Technical Intelligence and the Operational Art*

James B. Longley[1]
DIRITECH, LLC, 6 Abby Lane, Yarmouth, ME 04096-8115

**EDITOR'S NOTE: The following is essentially the text of the keynote address by the Hon. J. B. Longley to the first workshop on Passive and Active Signatures at the 2009 SPIE DSS Meeting.*

ABSTRACT

The scientific method applies to more than science or technology. It has application equally to processes of technical development, invention, innovation, communications, practical application and, ultimately, operations. Differences between the practice of pure science and the themes of effective operations exist only in terms of the ultimate objective and the standards by which success is measured. The standard for science is proof of concept; the standard for operations is a particular utility or effectiveness in solving an operational problem. The scientific method is ideally able to manage each process against distinct objectives and still achieve the desired success. This paper discusses the tension between the two orientations and argues for the application of the scientific method to the urgent need for changes to obsolete organizational structures and processes that impede the effective implementation of new capabilities into operations. This must occur even as, simultaneously, we must operate within these obsolete structures to achieve the transition results we desire.

Keywords: Technical Intelligence, Measurement and Signature Intelligence (MASINT), Signatures, Technology, Applications, Invention, Communications, Transition, Innovation, Operations.

1. INTRODUCTION

It is said that much of history is a battle between the forces of 'order' and 'disorder'. Not to oversimplify, 'order' seeks to achieve degrees of standardization, even perfection, while those confronted with 'disorder' tend to accept the premise that perfection is impossible, and diversity of experience a given, and focus on the *management* of tumult rather than seeking its elimination.

These are abstract concepts that can take the form of contrasts based on theoretically-driven conceptions of an "ideal against more mundane considerations of "practicality" based on perception of "reality" or a judgment of 'What's good enough' as a solution to a particular problem. These 'opposites' are part of the wide continuum that can divide the scientist and the perceived 'realist' even as they each pursue strikingly similar objectives managed against vastly different standards. It all depends on the objective: *Is one seeking to 'prove' a process? Or just 'make it work'?* Yet, often, we ignore the distinctions then are surprised when the evaluations are contested.

Our 'forgetfulness' over these distinctions ignores that our ability to measure or evaluate any activity can, depending on whether the perspective is *science*- or *operationally*- based, vary greatly. More troubling, we can also fail to acknowledge that the differences can be highly complementary. This can easily add to confusion in our understanding of the problem as we fail to distinguish between what appear to be two relatively simple and straightforward processes.

Also, recall that, in our culture, the desire for human perfection goes back to the earliest passages in the Book of Genesis extolling the temptation of Adam in the Garden of Eden. In addition, to the extent that science has followed closely behind religious belief, the desire to merge 'magic' and science is evidenced by millennia of experience with alchemy

Atmospheric Propagation VI, edited by Linda M. Wasiczko Thomas, G. Charmaine Gilbreath,
Proc. of SPIE Vol. 7324, 73240Q · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.822544

and experiments to turn lead into gold, even the desire for "eternal youth". This is not to say that science hasn't achieved what can only be described as miracles. The battle to prevent aging, for instance, today focuses attention on the science of Botox but history is replete with legends and folk wisdom along the lines of Ponce de Leon's fruitless search for a 'fountain of youth' in Florida in the early 1600s and similar excursions over time.

What is clear is that, despite the expenditure of significant energy and resource, every effort to 'turn back time' experiences nothing but failure or death and, at least in the case of human beings, *always both*. This is the blunt contrast between goals of idealistic perfection and practical, often unpleasant, reality.

Again, what's notable is the tendency to ignore the polar differences in approach even as we express surprise that the standards of success for a scientist and an operator are different.

Yet, even as dreams *do* inform science, hard-earned experience, especially the scientific method, introduces reality into our personal and professional equations to the benefit of our 'science'. And, even as the process of 'reconciling' scientific goals with reality has produced outstanding achievement in our laboratories, the degrees to which those same ideas can achieve practical utility in the real, work-a-day world can also be successfully managed but through the recognition that the discipline of the scientific method applies to far more than just science.

Nor is this our only challenge. In present times, in addition to the challenge of reconciling dreams with reality (or however we delineate the polar opposites of 'order' with 'disorder', perfection with imperfection, etc.), we now face the added difficulty of doing so in the midst of a transition from an information infrastructure still permeated with attitudes shaped by five centuries ago by the 'linear', 'mechanical', technology of Johannes Gutenberg (1398-1468) as it is now being overwhelmed by the 'spatial', 'electronic'-media of our more modern era.

Many recognize Gutenberg as the 'innovator of the millennium' for his merger of the technologies of the wine-press, ink and smelting to produce the concept of moveable type in his new system of printing. Yet, five centuries later, the pervasive impact of a social and organization structure shaped by a Gutenberg-era information infrastructure consisting of '*letters-in-sequence*' forming '*words-in-sequence'* forming '*sentences-in-sequence'* forming '*paragraphs-in sequence'*, etc., and leading to layer-on-layer of hierarchical management structures is still poorly understood. More so the subtle, but pervasive impact of that structure on society and culture as every aspect of education, learning and social activity actively embraced this largely-linear system of expressing and managing information.

