schmid and Jongman (2005: 179) and Medawar (1967, p.97), become "students of combustion" and understand how to "solve problems, not merely to grapple with them".

Finally, as professionals in and students of security we are practiced at analysing the effectiveness of security systems. When we consider what security means–we can only conclude that, in principle, air transportation security, however infuriatingly, is still essentially the same system which preceded 9/11. This is a problem that will continue to play out in the same way for decades to come, and only when we attain the highest form of knowledge will we have the capability to overcome the challenge posed by adaptive adversaries – identifying those who are already 'in the machine', where they could even be modifying the machine so that it continues to tell us what we wish to believe – whilst it is actually – like a Botnet – actually under the command and control, or at least heavy influence, of others. We have not learned from the meaning that they have, many times now, attributed to security. And, until that changes, the future will inevitably be written again, by authors like Updike—in terms of the colossal events of the day before.

References

Medwar, P. (1969) The art of the soluble: creativity and originality in science. Meuthen: London