



CLOSING THE INFORMATION GAP IN BIOSECURITY READINESS¹

Zachary Tumin

Abstract. As mounting effective responses to fast-moving disasters has become a matter of national priority, shared missions have become the norm, and inter-agency coordination has become both more important and more challenging. To improve preparedness, local authorities currently exercise cross-boundary/joint decision-making in which they train and identify deficiencies for various disaster scenarios, among them flu pandemics. In these exercises, information availability is assumed but rarely tested. Participants generally receive pre-set/package information. Accurate situational awareness is critical to sound decision-making in such crises. As accuracy of situational awareness is entirely dependent on the character of information availability/sharing, exercises which assume information availability cannot validate situational awareness. Deficiencies in information sharing/availability which can lead to inaccurate situational awareness are therefore left unidentified and un-remediated. Many factors can affect information sharing/availability, and ultimately impact the accuracy of decision-makers' situational awareness: lack of interoperability of data and systems; legal, policy and regulatory constraints on use; sensor (human and technical) bias of many types; disparate infrastructures and platform capabilities of data producers and consumers; etc. Only exercises which test accuracy of situational awareness can reveal critical gaps in information flow and sharing, and identify its sources. Once identified, the value of addressing the problem is known; investments can be made; remedies can be implemented, and gaps closed. Exercises which would therefore assume clear decision-making roles and responsibilities, and instead test for accuracy of situational awareness among decision-makers are necessary, and here proposed. These would identify critical issues in information availability/sharing which impact situational awareness in pandemic planning, and ultimately the performance of the custodians of the shared-mission response at the local level.

* * *

In Plato's *Meno*, Socrates suggests that knowledge is virtue: the more we know, the better we will act. While the lessons of history before and since 387 AD seem to offer ample evidence to the contrary, the fact is that knowledge and right action go hand in hand. In *Laches*, Plato offers that the warrior who puts himself unknowingly in harm's way shows not courage but foolishness. It is knowledge, Socrates tells us, that transforms action from foolishness to heroism – to righteousness.

¹ Copyright © 2007, the President and Fellows of Harvard College. All rights reserved. ver 12.05.08.

With knowledge, we can do better. We are obliged to seek knowledge in order to do well.

In any biosecurity event, political leadership has responsibilities to assure the welfare of communities. Such obligation impels leadership to assure the accuracy of its situational awareness, clarity as to the interventions it must consider, and knowledge of its options for action – all grounded in sound assessments of its capabilities, the likelihood of success, and its costs. For the decisions faced by men and women who will be called upon to act in a biosecurity episode are fraught with terrifying consequences. All demand knowledge.

To understand the decisions it faces, leadership must know its current situation, and the velocity and trajectory of the crisis. “Where are we today? If we do nothing, where will we be tomorrow?”

To choose wisely, leadership must know its goals, its options for action, and the likely consequences of choice – for the crisis, for communities and institutions, and for individuals. “Are we able to deflect the trajectory to a more satisfactory result?”

To achieve its goals, leadership must act decisively: it must know itself. “Are we able to reason through our options for action, discern any moral dilemmas, and act in time to mobilize, saving the many even at grave cost to the few?”

This last is arguably leaders’ greatest challenge. One month after the Kennedy Administration’s Bay of Pigs saga, former Undersecretary of State Chester Bowles wrote in his diaries of the moral framing of such difficult decisions.

Anyone in public life who has strong convictions about the rights and wrongs of public morality, both domestic and international, has a very great advantage in terms of strain, since his instincts on what to do are clear and immediate. Lacking such a framework of moral conviction or sense of what is right and what is wrong he is forced to lean almost entirely upon his mental processes; he adds up the pluses and minuses of any question and comes up with a conclusion. Under normal conditions, when he is not tired or frustrated, this pragmatic approach should successfully bring him out on the right side of the question.

“What worries me are the conclusions that such an individual may reach when he is tired, angry, frustrated, or emotionally affected. The Cuban fiasco demonstrates how far astray a man as brilliant and well intentioned as Kennedy can go who lacks a basic moral reference point.²

Biosecurity matters as much as natural disasters or national security events challenge leaders to act justly, effectively, and with compassion even if – and especially when -- they are “tired, angry, frustrated, or emotionally affected.” In an anthrax attack or a pandemic event, a failure to act in time, for example, or acting without cognizance of consequence, or indecisively, can have devastating impact. The obligation is upon leaders to prepare now for these exigencies, to assure that the information they require to decide well – even under circumstances that impair their view or cloud their judgment – is available and actionable.

But will it be?

We Have Made Progress

² Quoted in Halberstam (1969)

In the aftermath of the attacks of September 11, 2001, the United States gained heightened awareness of its vulnerability to other types of attacks, including bioterrorism. As if on cue, an unsettling chain of events soon unfolded when anthrax spores were found to have been transported through the United States mail system. For those agencies and institutions that were caught up in the event, including the Centers for Disease Control and Prevention (CDC) and the FBI, it was a new and fast-evolving challenge. Its demands soon revealed the complexities of coordinating science, law enforcement, and politics in real time. It exposed both the vitality and vulnerability of our nation's capabilities to address localized bioterrorist events on a national scale.

CDC soon found itself at the forefront of the nation's response to the anthrax threat. With data streaming in from all quarters – international, domestic, scientific, and law enforcement organizations – CDC's capacity to manage the stream was soon overmatched. It was challenged, also, by having to use data that originated from sources with whom it had never worked before – FBI, local law enforcement, the U.S. Postal Service, and others. Uncertain of the quality, meaning, or authenticity of its data, CDC lacked a clear view of the data's value, its meaning, or how to use it.

At the same time, CDC discovered that it was, itself, also a potential target of attack and was told by law enforcement and intelligence agencies to expect it. Federal authorities soon directed CDC leadership to evacuate its Clifton Road facilities and set up shop five miles away at the CDC Chamblee Campus. CDC directed its national operations throughout the anthrax episode from this location. Under its own threat in these harried days, the warnings CDC received amplified the din of anxieties and pressures for its staff, scientists and analysts.

The confusion experienced at CDC was matched in the field. For the first time, it was called upon to conduct an epidemiological investigation, while the FBI concurrently conducted its criminal investigation. At first, working side-by-side engendered conflict and confusion for the agents and investigators, rather than cooperation. On the matter of "evidence/chain of custody", for example, each agency had competing interests and procedures – the one to preserve evidence as for a crime scene, and the other to remove it to prevent dispersal. While the CDC's field epidemiologists and the FBI's investigators were both generating huge amounts of information, the two agencies lacked protocols for sharing what they knew and distributing it correctly. The unfortunate result was that data became conflicted, partitioned, and diminished in value.

In the aftermath, CDC took these warning signs seriously and made improvements. It established a new emergency operations facility and by all accounts created a structured rhythm that channeled data more effectively. Together with the FBI, the CDC trained thousands of first responders in new forensic epidemiology courses. Two years later, when the SARS outbreak unfolded, the CDC's ability to respond to a biosecurity event was, by all accounts, markedly improved.³

Some Information Sharing Issues Remain a Critical Concern

Although progress has continued, there remain today some concerns about whether information sharing – including data distribution, assessment of data quality and reliability, and data analysis supporting decision-making – will be well managed in the event of a national biosecurity incident where action must be local.

Currently, the federal government has a strategic game plan at a high level, represented, for example, by the draft National Response Framework (NRF), supported by the National Incident

³ For an excellent summary of these events, see Howitt and Pang (2003), and Lagadec et. al. (2006).

Management System (NIMS), and most recently augmented by Homeland Security Presidential Directive 21 (HSPD-21). In essence, these plans devolve decision-making responsibilities to the various emergency support functions, where it will be up to the experts responsible for those functions to process and understand the assembled data. In this way, the response is compartmentalized and delegated to the appropriate experts.