Modern electronic technology has turned this thinking on its ear as existing organizational structures, based on five centuries of linear organization, and now confronted with the wonders of computers and the internet, has sought to embrace the new technologies even as it failed to comprehend the changes in organizational capability that the new technologies brought.

It is beyond the scale of this effort to address this phenomena except to pose the question that, assuming that the major priority of social, business, governmental or other organizations is the management of information, shouldn't the exponential increase in individual capability brought about by the computer and the internet have at least some impact on our modes of organization?

The shift from the linear, mechanical approaches of the Gutenberg-era began brewing as our understanding of electricity began to take shape, especially in the last two-hundred-fifty (250) years following Benjamin Franklin's (17096-1790) experiments with his kite and began to escalate slowly with the development of the electronic telegraph in 1843 and later nineteenth-century developments in audio and visual technologies. More recently, they are now exploding in full force on society as the speed and informational and computational power of modern computers and the internet are now generating exponential increases in the *quality*, *quantity* and *velocity* of the *aural*, *visual* and *textual* information routinely available.

Where Gutenberg provided the means for the public to transgress the domains of clergy and the elite, modern electronics has introduced a level of capability that now threaten to overwhelm every last vestige of existing, legacy-oriented state- or structure-based authority.

There has been a saying in management circles for some time that, "If you don't know where you are going, any road will take you there." The modern corollary is that, today, if you do not know where you are going, any road will take you there *at the speed of light*.

So we have two more challenges to contend with: not only 'knowing where we're going' but the additional requirement that we go there 'at speeds faster than any humans have ever known', speeds barely comprehensible in terms of the legacy organizations and information infrastructure with which we must contend on a daily basis.

To summarize, to the difficulties of 'crossing the barrier' between science and operations, there is now the added challenge of implementing entirely new capabilities premised on electronic capabilities hitherto unknown and doing so into pre-existing organizational and mission infrastructures premised on obsolete organizational concepts based on non-electronic technologies and our tendency to make these decisions by habit and not design. If the true capabilities of our new concepts were fully understood, they could inspire entirely new missions, not just modify the tactics of the old. The challenge is further compounded, even as the new ideas are absorbed, as the linear structures not only fail to comprehend the profundity of the scale of change they are now encompassing, they resist it mightily.

2. MODELS IN COLLISION

Winston Churchill once observed that Great Britain and the United States were, "two great countries divided by a common language." In so many words, this accurately describes the parallel relationship between science and technology, especially technical intelligence, and the use of science to 'prove' a concept, as opposed to the realities of applying those concepts to unique, often irrational practical situations that might occur in the operational world where, as we have already said, proof of concept lies less in the science and more in its practical utility. As very similar as they are in many ways, they are vastly different in others.

On an abstract level, there are many important reasons for these differences. Science, by and large, is concerned with an objective, disinterested search for 'truth' or, for our purposes, an accurate understanding of a certain phenomena. Those who must effectively employ or face the effects of the phenomena, however, are far less interested in a disinterested and abstract understanding of the subject than they are with the highly subjective perspective of its possible immediate utility to them especially as it pertains to some immediate objective. The concern is less a desire to achieve an 'ordered' understanding of the subject itself that it is in employing that science for the purposes of applying it to some other disorder often remote from the science itself. In simple terms, the former seeks what is logical; the latter, what is practical and useful.

By necessity, science seeks a very high standard of technical and theoretical accuracy and goes to great lengths to pursue it. Time can be less of a factor than accuracy. Operators, on the other hand, are far less involved with theory, or the science involved in pursuit of a theory, and are far more concerned with the mundane reality of an idea's utility and effectiveness in actual practice in solving a problem. Time is often an immediate, even urgent consideration; in an operational environment, time can also, literally, be a life-or-death matter.

Yet, both are similar as the task confronting those engaged in either aspect have the responsibility of performing to the expectations of the standards set.

As we explore these thoughts, let us consider several situations that have recently been publicly reported–one does not have to look very far to find them. The differences between science and operations, however, and the concept and execution inherent in each, appear to have been substantially misunderstood.

2.1 Examples of Contemporary Technical and Operational 'Mismatches'

There has been an ongoing series of especially compelling technical and operational 'mismatches' reported in the public press in recent months. Some of these situations include:

> *Space News* reported in March that U.S. Special Operations Forces in Iraq and Afghanistan "often carry two GPS terminals: a commercially procured system and the military-issued receiver capable of using the encrypted (data) code." It seems that one is made to military specifications over a five year development cycle while the other, a commercially-developed model, has a *one-year* cycle. As *Space News* reports, "One official said many troops refused to carry the military-issued terminals, sticking with commercial models because they are easier to use, lighter in weight and feature longer battery life." The unnamed military official was quoted as stating, "The bottom line is the soldier in the field is going to use what is easiest for him." The article concludes that "*the*

nature of military procurement" and the need for encryption will keep military gear "forever behind the consumer cycle", according to the "U.S. military and GPS experts" cited. (Emphasis added.) (1)