These frameworks and systems have made headway towards clarifying the confusion of roles and responsibilities that CDC and FBI encountered in their baptismal anthrax efforts. However, the same tangle still exists in the prospects for information sharing at the tactical level, yet we have neither plans nor resolution for it.

The Cross-Boundary Challenge

The strategic and tactical challenge for such disasters is profoundly cross-boundary. Dutch Leonard and Arn Howitt assert the “inherent and ineluctable interagency nature of the problem,”⁴ creating what is for Victor DeMarines, David Lehman and John Quilty an “inherently horizontal challenge in a world of inherently vertical service authorities and prerogative.”⁵ Ashton Carter cautions that even deciding how to classify such events has vast implications for the nature and character of the response and solution that will be forthcoming – is it an act of war? A crime? A disaster? All three?⁶ In any event, “the ‘maker’ of government policy,” Graham Allison warns, will be not “one calculating decision-maker but rather a conglomerate of large organizations and political actors.”⁷ The situation is, Russell Ackoff observes, of its nature “messy.”⁸ In the words of MIT’s Donald Schön, “The crucial leadership challenges in these situations tend to lie not in the “hard ground overlooking a swamp, but in the swampy lowland defy[ing] technical solution.”⁹

Furthermore, our nation’s vulnerability to a biosecurity attack or incident is best seen as spanning the vast global stage. In 1964, Marshall McLuhan presciently called attention to the impending “global village” when communications technologies might soon flatten our world, just as Thomas Friedman found they had 40 years later.¹⁰ In that global village, both physical and logical problems, rooted in village affairs halfway around the globe – “global turbulences and large scale dislocations that result [from] local events,” as Lagadec and Ellis describe them – speed towards us with ever faster consequence. Even in 1971, Alvin Toffler of Harvard noted that “as interdependency grows, smaller and smaller groups within society achieve greater and greater power for disruption. [A]s the rate of change speeds up, the length of time in which they can be ignored

⁴ Leonard and Howitt (2007).

⁵ See DeMarines, et. al. (2000) for an outstanding treatment of these issues in the US military.

⁶ Carter (2001). RAND researchers intimate, to the contrary, that perhaps it matters little what we call it – so long as we are prepared. “Given the catastrophic impact of hurricanes Katrina and Rita, controversy has arisen over whether state and local organizations have overemphasized preparedness for terrorism at the expense of emergency preparedness for natural disasters. Our results suggest that the events of 9/11 spurred response organizations not only to undertake preparedness activities for terrorism-related incidents but also to make general improvements in emergency response. All these activities support overall preparedness for any catastrophic event.” Davis, et al. (2006)

⁷ Allison (1971)

⁸ Ackoff (1987)

⁹ In this “swampy lowland” unique events, conflicts in options, and uncertainty as to the nature of the problem leaders should solve next prevail. See, Schön (1990) for his classic treatment of this.

¹⁰ McLuhan (1994) anticipated 50 years ago that “the technologies through which we take in information—the media, broadly defined—[would soon exert] a profound influence over how we think and act.” See, Carr (2007) for his treatment of this.

shrinks to near nothingness.”¹¹ The mail-borne anthrax attacks of 2001 proved the same channels that shrink our world to be potent new pathways for risk. We are in McLuhan and Toffler’s world, today.

Ultimately all solutions to the challenge of biosecurity, like politics, will be “local.” In the global village these can nonetheless have transnational impacts. Given the complexities of the interests to be resolved in any community solution, especially when considered against the challenge to act rapidly and decisively to reduce morbidity and mortality, it seems critical to remedy the gaps that exist in our capabilities. Indeed, the better our leaders who will be responsible for tactical decision-making can close these gaps now, the more time they will have in the midst of crisis to focus on the unknowns that will inevitably remain.

The Need to Know: Likely Requirements for Information and Analysis

With the international outbreak of SARS and avian influenza in recent years, and increased awareness of the role of climate change and warming oceans on outbreaks of infectious diseases, U.S. government and health officials have devoted increasing attention to planning for a non-hostile biosecurity event on American soil.¹² In a flu pandemic, for example, it is critical to know the pace, direction and intensity of infection in real time, as the pandemic takes hold, and throughout its lifecycle. Decision-makers can source this data from a wide variety of data producers. They can gain important insight to the spread of the disease using employer data on absenteeism, pharmacy reports, queries to medical websites, insurance records, and provider encounters, for example. Businesses, school systems, religious organizations and many other institutions and individuals can provide valued data as well.

However, the question remains of whether this data will be available when first responders and leaders need it. Who can say in advance whether the big-box store on the Interstate or Main Street Shoes downtown will share their employee absentee data? How should the parochial, private and public school systems share that same data – about their staffs and students? What about municipal, county and state employees and their bargaining units? Religious organizations may know who among their congregations is ill – how shall they make this known, if at all? How shall individual health care providers share data on patient encounters and via what systems? Which laws will govern data privacy, and how will they affect reporting? Will data formatted for use in an employers’ absence-management system service the needs of public health officials?¹³ What does “absent” mean – to an employer as opposed to a school, for example? How can leaders resolve these semantic differences so that everyone has a clear understanding of the import of absentee reports?¹⁴

¹¹ Toffler (1971), cited in Ackoff (1974)

¹² Colwell (2006), for example, suggests that with changes in ocean surface-temperatures now linked to cholera outbreaks, predictive models for infectious diseases should now include climatic data from satellite sensors and other environmental sources.

¹³ The Department of Defense’s recent efforts to stream data from multiple sources to create comprehensive maritime domain awareness for Navy and Coast Guard commanders raised concerns that civilian data which had been commercialized to provide ship-board capabilities for collision avoidance might have limited utility when pressed into service for other purposes. See, Tumin (2007a).

¹⁴ Such definitional challenges are not unique to cross-boundary work. The author was Director of School Safety for the New York City Board of Education in the 1990’s. In the course of reorganization, it was discovered that the school system had many different definitions for the term “school.” When asked, “How many schools are there in the New York City public school system?” as many people who were asked provided a different answer. Imagine the opportunities for semantic confusion that might result if an outside party sought to determine how many “students” were out “ill” from the “schools” on any given day!

Moreover, decisive action in a biosecurity episode requires resolving the semantic, legal, and technical issues not just for one data element, but for many. Where will we get vaccines, and how soon will they be ready? Should we consider quarantining the infected population, and how will these decisions be enforced? Can we hold people who have the disease in isolation to the point where they are no longer infectious? What social distancing actions should we impose to keep people away from each other so that they do not further transmit the disease? Do we close schools, and businesses? Do we limit or restrict travel in communities and, more importantly, across state and Federal borders? How do all these factors affect our options for action, and the decisions we should make?¹⁵

Understanding these myriad issues will better prepare leaders to act wisely. But moving the data to actionable platforms is a complex process. It takes considerable time to work through these constraints, and it is preferable to spend that time before crisis rather than in its midst.

The Need to Share: The Challenge of Response and Its Impacts

National governments, local authorities on the ground, and the many actors in between may have little prior experience addressing such complex operational, political, moral, and technical questions, each requiring its own information and analysis. In a “reload” scenario, for example, dispersed regions witness similar events, and communities across the country may move to heightened states of readiness and action. They may find themselves quickly inundated by demands for data, analysis, and response.

Even if specified well in advance, will local decision-makers, at once the consumer and producer of rich streams of data, be up to the task of distributing and analyzing it to reveal its many dimensions, causes, impacts and potential responses? Will it be complete and timely with all sources tapped, vetted and integrated into a consolidated view of the situation? Or, will information streams still be crossed, resulting in conflicting and unreliable data from multiple sources, including health agencies, law enforcement, religious institutions, local emergency management, and individual responders? Will it be usable in an integrated view of the situation as it is today, or will data be garbled, dispersed in pockets, or unusable as a result of technical incompatibilities or legal obstacles?

Authorities will feel pressure to act using whatever information they may have. Pandemic protocol, for instance, calls for mass administration of antiviral drugs, together with quarantine and social distancing, within 21 days of first detecting the virus.¹⁶ Pressed for time, and even lacking full information sharing capabilities, first responders will improvise information sharing arrangements, turning to their professional relationships to “make it happen”. Under such circumstances, “gentlemen’s agreements” to be open and share may well be the principal instrument for information sharing. Local-level responders are proven masters of improvisation, after all; even with steep

¹⁵ Carley (2004).describes the complexities of modeling the spread of infectious disease through the mountains of valleys of social networks comprising the urban landscape. These can best be addressed now only with best-guess models, and answered with large-grained policy solutions. The simple question, “What happens in [my city] if three people return from vacation with small pox?” requires analysts to model factors as disparate as wind and climate, differential risk associated with ethnicity, age and race, and variable access to social communication and knowledge networks.

¹⁶ World Health Organization (2006)

learning curves to the particular disaster, they will act with confidence that, in the end, they will have proven themselves up to the task, and be smarter, better, and faster.¹⁷

But what will be the consequences for the community in that two-week window while first responders are learning as they go – consequences that might be averted with improved planning, drilling, and information sharing? There is vulnerability for significant consequences – truly high morbidity and mortality, for one, and significant social, economic and enduring personal consequences, for another. It is the nature of flu pandemics that, over time, consequences will deepen, and more people will be affected. We will hear of neighbors dying, and not just the elderly, immunocompromised, or the young. If many people fall ill in a small community, it may affect single large employers significantly, and engender economic consequences. There will be social consequences around shelter and place, when children cannot go to school.

All the while, demands for action will be intense, if not overwhelming. How durable will improvised agreements be under the duress of chaos, tragedy and continued threats? Is a “gentlemen’s agreement” for information sharing the optimal infrastructure for the circumstances that will be upon us in a flu pandemic? Should such agreements even count in the context of any reasonable discussion of preparedness?

Where We Are Today

To some analysts, such issues represent the “Achilles heel” of our current planning. Beyond specifying roles and responsibilities, as the National Response Framework ably does, or resource and equipment sharing, as Emergency Management Area Coordinators (EMACs) do, there is yet the absence of a tactical communication strategy for information sharing (distribution, assessment, and analysis) spanning the many levels, but devolving most importantly to the local level. Thus, while there is clear partitioning of roles and responsibilities at each level, the basis of information sharing among the vast number of local, mid-level, national and global sources is still unspecified, untested, and viewed as unknown at the moment.¹⁸

This challenge is especially potent in light of the highly networked environment in which information sharing must take place, decisions made, and action taken. It comprises, for example, not a single command-and-control authority, but rather multiple authorities that are distributed and diverse. They may operate under quite different legal and political mandates, with culturally apposite workforces and management styles, non-aligned organizational goals and procedures, and utterly different technology infrastructures and capabilities. As the CDC/FBI Anthrax experience demonstrated, at any given time these organizations can hold diverse, persistent, and sometimes clashing views as to the single most important outcome to achieve and the best method for doing so.¹⁹

¹⁷ Some researchers have suggested that such “soft” attributes are in fact critical success factors, including, for example, pre-existing relationships, good understandings between individuals and organizations, shared views of the mutual benefit of coordination, and good facilitative processes. See, Davis (2006b).

¹⁸ It is interesting to note, however, that in the recent FEMA ICS guidelines there is (a) no command staff position indicated for analysis, and (b) no command staff position indicated for data acquisition, technology linkages, data security and integrity, or for establishing technical data interfaces. See FEMA (2005)

¹⁹ Seid, et. al. (2006) call attention to the incredible diversity of organizations and authorities within the public health extended enterprise itself. “The public health system includes more than 3,000 county and city health departments and local boards of health; 59 state and territorial health departments; tribal health departments; more than 160,000 public and private laboratories; parts of multiple federal departments and agencies; hospitals and other health care providers; volunteer organizations, such as the Red Cross; private vaccine and drug

In such “extended enterprises”, critical hard-edged issues arise with respect to technologies for sharing; the financing procurement and acquisition of needed investments; standards and agreements for data interchange; and aligning business processes for cross-boundary sharing, among other factors affecting information capabilities.²⁰

By our best accounts, these capabilities are neither specified nor well known at the local level yet. As a nation, we have done strong work to outline and rehearse decision-making at many levels. Exercises typically focus on clarifying decision-making roles and responsibility, however. Even so, they have highlighted recurring gaps and training deficiencies, which some surmise recur because the exercises have not yet incorporated information sharing to the degree required.

Efforts to specify tactical information sharing requirements and assure local readiness have thus far been cursory. What few efforts are visible seem to rely upon top-down, command-and-control models that might assume data repositories are populated by willing, if not supplicant, data owners and producers standing at the ready to grant access to information, given the word.²¹

The world may be flat, but our networked world, where information and decision-making must meld, is truly messy. No one commands the agency or firm next door; they are in any event anything but monoliths. In our logical global village, “next door” could be 12,000 miles away. Moreover, two data systems that are actually next door in our physical village could define “sick” as if they were speaking different languages, with enormous consequences for decision-makers trying to gauge a pandemic’s spread. Should leaders start ordering things around in a command-and-control model, they might soon see how little they either command, or control. However, should they wait for the day of reckoning, to “know what we know”, they may spend days unaware, while system gauges creep stealthily to “red”. Neither posture is a solution for readiness.

Closing the Information Gap in Biosecurity Preparedness: The Questions We Must Ask

Six Questions for Leadership. By specifying and testing information sharing in advance, leaders can assure that the predicates are laid for accurate situational awareness and that they will have clarity regarding the interventions they must consider, knowledge of their options for action, and choices that are grounded in sound assessments of our capabilities and the likelihood of success. Testing these critical elements of decisioning and remedying any gaps in information that inform them will

manufacturers and distributors. Responsibility for the system is divided among the states, which typically have greatest authority for public health; the federal government, which can influence public health through funding decisions and via its authority over interstate commerce; and local public health departments, which exercise a great deal of independence and authority in many states. In addition, public health is only one part of a much broader emergency preparedness community, which also involves the heads of 32 federal agencies and departments, including the Department of Health and Human Services.”

²⁰ For a description of these challenges, generally, particularly in back-office transformations, see Mechling (2006)

²¹ See, Markle (2002), and Allison (1971) who reminds us that it is a mistake to treat “government” as a monolithic, non-differentiated “black box” with unity of purpose and action. That “black box” in fact “cover[s] various gears and levers in a highly differentiated decision-making structure [where] large acts result from innumerable and often conflicting smaller actions by individuals at various levels of bureaucratic organizations in the service of a variety of only partially compatible conceptions of [jurisdictional] goals, organizational goals, and political objectives.” Schein (1992) asserts, similarly for industry, that “with large organizations of a certain size, variations among the subgroups are substantial, suggesting that it is not appropriate to talk of ‘the culture’ of an IBM or a General Motors or a Shell Oil.”

reduce reliance on improvisation, improve the likelihood of effective action, and help leaders achieve their goals.

To prepare for a pandemic, any leader of any organization would want to assure prior to the event that should a pandemic occur he/she could quickly get answers to these five questions – and that he/she has a dynamic capability for updates as the pandemic may spread.