USA Today reported on April 15 in a 'Page One' story that a $250 Million program initiated in 2002, in consequence of 9/11 and designed to secure the nation's seaports, had required workers to spend $132 apiece for "high-tech ID cards that have their fingerprints embedded in them". Unfortunately, the ID cards have been issued but working fingerprint scanners have not been installed in time to use the cards. As the paper reported, "...more time was needed to make sure the readers work". In the meantime, if the article is correct, 1.2 million workers have spent $158 million spent to obtain the special, expensive cards with no readers to read them. (2) A U.S. Congressman, Representative Bennie Thompson of Mississippi was quoted as stating, "Most people would say it's real dumb to have security cards that rely so much on technology and yet you fail to provide a reader for the card." (3)

Modern Piracy: Last November, the author witnessed a senior U.S. maritime official comment on the increased pace of pirate attacks off the coast of Somalia. He downplayed the problem and referred to it as "cost of doing business" for the commercial maritime shipping community. In fairness to the commentator, his views reflected a prevailing view in the Defense Department and the Navy that is not interested in taking action to solve the problem. Far more effective, in their viewpoint, is to let commercial interests in the maritime and insurance communities sort the issue out for themselves. That view, of course, came to a significant 'bump' in the road, so to speak, for both the Navy and the pirates with the failed attempt to capture the *M.V. Maersk Alabama*. In desperation, the pirates, however, took the *Alabama's* Captain, Richard Phillips of Vermont, hostage. He was rescued four days later. (4)

In commenting on the pirate's failure to capture the ship, John Robb wrote sardonically, "Dead in the water, the pirates adapt, take the captain hostage and flee the ship. They negotiate for his release via satellite phone. For small violent groups interested in making a buck, the global economy is just a phone call away." (5)

Even as a naval view of matters might appear to be that piracy is a *commercial* problem, from the commercial perspective, actively dealing with the challenge of crew-based initiatives or military actions to protect ships poses an unacceptable risk to the crew if not the financial interests of the carrier. Needless to say, these concerns, or lack thereof, is of small consolation to the crews of the eighteen (18) seized ships--and three-hundred-twenty (320) sailors—seized and being held hostage by pirate warlords in Somalia as of April 15, 2009. (6) Whether our naval and maritime interests appear to recognize the concern or not, certainly the American public can be presumed to have an interest in the principles of safe passage and open seas. (7)

Neither the seizure of the *Alabama*, nor the public concern that innocent mariners were being seized on the high seas, were unprecedented. Piracy, one might think, can be anticipated. What cannot be accepted, however, is the notion that such acts are not preventable, or, if not prevented, capable of resolution in the interest of the public. As one opinion writer suggested, "...ultimately the goal should be to prevent hijackings, not rescue hostages". It is not that we do not have the tools to deal with the problem, it is that those charged with the problem have been unwilling to use them or make the doctrinal adjustments in our operational theories necessary to accommodate the practical situations we have encountered. (8)

2.2 Examples of Possibly More Substantive, Technical and Organizational 'Mismatches'

What are being presented daily as routine examples of technical and operational mismanagement and/or miscalculation, however, could be indicative of a far more troubling, and substantive, lack of appreciation of the scale of change we are enduring. The examples cited above are the 'tip' of the management iceberg. Other, far more consequential events in the last ten years, at a minimum, might raise the question of whether we have attained a level of *national* vulnerability on these matters with social and cultural roots far deeper than most may appreciate.

On September 11, 2001 (9/11) nearly 3,000 innocents were killed as the result of terrorist attack. As we shall see, there are clear suggestions that the attack might have been prevented, or its consequences moderated, but for certain actions taken or not taken. There may also be a trend: Since 9/11, and beginning with the natural disaster of Hurricane Katrina, we have witnessed a series of situations ranging from failures in the organization and management of the occupation of Iraq, including the failure to find Weapons of Mass Destruction (WMD) and the difficulties experienced in providing the proper equipment for our troops in combating "Improvised Explosive Devices (IEDs). More recently, we experienced the near-'meltdown' of our financial system with an accompanying expenditures of hundreds of billions of dollars in a

desire to 'stabilize' the financial system. Then, only several months ago, another terror attack, costing the lives of one-hundred-and-eighty persons, occurred in Mumbai, India.

What has been missing in each of these situations has been an honest evaluation of whether the technical capabilities we employed in each situation—*before, during and after*—were adequate to the operational tasks to which they were assigned and, if they were not, was it a result of a *technical* or an *operational* deficiency? Was the technology 'proven' or, more practically-speaking, did it 'work' when it was called on? And, if it was an operational deficiency, was it the result of a 'mismatch' between the idea and the technology? Or was there a 'mismatch' between the technology and the organization and operation? Or, more troubling, was the technology ahead of the organizational thinking by which the operation was conducted? Certainly, there can be factors relating to human or management 'mistakes' but the really serious question is, 'Was the implementation of the technology appropriately embraced or were there possibly more challenging organizational circumstances in play, beyond our ordinary understanding of management and operational principles?'