- 1) What is the nature of the incident and its potential impacts? This will tell us the facts we need to gather about it and what its likely path will be if we do nothing, or do not act in time.
- 2) What are our goals in managing it? This will specify the results we want to achieve in dealing with it and the values we will try to harmonize and realize in any solution.
- 3) What trajectory are we on now? Whose actions will alter the terrain or constrain our options? This will tell us whether we have to alter the trajectory.
- 4) What decisions do we face now and throughout the crisis? This will reveal the options for action in managing the crisis and the choices we can make to deflect its trajectory from its natural path and toward our intended goals
- 5) Do we have the information we need in order to make those decisions well? This will tell us what we need to know to gauge the consequences of our various options in terms of their impact on goals, and values as we reach for them.²²

Informed, rational, moral, and effective decision-making is predicated on the information filling these “knowledge buckets”. Leaders can test situational awareness, awareness of interventions they must make, knowledge of options for action, and estimates of likely results against their ability to answer these five questions accurately, completely, and in time.

The requirement to keep these “knowledge buckets” full and fresh is therefore imperative and dynamic. Data must be available and usable against proven standards of worthiness, both technical and operational.

To assure that that will be so, leaders of organizations with a pandemic leadership role must assure that there is current knowledge and a dynamic updating ability with respect to these critical elements. There is, therefore, a sixth pre-event challenge for knowledge:

- 6) What is required to provide this information data? This will reveal to us the gap between our current capabilities to provide data for decisioning and our required capabilities, so that we can take steps now to close those gaps.

18 Questions for the Stewards of Preparedness and Response. Below are 18 specific, tactical, critical elements of knowledge required by those who will steward the collaborations of government, citizens, industry and commerce through the crisis of a local biosecurity event. As the custodians of the response they must ask these questions in advance of crisis, so that they can see and remedy any gaps in information sharing capability, and know which remain. Having done so, they will be able to state affirmatively to political leadership that to every extent possible leaders will have the information they will need and

²² This framework derives in part from the work of Wharton’s Russell L. Ackoff, a visionary of systems engineering. In particular, his construct of “reference projections” to assess a current trajectory against envisioned desirable futures is an invaluable tool for clarifying options for intervention. See, Ackoff (1987). See, also Howitt and Leonard (2006) for their powerful conception of “robust” situational awareness to include awareness of likely futures, options for action, and probable impacts.

the awareness they require in order to decision the crisis and act to protect the wellbeing of the community.²³

- 1) **The Makeup of the Extended Enterprise of Information Producers and Consumers.** In a biosecurity event, who will be the principal data producers and consumers? These will span sectors and jurisdictions, and include industry, commerce, and diverse government agencies. Each may have data products, services, and capabilities, and roles to play.
- 2) **The Platforms for Information Sharing** What are the various data products and services used by enterprise data producers and consumers that would be valuable in a biosecurity event, together with the infrastructure and rules for their use?²⁴
- 3) **The Platform Capabilities of Exchange Partners.** Who can use the various platforms to push and pull data? Understanding partners' different capabilities for access to data in a crisis is critical. (Can everyone see CNN? Who has email or web access?)²⁵
- 4) **The Readiness of Data for Information Sharing** How ready is data for sharing among partners? Is it visible, findable, and usable?²⁶
- 5) **The Networks Where People Exchange Knowledge.** What networks exist where groups of like-interested individuals and groups already move and share knowledge and information? Which platforms do they rely on?²⁷
- 6) **Legal, Regulatory and Liability Issues:** What statutory or other restrictions will affect the availability of information for sharing, and what liabilities pertain to its use? Health data, data on juveniles, secret or top secret data, criminal history data, competitive commercial and industrial data – all will be demanded, available, or searched for. Having a clear idea of the constraints that govern sharing of such information prior to any urgent need is essential to assuring its availability when necessary.²⁸

²³ The US federal government's Information Sharing Environment Implementation Plan (2006) treats several of these same challenges in broader form – mentioning general requirements to “[leverage] ongoing information sharing efforts and [promote] a culture of information sharing – as well as “define common standards”, “develop a common framework”, “standardize procedures” and “facilitate information sharing.” The DoD Information Sharing Strategy similarly establishes five broad “areas” for information sharing efforts - culture, policy, governance, economics and resources, and technology and infrastructure. DoD (2007).

²⁴ See, Eisenmann, et. al. (2006) for his treatment of platform issues in two-sided markets.

²⁵ Among other capabilities, interoperability of systems, for example, will determine information flow and availability. US Department of Defense (“DoD”) has defined five levels of interoperability of systems in its Levels of Information Systems Interoperability (LISI) Maturity Model, ranging from “connected” to “enterprise”. See, Tolk (1998).

²⁶ These concepts are the foundation of DoD's netcentric data strategy. See, for example, Department of Defense (2003) and (2007).

²⁷ The extended enterprise comprises numerous informal and formal communities of like-interested individuals and groups. They use a variety of channels and platforms to share information and insight, and to give meaning to data and events. Davenport (1998)

²⁸ For issues raised by HIPAA regulations impacting information sharing during Hurricane Katrina, see Department of Health and Human Services (2005). For an outstanding framing of the risks and issues in the use of public and private citizen data during times of national exigency, see Heymann and Kayyem (2005).

- 7) **Strategies for Information Sharing.** What pre-existing formal frameworks for data sharing will data consumers encounter within the extended enterprise, and in a biosecurity event, pursue? Four frameworks are likely: **delegation, integration, consolidation, and provisioning.** Each has jurisdictional, business, and technical requirements and implications for access and sharing – and issues.²⁹
- 8) **Governance and Agreements for Sharing.** Will we be able to “get our hands on” what we need, when we need it? What agreements would be best to lock in ahead of time? What force will they have, what issues might intervene when invoking them, and how might we assure compliance?³⁰
- 9) **Financing of Information Infrastructure Procurement and Acquisition.** What investments do we require to assure information sharing? Such investments could include improving partner platform capabilities; assuring interoperability of devices and systems; undertaking systems development and standard setting. Should individual organizations fund such development, or should there be some kind of joint or multi-source funding?³¹
- 10) **Adapting to Unanticipated Events and Users.** What capability do we have to adapt to novel events, together with data producers and consumers whom we will encounter?³² How will “web 2.0” capabilities of blogs, wikis, and other user-generated, open-source sites impact events, perceptions, and decisions?³³

²⁹ These four strategies are detailed in Mickelson, et. al, (2007).

³⁰ Such agreements are needed to compliment technical availability and realize sharing. “The availability of Lotus Notes,” Thomas Davenport and Laurence Prusak (1998) remind, “does not change a knowledge-hoarding culture into a knowledge-sharing one, alas. The medium turns out not to be the message and does not even guarantee that there will be a message.” Even with such agreements, the authors observe, sharing behavior occurs within a knowledge exchange marketplace and remains contingent on its political economy. In this market place, social relations, political arrangements, and non-cash “prices” drive knowledge transactions among producers, consumers and brokers.

³¹ The challenge of funding shared enterprises, generally, is recounted in a case study of Iowa CIO John Gillispie’s efforts to finance a shared recovery center. See, Tumin (2007e). For a discussion of these issues in DoD settings, see DeMarines, et. al. (2007). If individual efforts that benefit all are to be funded by individual organizations, each agency’s budget might compete with other (non-biosecurity) items in the same service budget, putting (biosecurity) investments at risk or differentially realized. If funded “jointly” or, for example, by a single acquisition authority, infrastructure investments might compete only with other broad investments by the jurisdiction. Rational values such as interoperability, low redundancy or overlap, or sub-optimal system selection might be easier to assure or less likely to be an afterthought.