It is important to understand that as we develop new technical capabilities, pathetically little thought goes into the question of whether the organizational construct within which the 'operation' will be conducted is adequate to utilize the new capability. Indeed, in failing to confront these concepts, we are inclined to take new ideas and apply them reflexively, by habit, rather than thoughtfully and by design.

For purposes of this paper, let us concentrate on Mumbai and 9/11.

Mumbai: On November 29, 2008, ten terrorists arrived by boat and, in the course of a three-day terror spree, "attacked two luxury hotels, a train station, a Jewish cultural center and other sites" in Mumbai, India, killing some one-hundred-and-seventy civilians, including a number of law enforcement and security officers. (9) According to the New York Times, "Several high-ranking law enforcement officials, including the chief of the anti-terrorism squad and a commissioner of police, were reported killed." (10) According to Bill Roggio, "The Mumbai police paid a heavy price. Early in the fight, the attackers killed the chief of Mumbai's Anti-terrorism Squad and two other senior officials. At least 14 police were reported to have been killed during fighting throughout the city." (11)

Within literally days, even hours, of the attack, a number of technical and operations experts 'pieced' together reports from news accounts, drawing a number of conclusions concerning aspects of the attack. The author reported on December 2, 2008, that John Robb, an Air Force veteran of the special operations community had summarized the ability of the Mumbai terrorists to use readily available, off-the-shelf technology to mount their vicious attack. Robb cited Blackberrys used in real time to, apparently, hack into and monitor the police response to the carnage and to activate cell phones to coordinate tactics. Notably, after cable television lines into the building were cut, the attackers accessed local and worldwide media coverage, including the forces mounted against them, over the internet. E-mail was sent to taunt the local media (and the public). (12) The terrorists phoned news and television stations to make their demands regarding "releasing jihadis from jail" or appealing for support for Kashmiri separatists. (13)

Robb, an Air Force veteran of the Special Operations Community and the author of Brave New War, wrote, "…these guerrillas were better connected to both the tactical and strategic environment than any US and other developed nation military personnel have ever been." (14) Noah Shachtman of Wired.com reminded us of former U.S. Central Command chief, Gen. John Abizaid's complaint that, "with their Radio Shack stockpile of communications gear, this enemy is better networked than we are." (15)

An early report indicated that, in accord with previously identified procedures in such situations, authorities acted to "cut off" the terrorist's access to outside news and press reports by cutting the cable carrying television channels into the hotel. In this case, however, the terrorists were actually bypassing the cable system and directly accessing that same information in real-time *through their cell phones*. (16)

"… It was the use of humble mobile phones and internet technology that proved a key weapon – one which caught the antiterrorist forces by surprise… The use of Blackberrys by the terrorists to monitor international reaction to the atrocities, and to check on the police response via the Internet, provided further evidence of the highly organized and sophisticated nature of the attacks… The gunmen were able to trawl the internet for information after cable feeds to the two luxury hotels and office block were cut by the authorities." (17)

Other technical innovations were demonstrated. The ten attackers not only communicated with each other by cell phone, they were in near-constant communication with an external 'handler', "probably in Pakistan", who was giving orders to the attackers and actively monitoring media reports, simultaneously relaying critical, real-time operational information derived from the media on the movement of law enforcement and security personnel marshalling against the attack. (18)

Some two months after the actual attack in Mumbai, India, the *Washington Post* covered the release of a Pakistani government report that, in a number of direct ways, confirmed the early comments of the Courier-Mail, Noah Shactman and this author that the technical sophistication and global reach of the attackers demonstrated previously unknown capabilities that badly outmaneuvered the abilities of the Mumbai and Indian government public safety agencies to respond. The *Post* quoted Pakistan's interior minister, Rehman Malik as stating that the terrorists, "communicated (in real time) using Internet telephone accounts… The Internet phone calls between the terrorists were set up by a militant operating from Barcelona, who was later lured to Pakistan on a pretext and arrested". The Post reported that, "Investigators traced a $238 payment from a Spanish account to purchase a domain name registered in Houston. Another was registered in Russia. A satellite phone used in the attacks was registered 'in a Middle Eastern country,' Malik said. Malik also said that Austrian SIM (subscriber identity module) cards allowing the transfer of data between phones were used by some of the alleged conspirators. (19) The same news report indicated that the ability of the United States to access information concerning the attack both prior to, and after-the-fact, exceeded that of comparable Indian government authorities. (20) Indeed, U.S. news reports indicated that U.S. intelligence agencies warned their Indian counter-parts in mid-October of a surprise attack." (21)

9/11: Ironically, the actual facts in the U.S. on September 11, 2001, may have been different but the lessons in failure to understand and appreciate the operational possibilities attendant with diverse technologies offer somewhat similar lessons. '9/11' actually began in Portland, Maine. Alleged ring-leader, Mohamed Atta and his co-conspirator, Abdul Aziz al Omari, had traveled to Portland from Boston the night before. Following an early morning wake-up call, they arrived at the Portland, Maine airport for a scheduled early-morning, 6:00 AM departure aboard a small commuter aircraft flying from Portland to Boston. (22)

The reasons for Atta's choice of a departure through Portland has been the subject of considerable but it is now widely assumed that he flew through Portland for two primary reasons. First, for command and control considerations, he and his partner wished to remain separate from the other members of the four teams under Atta's control. This was probably intended, however, to protect his ability to maintain situational awareness and command and control as he made the "go" or "no go" decision for the operation. (23)

While there is no conclusive evidence as to why Atta and al Omari chose to begin their day with a flight from Portland, there is strong supposition that they did so because it the closest non-stop flight into Boston that would arrive in time to effect a transfer onto the ill-fated, Boston-Los Angeles flight that was due to depart at 7:45 AM that morning. That flight would also be the first aircraft to crash into New York City's Twin Towers that morning. In connection with the objective of boarding that flight following his arrival in Boston, he also planned to obtain his boarding pass for the Boston-LA flight prior to boarding his aircraft in Portland. It is a safe assumption that, in obtaining a boarding pass for the later flight, he hoped to shift any risk of discovery or resulting delay to the earlier time in Portland. This would be consistent with sound operational planning. A footnote in the "*The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*"(hereinafter, '*The 9/11 Commission Report'* or, more informally, 'the Report') validates this hypothesis by disclosing that "Atta reacted negatively when informed in Portland that he would have to check in again in Boston." (24)

In evaluating the terrorist's choice of airport, the Commission Report discloses that, "Nothing stands out about any of (the airports) with respect to the only security layer that was relevant to the actual hijackings: checkpoint screening." (25) On arrival at the airport, Atta was randomly selected by the Computer Assisted Passenger Prescreening System (CAPPS) designed "to identify passengers who should be subject to special security measures." (26) Under security rules in place at the time, the only consequence of Atta's selection by CAPPS was that his checked bags were held off the plane until it was confirmed that he had boarded the aircraft. (27) The same rule and procedures also applied to the others identified by that system. (28)

In addition to Atta, another nine hijackers were identified in the CAPPS system for a total of ten out of the nineteen hijackers. Fifty-two percent were identified by the CAPPS system. On the two American Airlines planes alone, nine out of ten hijackers—ninety percent (90%)—were identified by the CAPPS system. Several others not in either group were also selected for extra scrutiny based on lack of identification, failure to answer the required questions or for, in general,

acting in a suspicious manner. Indeed, several customer service representatives were to reach this conclusion. Several hijackers also set off the metal detector and were re-tested or hand-wanded; one failed the metal detector multiple times before being hand-wanded and pushed through security. As *The 9/11 Commission Report* indicated, some of these measures encompassed asking standard security questions until correct answers were elicited. (29) Per the applicable regulations in force on the day of the attack, American Airline ticket agents were specifically required to indicate those passengers who did not provide correct answers to security questions, did not have proper identification, or who met other criteria not indicated in the Report. (30)

3. OBSERVATIONS

A recent announcement of an upcoming space conference carried a curious line. It said that "breakthroughs in component technologies often act as key enablers of new mission capabilities." (31) This raises an intriguing question: "Do the 'breakthroughs' reference "new mission *capabilities*"? Or, perhaps, do the 'breakthroughs' suggest the possibility of "new *missions*" enabled by the new capabilities?

This is part of the challenge that this paper seeks to address. In pioneering the development of new ideas, it is important that the concepts be proven scientifically, i.e. in accord with the principles of the scientific method. At the same time, the scientific method has application in the transition to the user in that, having proven a new concept, a new process begins all over again as we seek to effectively employ the new capability.

We also certainly understand that science and technology can better perform existing missions but at what point do we consider whether they might actually enable new missions? Do we apply 'new mission capabilities' to *old* missions out of reflexive habit? Or do we apply them by design? In the process—and assuming there *is* a 'process' to evaluate these considerations—do we even raise the question of how new capabilities might actually make entirely *new* missions possible? How do we address this dilemma?

In some of the earlier examples mentioned we have observed several specific "mis-matches". In the case of government officials defending a five year development cycle for a military GPS receiver that the troops only use when they have no other choice contrasts sharply with a more effective commercial approach that can perform the same function in one-fifth the time and producing a far more user-friendly product in the process, there is an obvious conflict. Even acknowledging that military requirements can be more stringent, *four more years* to develop a similar product seems extreme. Even then, the government is not succeeding in making it useful to the soldier.

Furthermore, given an attitude that piracy is "just a cost of doing business", and a long history of freedom of the seas courtesy of the U.S. Navy, it would appear that military 'convenience' has been confused for a maritime 'policy'. To suggest that we should tolerate piratical interference with principles of open seas and safe passage when we have the military resources to prevent it, merely because the cost of enforcing freedom of the seas should be "a cost of doing business" for someone else is equally absurd.