³² For a cogent treatment of this issue, see Department of Defense (2007). See, also Markle (2002): “Because of the diverse, constantly adapting, and furtive nature of the new security threats, “hardwiring” the analytic and user communities is not only difficult, but also counterproductive. Relevant information comes from a much wider range of sources (dedicated intelligence collectors, users themselves, state and local officials and the private sector), and it is difficult to know a priori what information will prove relevant to analysts or useful to users.”

³³ During the recent California fires, for example, bloggers posted 7,000 unique entries pertaining to the fires in a three-day period October 22-24, when fires raged most fiercely. Over on another user-generated “channel” – Wikipedia -- on October 22 an individual with a screen name of Plainsong created a page titled, *October 2007 California Wildfires*. Within five hours this page received 74 unique updates, and ultimately referenced 106 Spanish and English-language primary sources. See, *Bloggers Blog* (2007) and *Wikipedia* (2007). Some researchers assert that user-generated, open-source platforms in general hold great promise for innovation and problem-solving: by “broadcasting” problems to “outsiders” having expertise at the periphery of problems, they engage those “most likely to find answers and do so quickly.” See, Lagace (2006). See, also, Mittu (2007) who discusses more formal approaches to sharing unclassified information among diverse communities of NGOs and others during disaster relief and humanitarian operations.

- 11) **Achieving Accurate Situational Awareness:** What information sharing and analysis is required to provide accurate situational awareness? What processes are in place to test, prove, and validate accuracy of situational awareness? (See, Pp. 14 ff, *infra* for a fuller treatment of this.)³⁴
- 12) **Leadership and Political Management:** What are the requirements for political leadership to assure information sharing, and what leadership capabilities should we select for and train? The role of leadership in transforming pods of stovepiped data from enterprise bastions into an enterprise-wide capability for consolidated, timely views with meaning and consequence for decision-makers is critical for success.³⁵
- 13) **Executive Sponsorship of Cross-Boundary Remediations.** How can we assure design, development, uptake and adoption of measures to remedy gaps? Executive sponsors of specific initiatives to assure information sharing across boundaries must manage technical, operational, legal and cultural issues. Given the difficulties of introducing new technologies and tools and gaining uptake and adoption, for example³⁶, executive sponsors' capabilities and strategies are critical.³⁷
- 14) **Communicating to Friends and Strangers.** What information is required for effective communication during crisis, and will crisis leaders have the data they need?³⁸
- 15) **Reasoning Through Grave Moral Dilemmas.** Will leaders have the information they will need, and in the framework they require, in order to see the dimensions of choice and reason through the grave moral dilemmas they will surely face? Given their biases and capabilities, their customs and habits, what are the information framing requirements for their consideration?³⁹

³⁴ Leonard and Howitt (2007) list this as first on their checklist of preparedness – “developing a detailed understanding of the nature of this ‘kind’ of situation and an understanding of its key elements—so that we know what facts and observations are relevant.” More than mere awareness of one’s circumstances, however, Leonard and Howitt (2006) mean “situational awareness” to be far more robust – to include, as Ackoff and others suggest, the ability to project forward, see the future, understand options to affect it and likely results, and to choose.

³⁵ LAPD Chief William Bratton’s efforts to lead collaborative change for information sharing with the FBI and county agencies are recounted in Tumin (2007c). Rick Friedman’s efforts at the US Department of Health and Human Services to transform 40 years of Medicaid systems architecture to adapt to state-level information needs is recounted in Tumin (2007d). See also, Marcus et. al. (2005) for discussions of such “metaleader” challenges, generally.

³⁶ Harvard’s John Gourville reports that users tend to underweight the benefits of replacement technology by a factor of three, and over-weight their loss of cherished technology by the same factor. McAfee (2006) , commenting, notes that this seems to suggest that to assure uptake and adoption, any new technology must be “9x” better than the system it is replacing.

³⁷ See, Tumin (2007b) for a treatment of six strategies of executive sponsorship.

³⁸ For the messages that must be communicated during a pandemic, see WHO (2006). These include, for example, communications around measures to isolate moderate-to-severe clinical cases; voluntary home quarantines and daily monitoring; administration of antiviral drugs for cases and for prophylaxis; guidance on strict infection control and use of personal protective gear; promotion of hand and cough hygiene; and domestic cleaning to reduce transmission, and waste removal

³⁹ The works of Lawrence Kohlberg and Carol Gilligan point to critical differences in capabilities and styles of reasoning through complex moral dilemmas – capabilities and styles which yield quite varied outcomes when different leaders tackle identical problems. See Kohlberg (1970) and Gilligan (1985).

- 16) Decisioning for Action, Acting In Time. Networks take on all shapes and sizes. Can information sharing accommodate the optimal arrangements for decision-making in a crisis?⁴⁰
- 17) Dynamic Auditing, Updating and Validation Capability – Before and During Crisis. How can we best test, prove and validate information readiness, and close gaps that may exist? Who will be responsible for managing overall operational risk of the extended enterprise -- assuring the overall readiness of the information “supply chain” and partners, testing, and preparedness, and taking remedial action to close any gaps and improve capability?⁴¹ During crisis, when systems may be degraded and information imperfect, how can system stewards continuously validate and update situational awareness? Do they have a process capability for doing so?⁴²
- 18) Assuring Minimum Essential Biosecurity Functions. In the event of a biosecurity event, what are the minimum essential information functions that must be assured at the local level? Who are the people, what are the processes, what is the information and technology infrastructure, and which are the facilities that are required to support those functions, and to restore them as a priority? What is our plan to monitor and protect the minimum essential information sharing functions?⁴³

Exercising Information Sharing

As decisions cascade down to the local level, the major issues confronting decision-makers occur not just under conditions of chaos and uncertainty, but within decision environments of uncertain authority, and with potentially grave consequences. Currently, many jurisdictions exercise these very decisions, to remove uncertainty where possible, or to plan for it as a contingency.

⁴⁰ For a useful discussion of alternatives, see DeMarines, et. al. (2000)

⁴¹ The Basel Committee on Banking defines operational risk as the potential for loss resulting from inadequate or failed internal processes, inadvertent or deliberate actions of people, problems with systems and technology, or external events. Caralli (2006) offers a broad discussion of the value of process capability models, in general, to help organizations plan for and adapt to novel risk.

⁴² See, Sparrow (1996) for his incisive treatment of the imperative to audit and validate current perceptions of dynamic problems against their true real world proportions and patterns. While he treats this specifically in the world of fraud control, its implications are generalizable to other domains where accuracy of situation awareness is essential. See, Argyris and Schön (1974) for imperatives and issues, generally, for decision-makers to “maximize valid information” and improve effectiveness by testing, validating and altering their “theories-in-use”.

⁴³ Operational resiliency as suggested here synthesizes the disciplines of security (physical, information, and network), business continuity, and IT operations management (Caralli et al , 2006). The concept of minimum essential X is borrowed from a white paper proposing to assure the nation’s minimum essential financial functions in the event of attack or disaster, including cash to ATMs, liquidity of capital markets, etc. See, Financial Services Technology Consortium (2004). See, also, Financial Services Sector Coordinating Council (2007) for a treatment of this. It is interesting to note that in a recent survey of 1000 firms, private industry assessed its principal readiness challenges to be not technical or infrastructural, but “people” problems of training, awareness and preparedness. (Continuity Insights/KPMG, 2007)

Whether such exercises, by tabletop or in the field, are amply undertaken is a matter for discussion elsewhere. We do know that they are principally designed to test plans (and their assumptions), identify training deficiencies, and align roles and responsibilities to the event.⁴⁴

In order to test decisioning, data and information relative to the scenario is shared widely with all players. Tests assume, but do not test, information availability. Yet it is precisely information availability that creates the most profound risk. Exercises which assume information availability also assume a world in which there is no gap between our perceptions of a situation and its reality. We know that to be profoundly uncertain, however: there is a dynamic gap between perception and reality that must be tested for, closed, and constantly monitored. Effective organizations have this capability.⁴⁵

What seems to be the case, then, is that there exists a need for deep, intensive, and unforgiving exercising of information sharing. Such sharing is the natural precursor and complement of effective decision-making. Without exercising information sharing we may be making flawed assumptions about the nature of the information that can and should be available to, and used by, decision makers under various scenarios.