In the case of the thumbprint scanners, it is difficult to precisely determine what part of the process is at fault but it appears that the flawed development of the technology now competes with the lack of management of the acquisition process for the highest degree of failure.

In each of these cases, it appears that serious flaws in the analytical and management approaches of the existing processes and organizations occurred, compounded by what can only be characterized as an inadequate commitment to the successful development or fielding of the desired operational capability.

The 9/11 Commission Report indicated that, "By 8:00 AM on the morning of Tuesday, September 11, 2001, (the terrorists) had defeated all the layers that America's civil aviation security system then had in place to prevent a hijacking."(32) More troubling is that, having drawn this very dramatic conclusion, the report contained the additionally startling observation that, *"Nothing stands out with respect to any of (the hijackers) with the only security layer that was relevant to the actual hijackings: checkpoint screening."* (33)

Needless to say, our own review of the facts reaches a profoundly different conclusion. It is even quite safe to volunteer that the most important information in the entire report could be said to exist on only *the first four, brief pages* covering the passage of the nineteen hijackers into and through the security systems of three different airports and onto the four fateful aircraft. The fact of this single, massive failure alone, is cause for far more serious scrutiny that as been contemplated to date. (34)

The technical means available at each airport were extensive and consisted, at a minimum, of the aforesaid, Computer Assisted Passenger Pre-screening System (the 'CAPPS' system), the metal detector and X-ray machines. In addition, voluminous federal and airline procedures and regulations governed nearly every action of the customer service and security personnel present in obsessive detail.

The *9/11 Commission Report* documents that, with the exception of Mohamed Atta, ten of the nineteen were largely identified *before* they even arrived at the airport. In addition, several other hijackers either could not answer the security questions or acted suspiciously and attracted the specific attention of airline customer service personnel. If that was not enough, there were other aspects of the hijacker's personal behavior that attracted attention. The ringleader, Atta, "reacted negatively" in Portland when told that he could not, as he had expected, obtain a boarding pass for his Boston-Los Angeles flight. It is likely that he had planned his mission carefully and fully expected to receive the pass as he was passing through Portland in order to minimize any scrutiny he might receive in Boston. Several customer service representatives noticed suspicious behavior, including Atta's. (35)

As we've already noted, several of the hijackers set off metal detectors and were re-tested or hand-wanded with one actually failing the metal detector test several times before being hand-wanded before being, in the author's opinion, "pushed through security". One did not even have photo identification. As the Report indicates, several hijackers "had trouble understanding the standard security questions", and the United ticket agent, a patient soul, in the words of the report, "had to go over (the questions) slowly until they gave the routine, reassuring answers." (36)

The *9/11Commission Report* even appears to acknowledge the futility of an approach based on the use of the standard questions without commenting on the highly troubling significance of that observation. In a footnote, it adds, that "Even had the hijackers been unable to understand and answer the two standard security questions, the only consequence would have been the screening of their carry-on and checked bags for explosives." (37)

4. LESSONS

Each of these situations, especially the examples of Mumbai and 9/11, remind us of the importance of the human powers of observation, analysis, judgment and action. That, whether it is the pursuit of scientific clarity or operational utility, it is those powers that enable us to find and review the facts and information at our disposal to make effective decisions. That any system is doomed to failure if it is designed based on outdated assumptions, as in the case of the Mumbai attacks, or based on incorrect assumptions and designed to blindly impose arbitrary rules in the absence of human judgment. This observation also underscores the importance of human judgment whether in the lab, on the security line or in any operational environment.

In the case of the Mumbai attacks, we see a clear example of the situation that can occur when the technical capabilities developed are not matched by the operational strategies used. There are numerous examples of this: the early warnings provided by signals intelligence were not so much ignored as they were misunderstood. Public service agencies—as personally brave and committed to their mission as they were—were no match for terrorists using cell phones and the internet in a manner that security personnel should have, but did not, anticipate. It is a tried and true security principle that it is not the adversary's *intent* that matters; it is his or her *capabilities*. *If it is conceivable, it is possible*; it is just that simple.

In any process of development or operationalization of a technical capability, a fair analysis has to be made of the extent to which the needs and values of those who would operate the capability needs to be brought into consideration in the transition. To use a simple analogy, would it make any sense to develop, say, an automobile and give it to someone without teaching them how to use it? The same is true for any technology.

Any system can only find that for which it is designed to look. Given that the security screening system in effect on 9/11 was designed to intercept *only* those weapons or explosives that a terrorist was expected to carry, and a terrorist were carrying something different like, say, a box-cutter, it did not matter. In short, the system was not designed to intercept people; it was designed to intercept *things*. This flawed approach carried over into the management of those responsible for the operation of the system. Those responsible for the system design clearly had no confidence in the judgment of those to whom they entrusted with its operation; customer service personnel and screeners were viewed as mere 'functionaries" in the process and given specific tasks and instructions as to how to respond in nearly every situation. Far be it for anyone to use their judgment; 'higher authorities' were always 'in charge'. This serious form of contempt was only reciprocated by the operators.