The value of exercising information sharing – testing, proving, and validating flows, availability, and accuracy – can therefore not be underestimated. Other than the anthrax event, we have had no chance to be involved nationally, or locally, in real biosecurity operations, against real enemies or threats. No one – certainly at the local level in the United States – has that experience, readiness level, or proven operational capability. Our systems for information flow, availability, and accuracy have never been tested in operational conditions, nor have their failures been observed, or their faults remedied.⁴⁶

Validating Accurate Situational Awareness⁴⁷

In particular, we recommend exercises that focus on validating the accuracy of situational awareness.⁴⁸ Accurate situational awareness is the lynchpin of successful action. From situational awareness flows our assessment of what we must do next. Any gaps in our perceived situation and the actual situation – caused by failures of information flow, or another impediment – threaten our security and safety. By exercising situational awareness, and auditing our perceptions of the situation

⁴⁴ The diversity of models, simulations, and games for domestic preparedness training and exercising is astounding. See, Agrait, et. al., 2004 for a review of one hundred such tools.

⁴⁵ Sparrow (1996) implies that capable organizations take steps to assure that such gaps are “self-revealing”, but aligns with with Argyris and Schön (1974) who suggest that much organization process tends, in fact, to be “self-sealing”. They argue that the move from “self-sealing” to “self-revealing” is vital to improving organization effectiveness, namely, assuring strong alignment between intention and effect (“when you can produce what you say you know”), detecting and correcting “mismatches”, and updating “theories in use.”

⁴⁶ For a detailed rendering of the complexities of the information challenge, see Program Manager, Information Sharing Environment (2006).

⁴⁷ Tactical situational awareness is vital in many domains, studied, and trained for – maritime, aviation, weather, firefighting, environmental disasters, to name a few. For twenty-two definitions of “situational awareness,” plus an annotated assessment of each, see, RAES-HFG (2000). It might be simpler to agree to Wittgenstein’s all-purpose solution to such linguistic jamborees, namely, “The meaning of a word is its use....” If the reader desires a quick round of training in situational awareness for tornadoes and other weather events, he/she may turn to the National Weather Service/NOAA’s online offering. (see citation in bibliography).

⁴⁸ See Sparrow (1996), *op cit.* for his treatment of the analogous requirement to regularly test and validate the accuracy of situation awareness in the fraud control domain.

against reality, we can identify significant gaps in information flow for remediation. Our situational awareness might show us 100 cases of infection, for example. Our exercise might show that we overcounted by 20 from several sources, and undercounted by 200 from the universe of “known” cases comprising the exercise.

The many risk points for accuracy in situational awareness are well documented. They include, for example, nine potentially serious system biases. Each can tilt information flow and affect decision-makers’ beliefs about the world:

- **Sensor Bias:** “The crux of the matter is that no single sensor is perfect,” DeMarines et al (2000) write. “Sensors ... are designed with specific purposes in mind, and hence all of them see some things better than other things.” Influenza surveillance means and indicators can vary widely across jurisdictions, for example.⁴⁹
- **Domain Bias:** Over-scanning some areas of potential impact, under-scanning others can create false weighting of trends or impacts.
- **Infrastructure Bias:** Differential access of data producers and consumers to platforms that move data can tilt bias in favor of some and against others. Time lags in access and reporting can have particularly nettlesome consequences.⁵⁰ Interoperability failures may further affect movement of data among some data producers and consumers.⁵¹
- **Semantical Confusion:** Different meanings attributed to like terms, such as “evidence” when used by CDC and FBI, can create great confusion
- **Data Non-Alignment:** Tracking the geospatial/temporal attributes of a pandemic from global sources can vary as sources rely on different data elements (e.g., “miles” vs. “kilometers”).⁵²

⁴⁹ Aldort, et. al. (2006) mention varieties in surveillance-indicators that can use quite different data, and give different meanings - national versus local data, for example; influenza-like illness (ILI) versus laboratory-confirmed cases, versus deaths; or proxy indicators, such as pharmaceutical purchases or school/work absenteeism. Some indicators may be used because they are cheaper and provide results faster; others might be used as they are specific, but take longer. Some jurisdictions rely more heavily on data obtained from private providers – leaving questions about cases that are laboratory-confirmed versus clinically diagnosed. Some jurisdictions might not have labs with the capability to perform influenza testing at all, or have wide variability in vulnerabilities that could impact collection, transport, testing and reporting of results, for example. For a remarkable variety of climate sensors, see

⁵⁰ The time lags in information sharing during fast-moving crises can prove disastrous. Decision-makers need to keep pace with the real-world tempo of events. Early-arriving data will bias action in its favor relative to late-arriving data. Schön (1971) observes that delays in assessment, choice and action risk taking so much time as to “include changes [in the situation] which invalidate conclusions once they are reached.”

⁵¹ The lack of interoperability among the world’s climate data centers, for example, severely constrains using such data to model global impacts of climate change. See, for example, Henricksen (2006) and “IEOS” (2004)

⁵² See, DeMarines, et. al., op cit. (2000) for a discussion of the great difficulties encountered in providing US air defense commanders with an accurate single integrated air picture (“SIAP”). “Consider an enemy aircraft that is sensed by three different systems. One system may provide the most accurate information about its location, another about the type of aircraft, and a third about its velocity. If the data from all three systems are combined correctly, then we know what we need to know. If they are combined incorrectly, we may believe there are two or even three enemy aircraft — or worse still, two enemy aircraft and one “unknown” aircraft that might be friendly. The failure to obtain reliable SIAP has [multiple] serious consequences...”

- Data Completeness: Lack of incoming sensor data (human or technical) may mean no sensor is in the area or a sensor transmission path is broken, or there really is no event. Which one? This problem is especially acute when streaming data together from disparate sources whose human or technical sensor dispositions and capacities may be uncertain or unknown.⁵³
- Analysts' Bias: The occupational bias of servicing some customers with particular intelligence products which are geared to a specific decision environment, together with flawed models ("model risk"), and a general over-reliance on systems to sort through huge data sets, can tilt interpretations and meanings ascribed to events. Whenever analysts contextualize, categorize, calculate, correct, or condense data, as they must, new bias inheres.⁵⁴
- Decision-Makers' Bias: Even with information available, the perceptual frame of the decision-maker and unique cognitive/emotional capabilities comprising his/her customs and habits of decision-making may uniquely over- or under-emphasize certain data. Gaining insight into how, for example, leaders will perceive the crisis and move under such circumstances depending on what information is given to them, when, and how, is critical to planning and execution.⁵⁵

⁵³ See, for example, the account given in Tumin (2007a) *op cit* for the maritime domain, where commercial, industrial, and diverse military sources may co-mingle in single integrated displays. Managing the coastal environment has similar challenges. The US Environmental Protection Administration, for example, has available to it a remarkable variety of coastal sensing sources and data, including aerial photographs, satellite imagery, acoustic data, and radar imagery. It uses these for mapping shorelines, floodplains, land cover, habitats, and vegetation; for regional planning, water quality monitoring, coastal management permitting, oil and toxic spill response planning, navigation, disposal site monitoring, and base maps. See the EPA's description of the 78 sensor systems available to it in its Remote Sensing Information Matrix (Lundquist, 2007)