It is also important to understand that an essential element of the screening "technology" in effect on September 11 was a regulatory system was intended to 'trump' any technical or human interface. In the process, the essential human-in-the-loop was minimized, if not destroyed. There were a number of instances where capable personnel with suspicions as to the behavior of others were not only not able to act on their observations, they were prohibited from doing so by the specificity of the rules under which they operated. It was the 'rules', not possible terror 'acts' or 'consequences', that mattered.

It would be too much to say that the attitude of customer and security personnel was "casual" but the same is not true of the regulations. Despite the highly advanced computer and software systems, metal detectors and magnetometers, the expectations of federal and airline authorities can only be described as primitive, even demeaning.

One would think that a pre-identification of ten of the nineteen suspects through the CAPPS system was an exceptional result. Despite the high level of apparent sophistication, however, *there was no regard whatsoever for the judgment and experience of the personnel utilizing this, or for that matter, any other systems*. Once a pre-identification was made, the actions that a customer representative could take were extremely limited. In the case of Atta, action was restricted to a requirement that his checked bags be held off the plane until it was confirmed that he had boarded the aircraft. (38) In the case of the other ten, the same rule and procedures applied. The selection in CAPPS, in fact, had absolutely nothing to do with checkpoint screening; it only imposed specific restrictions on the handling of their baggage. (39) The elaborate 'processes' followed in the case of the magnetometer and the X-ray machine, and the hand-wanding or bag checks employed, were not much different in their philosophy. The sole purpose of the screening was to "identify and confiscate weapons and other items prohibited from being carried on a commercial flight." (40) In short, if you were on the security screening force, and you were looking for a terrorist, you were in the wrong place. The policies in force then and now were designed to prevent such misbehavior; indeed, even making such a judgment was a cause for concern. (41)

Given what we now know actually happened, it strains the mind to consider the Report's refrain that, "<u>None of the checkpoint supervisors recalled the hijackers or reported anything suspicious regarding their screening</u>." (42) It is equally straining to consider that a later investigation by the Federal Aviation Administration determined that <u>none of the gate security personnel were even aware that any of the terrorists passing through their checkpoints had been identified by the CAPPS system</u>. In the words of the Report, "…the screeners recalled nothing out of the ordinary. [The screeners] could not recall that any of the passengers they screened were CAPPS selectees." (43)

It is quite clear that platoons of customer service representatives and screeners reinforced with an extensive, thorough and effective system of computers and screening technologies were in place on September 11, 2001. It just was not anyone's job to find terrorists. (44)

5. CONCLUSIONS

It is not my purpose to present an exposition of scientific principles here but there are several important, and quite basic, statements about science, operations and life, that are instructive. We have reviewed conclusive evidence of technical capabilities either mismanaged, misunderstood or ignored either in the development or operational phase. No example is more startling, however, than the extensive capabilities arrayed to defeat the threat of a terrorist attack on September 11 yet placed into an operational environment wherein the management structure, by design, prevented its effective utilization. Worse, where these failures were essentially ignored and left completely unscrutinized.

In every example covered in this paper, whether it was problems arising from deficient military GPS systems, the failure to acquire thumbprint scanners or piracy off the coast of Africa, or the far more serious attacks on Mumbai or on our own shores on September 11, 2001, the human factor provided the decisive factor in the outcome of the situation. There has been a pervasive tendency in our government to place its faith in the presumed *science* of security rather than its more difficult cousin, the art and reality of its effective application. An emphasis was on the role of 'rules' rather than the role of people. It is fairly clear to even a casual observer: *a thinking enemy will always outwit an unthinking bureaucracy* and that was never more true than on 9/11. On that day, there were dozens of person-to-person encounters wherein good people with little in the way of rank or position were able to notice behaviors that called for action yet their ability to do so was constrained severely. To the extent that we fail to respect others, and seek to control their ability to think for themselves, or worse, demean their human dignity by subject them to unthinking sets of regulations, we are asking for trouble. We have paid a stiff price for these failures in our past and we will pay a stiffer price yet, if we fail to correct this mistake for the future.

Our scientific and technical abilities and procedures provide a unique basis on which to develop the operational models that we need. Fundamental to any success we enjoy, are the uniquely human powers of observation, analysis and judgment that are responsible for every major success our society has experienced. At the same time, when we fail to respect those abilities, we can—and do—suffer our greatest failures.

In wrapping up this paper, the author would like to cite the importance of science and invoke its principles and utility for broader purposes in the study of this subject. There is also a great debt to be paid, especially, to the late Air Force Colonel John Boyd, whose seminal work in science and engineering has provided some of our greatest insights into the interplay between theory and science and the stark reality of operational endeavors. (45) This author is not a scientist, nor an engineer, yet the principles of science, mathematics and physics have extremely important application to the management and utility of technical and operational concepts and the communication and interaction that needs to occur between those separate endeavors. Indeed, they prove in fact that there *is* such a thing as a scientific basis to common sense… and that we ignore it at our peril.