⁵⁴ Allison (1971) *op cit.* warns that the analyst's job to explain the world and predict the future is inherently biased to particular customers as analysis relies on conceptual models which both "fix the mesh" of the analyst's nets, and direct his cast to "select ponds, at certain depths, in order to catch the fish he is after..." Carley (2004) asserts that modeling to predict morbidity and mortality in bioattacks is nonetheless essential. Since such models must draw from very preliminary understandings of "how social networks affect disease propagation and how the consequences of disease change social networks," however, "there is simply not enough actual data on bioattacks" to now build such models. Sparrow, (1996) *op cit.* cautions, generally, that even if there were such data the typical model-driven strategy of many organizations – which he calls "systems select – analysts inspect" – can still fail to detect crucial novelty. "Systems," Sparrow says, "do not spot interesting or unusual patterns. They never get suspicious. They never make telephone calls just to check the facts." And it is precisely in novel, never-before-seen events where risk can be highest – yet where "it can seem like an impossible luxury to provide increased protection against an event with an incalculable probability and unknown consequences." (Lagadec, et. al. 2006) Sparrow (1994) argues further that organizations' variable embrace of analysis ultimately affects what some know and some don't about the world. Whether in intelligence or political discourse, US Senator Daniel Patrick Moynihan was given to observe, with some exasperation, "Everyone is entitled to their own opinion, but not their own facts."

⁵⁵ Schön (1990) *op cit.*, characterizes this as a challenge of "framing problematic situations" – we see the world through the lens of our disciplinary backgrounds, organizational roles, past histories, interests and political/economic perspectives, weighting and discounting facts heavily as a result. "Those who hold conflicting frames pay attention to different facts and make different sense of the facts they notice. It is not by technical problem solving that we convert problematic situations to well-formed problems; rather, it is through naming and framing that technical problem solving becomes possible." May (1973) notes the power of decision-makers' beliefs about history – often incorrect - to shape their decisions. Argyris and Schön (1974) warn about the "self-sealing" bent of such frames to prevent reality from seeping in and learning to occur when incorporated into a decision-culture. As Schön, Argyris, and May stress the potency of such frames, others point to their durability over time. Stark (2005) observes that "corporate imprints," for example, leave lasting

- Enterprise Bias. The political economy of the extended enterprise's knowledge exchange "market" will yield patchwork or asymmetrical knowledge within organizations and across them, tilting situational awareness towards some decision-makers and away from others.⁵⁶

Anticipating Novelty

To assure biosecurity readiness we are obligated to exercise information sharing; to test in particular the accuracy of situational awareness of decision makers; to assess the gap between their perceptions and the true world; and to take steps now to address the sources and causes of that gap. We cannot afford ad hoc just-in-time inventions to address gaps that we discover in the midst of crisis; these must be fleshed out before hand and remedied. Adaptation should not be to known and preventable failure; but to events that are unknown or unanticipated because they are utterly novel. There will be crisis enough, and gaps aplenty from the messiness of the actual situation, to handle without adding to otherwise preventable failures.

If what is required is a dynamic capability to adapt to predictably novel events, then having a clear sense of our capabilities to do just that, in effect, anticipating novelty, requires a very special set of sensors, metrics and measures of our capability. We are reminded of the capability stages and sequences comprising the Capability Maturity Models Integration® of the Software Engineering Institute.⁵⁷ Such models may provide a suggestive framework for understanding our information sharing capabilities with respect to biosecurity readiness at any given time. As stated, we may think of critical information sharing components such as situational awareness as resting on everything from ad hoc arrangements, where there is no established process, and efforts to share data are heroic; to repeatable and ultimately standardized processes, which still focus on maximizing results for individual organizations rather than for the extended enterprise; to enterprise-wide, inter- and intra-organizational processes that are measured, metricized and optimized for enterprise-wide outcomes with continuous testing and improvement as needed. Efforts to further describe such a capability maturity model for information sharing are now underway at Harvard.⁵⁸

residues of corporate strategy, structure and culture on young workers. "There is a GE imprint, an IBM imprint, a Bain imprint—all of which influence future decision makers." These may sum and determine aspects of non-deliberative dimensions of decision making described variously, for example, as intuition-based decision-making (Matzler et. al. 2007), thin-slice decision-making (Gladwell, 2005) and recognition primed decision-making (Klein, 1999). These conceptions owe much to John Dewey's towering work in social psychology, *Human Nature and Conduct*, which has served as the foundation for many such notions and conceptions since its publication in 1922 – none surpassing the original. "Honesty, chastity, malice, peevishness, courage, triviality, industry, irresponsibility are not private possessions of a person," Dewey wrote. "They are working adaptations of personal capacities with environing forces [my emphasis]. All virtues and vices are habits which incorporate objective forces. They are interactions of elements contributed by the make-up of an individual with elements supplied by the out-door world. They can be studied as objectively as physiological functions, and they can be modified by change of either personal or social elements." (Dewey, 1930)

⁵⁶ Davenport (1998)

⁵⁷ See, Carnegie Mellon Software Engineering Institute (2002). "One of the benefits of model-based process improvement is the ability to benchmark an organization's current level of capability. Based on their unique requirements and objectives, organizations can determine if they need improvement and can develop plans to close the gap between current performance and expected performance." Caralli et. al. (2006). Capability Maturity Model, Capability Maturity Modeling, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

⁵⁸ "Unfortunately," RAND researchers recently reported, "we cannot tell how much better prepared the nation is ... because we lack standardized measures of organizational and community readiness ..." Davis (2006). It

Given the challenge of maintaining networked linkages in a deeply verticalized world, negotiating ad hoc information sharing arrangements can prove deadly. Exercising can reveal our gaps; leaders can help us improve our capabilities from ad hoc arrangements to more regularized processes, reducing reliance on improvisation, and improving our capabilities to handle true novelty when our “flat world” demands it.

It is essential not only that there is a clear set of roles and responsibilities, but a sound, validated decision framework for choosing well – for making good decisions. The inherent biases of information sharing will change weights and decisioning. Decision-makers’ own styles will process identical data differently. Only exercising and testing will give us the capability to understand, adjust, and re-decision. Exercising for information sharing is emerging as a critical next step on our nation’s readiness agenda.

About the Author

Zachary Tumin is Executive Director, Leadership for a Networked World Program, at Harvard University’s John F. Kennedy School of Government.

will be critical to develop relevant metrics of readiness by which local leaders can assess tactical capabilities to handle the likely demands of crisis.