REFERENCES

[1] News report, "Military GPS Devices Lag Consumer Gear in Usability", *Space News*, March 9, 2009, p. 12; emphasis added.

[2] Thomas Frank, "$250M effort to secure ports lags: Fingerprint scanners blamed for delay", *USA Today*, April 15, 2009, p. 1A.

[3] Thomas Frank, "$250M effort to secure ports lags: Fingerprint scanners blamed for delay", *USA Today*, April 15, 2009, p. 1A..

[4] Report and observation of the author.

[5] John Robb, "GlobalGuerrillas (e-mail)", *GlobalGuerrillas.com* (website and blog), April 9, 2009.

[6] Thomas Penny and Caroline Alexander, "France Seizes 11 Pirates; U.S. Aid Ship Foils Hijack (Update 1)", *Bloomberg News*, April 15, 2009.

[7] Opinion of the author.

[8] Wickham, DeWayne, "You don't need an armada to deal with Somali pirates", *USA Today*, April 15, 2009, page 11A; opinion of the author.

[9] Rama Lakshmi and Shaiq Hussain, "Assault on Mumbai Planned in Pakistan", *The Washington Post*, February 13, 2009.

[10] Somini Sengupta, "Dossier Gives Details of Mumbai Attacks", *The New York Times*, January 7, 2009.

[11] Roggio, Bill, "Analysis: Mumbai attack differs from past terror strikes", *The Long War Journal*, November 28, 2008; link: http://www.longwarjournal.org/archives/2008/11/analysis_mumbai_atta.php.

[12] Longley, James B. "Implications of Mumbai", *Defense and the National Interest* (website), December 2, 2008, citing John Robb, GlobalGuerrillas.com (blog), December 2, 2008.

[13] Roggio, Bill, *The Long War Journal*, November 28, 2008.

[14] Longley, James B., "Implications of Mumbai", citing John Robb, GlobalGuerrillas.com, December 2, 2008.

[15] Longley, James B., "Implications of Mumbai", and John Robb, *GlobalGuerrilla.com*, December 2, 2008, each citing Noah Shachtman, "How Gadgets Helped Mumbai Attackers", *Wired.com*, December 01, 2008, 9:39:23 AM; http://blog.wired.com/defense/2008/12/the-gagdets-of.html)

[16] "Terrorists turn technology into weapon of war in Mumbai: Their battle fatigues are jeans, T-shirts and trainers. They are the new breed of terrorist - using everyday technology as a weapon of war", *The Courier Mail* (Australia), Sunday, November 30, 2008.

[17] "Terrorists turn technology into weapon of war in Mumbai", *The Courier Mail* (Australia), Sunday, November 30, 2008.

[18] Sengupta, Somini, "Dossier Gives Details of Mumbai Attacks", *The New York Times*, January 7, 2009.

[19] Lakshmi, Rama and Shaiq Hussain, Shaiq, "Assault on Mumbai Planned in Pakistan", *The Washington Post*, February 13, 2009.

[20] Lakshmi, Rama and Shaiq Hussain, Shaiq, "Assault on Mumbai Planned in Pakistan", *The Washington Post*, February 13, 2009.

[21] Richard Esposito, Brian Ross and Pierre Thomas, "U.S. Warned India in October of Potential Terror Attack", *ABC News*, December 1, 2008.

[22] Hon. Thomas H. Kean, Hon. Lee H. Hamilton, et al., *"The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States"* (Authorized Edition), (W.W. Norton & Company, New York, 2004), 567 pp., p. 1. (Hereafter cited as "The 9/11 Report")
[23] Opinion of the author.
[24] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 1, 2; footnote 1, page 451; opinion of the author.
[25] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, footnote 1, page 451.
[26] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 1; footnote 1, page 451.
[27] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 1; footnote 1, page 451.
[28] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, pp. 2, 3.
[29] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, pp. 2, 3; footnote 2, page 451; opinion of the author.
[30] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, footnote 2, page 451.
[31] 3rd Space-based Sensing & Protection Conference, "Conference Announcement" (handout), Spring, 2009.
[32] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 3.
[33] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, footnote 1, page 451 (emphasis added).
[34] Opinion of the author.
[35] Note: Atta was randomly selected by the CAPPS system on his arrival at the Portland, Maine, Airport; nine other hijackers had been pre-identified by the system; Kean, Hamilton, et al., *"The 9/11 Commission Report"*, pp. 2, 3; footnotes 1, 2, page 451.
[36] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, pp. 2, 3.
[37] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, footnote 5, page 451.
[38] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 1.
[39] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, pp. 2, 3.
[40] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 2.
[41] Opinion of the author.
[42] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 2 (emphasis added).
[43] Kean, Hamilton, et al., *"The 9/11 Commission Report"*, p. 3 (emphasis added).
[44] Opinion of the author.
[45] Coram, Robert, "*Boyd: The Fighter Pilot Who Changed the Art of War*", (Little Brown, Boston, 2002), 485 pp.