Bibliography

1. Ackoff, Russell L. *Redesigning the Future: A Systems Approach to Societal Problems*. New York: John Wiley & Sons, 1974.
2. Ackoff, Russell L. *The Art of Problem Solving: Accompanied by Ackoff's Fables*. New York: John Wiley & Sons, 1987.
3. Agrait, Rebecca, et al. "Abbreviated Reviews of 100 Models, Simulations, and Games for Domestic Preparedness Training and Exercising." Prepared for the Department of Homeland Security. Vienna, VA: ThoughtLink, Inc, 2004. Accessed online at http://www.ojp.usdoj.gov/odp/docs/Abbreviated_Product_Reviews.pdf
4. Aledort, Julia E., Nicole Lurie, Karen Ricci, David J. Dausey and Stefanie Stern. "Facilitated Look Backs: A New Quality Improvement Tool for Management of Routine Annual and Pandemic Influenza." The RAND Corporation, Center for Domestic and International Health Security 2006. Accessed online at http://www.rand.org/pubs/technical_reports/TR320
5. Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston, MA: Little, Brown and Company, 1971.
6. Argyris, Chris and Donald A. Schön. *Theory in Practice: Increasing Professional Effectiveness*. San Francisco, CA: Jossey-Bass, 1974.
7. Bloggers' Blog. "Bloggers Cover the California Wildfires, Part II." (Posted October 25, 2007) Accessible online at: <http://www.bloggersblog.com/cgi-bin/bloggersblog.pl?bblog=1025071>
8. Caralli, Richard A., James F. Stevens, Charles M. Wallen, and William R. Wilson. "Sustaining Operational Resiliency: A Process Improvement Approach to Security Management." Software Engineering Institute, Carnegie Mellon University, Networked Systems Survivability Program. CMU/SEI-2006-TN-009. 2006.
9. Carley, Kathleen, et. al. "BioWar: A City-Scale Multi-Agent Network Model of Weaponized Biological Attacks." Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Technical Report CMU-ISRI-04-101. 2004. Accessed online at: http://www.casos.cs.cmu.edu/publications/papers/carley_2003_biowarscalablemulti.pdf
10. C4ISR Architecture Working Group (1998) "Levels of Information Systems Interoperability (LISI)" US DoD, March 1998, cited in Knight, Michele, Les Vencel and Terry Moon. "A Network Centric Warfare (NCW) Compliance Process for Australian Defence." Australian Government, Department of Defence, Defence Science and Technology Organisation. Accessed online at <http://dSPACE.dsto.defence.gov.au/dSPACE/bitstream/1947/4555/4/DSTO-TR-1928.PR.pdf>

11. Carnegie Mellon Software Engineering Institute. "Capability Maturity Model® Integration (CMMISM), Version 1.1." Carnegie Mellon University, 2002. Accessed online at <http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr012.pdf>.
12. Carr, Nicholas. "McLuhan's Web". Rough Type: Nicholas Carr's Blog (November 1, 2007). Accessed online at http://www.rough.type.com/archives/2007/11/mcluhans_net.php
13. Carter, Ashton B. "The Architecture of Government in the Face of Terrorism." *International Security* 26 (3) (Winter 2001/02): 5-23. 2001. Accessed online at http://www.belfercenter.org/publication/350/architecture_of_government_in_the_face_of_terrorism.html.
14. Colwell, Rita R. "Global Climate and Health: Predicting Infectious Disease Outbreaks." *Innovations*. 1 (3): 19-23. 2007.
15. Continuity Insights/KPMG. "Final Results: A Review of the Factors Influencing Business Continuity Management Programs." 2007. Accessed online at <http://www.continuityinsights.com/eprise/main/SiteGen/Uploads/Public/continuity/documents/CIKPMG2007FinalResults.pdf>
16. Dewey, John. *Human Nature and Conduct: An Introduction to Social Psychology*. (New York: Modern Library, 1930.)
17. Davenport, Thomas and Laurence Prusak. *Working Knowledge*. (Boston, MA: Harvard Business School Press, 1998).
18. Davis, Lois M. et al. *Combating Terrorism: How Prepared Are State and Local Response Organizations?* RAND Corporation. (2006a). Accessed online at <http://www.rand.org/pubs/monographs/MG309/>
19. Davis, Lois M., et al. "Public Health Preparedness: Integrating Public Health and Hospital Preparedness Programs." The RAND Corporation, Center for Domestic and International Health Security (2006b). Accessed online at http://www.rand.org/pubs/technical_reports/TR317
20. DeMarines, Victor A., David Lehman and John Quilty. "Exploiting the Internet Revolution." *Keeping the Edge: Managing Defense for the Future*. Eds. Carter, Ashton B., and John P. White. Cambridge, MA: Preventive Defense Project, September 2000. 61-102. Accessed online at http://www.belfercenter.org/files/kte_ch3.pdf
21. Department of Defense, Office of the Chief Information Officer. "DoD Net-Centric Data Strategy." 9 May 2003. Accessed online at <http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf>
22. Department of Defense Information Sharing Executive, Office of the Chief Information Officer. "Department of Defense Information Sharing Strategy." 4 May 2007. Accessed online at <http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf>
23. Department of Health and Human Services, Office of the Secretary. "Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations." 2 September 2005. Accessed online at <http://www.hhs.gov/ocr/hipaa/KATRINAnHIPAA.pdf>

24. Eisenmann, Thomas R., Geoffrey Parker, and Marshall W. Van Alstyne. "Strategies for Two-Sided Markets." *Harvard Business Review*, HBR OnPoint Enhanced Edition, October 2006
25. Federal Emergency Management Agency. "Incidence Command System Training." September 2005. Accessed online at <http://training.fema.gov/EMIWeb/IS/ICSResource/assets/reviewMaterials.pdf>
26. Financial Services Technology Consortium. "The Joint Industry Executive Session on Minimum Essential Finance: Defining, Developing, Testing/Proving and Implementing Measures to Assure Minimum Essential Functionality of the US Financial Services System". Unpublished monograph, 2004.
27. Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "2006 Annual Report". Accessed online at https://www.fsscc.org/reports/2006/annual_report_2006.pdf
28. Gilligan, Carol. "In a Different Voice: Women's Conceptions of Self and of Morality." *The Future of Difference*. Eds. Eisenstein, Hester, and Alice Jardine. New Brunswick, NJ: Rutgers University Press, 1985.
29. Gladwell, Malcolm. *Blink: The Power of Thinking Without Thinking* New York: Little, Brown and Company, 2005.
30. Halberstam, David. *The Best and the Brightest*. New York: Random House, 1969.
31. Heymann, Philip B. and Juliette N. Kayyem. *Protecting Liberty in an Age of Terror*. Cambridge, MA: The MIT Press, 2005.
32. Howitt, Arnold M. and Herman B. "Dutch" Leonard. "Beyond Katrina: Improving Disaster Response Capabilities." Center for Public Leadership Working Papers, John F. Kennedy School of Government, Harvard University. Spring 2006. Accessed online at http://www.ksg.harvard.edu/taubmancenter/emergencyprep/downloads/beyond_katrina.pdf
33. Howitt, Arnold M., and Robyn L. Pangi. "Introduction." *Countering Terrorism: Dimensions of Preparedness*. Eds. Howitt, Arnold M., and Robyn L. Pangi. Cambridge, MA and London, England: The MIT Press, 2003. 17-36
34. Interagency Working Group on Earth Observations of the NSTC Committee on Environment and Natural Resources ("IEOS"). "Draft Strategic Plan for the U.S. Integrated Earth Observation System." 2004. Accessed online at http://usgeo.gov/draftstrategicplan/IEOS_draft_strategic_plan_111004.pdf
35. Kohlberg, Lawrence. "Education for Justice: A Modern Statement of the Platonic View." In Theodore R.Sizer and Nancy F. Sizer, (Eds). *Moral Education*. Cambridge, MA: Harvard University Press, 1970.
36. Klein, Gary A. *Sources of Power: How People Make Decisions*. Cambridge, MA: MIT Press 1999

37. Lagadec, Patrick, Erwann O. Michel-Kerjan, and Ryan N. Ellis. "Disaster via Airmail: The Launching of a Global Reaction After the 2001 Anthrax Attacks." *Innovations* 1 (3) 2006.
38. Lagace, Martha. "Open Source Science: A New Model for Innovation: Q&A with Karim R. Lakhani." Harvard Business School Working Knowledge for Business Leaders. November 20, 2006. Accessed online at <http://hbswk.hbs.edu/item/5544.html>
39. Leonard, Herman B. "Dutch" and Arnold M. Howitt. "High Performance in Emergency Preparedness and Response: Disaster Type Differences." Taubman Center Policy Brief PB-2007-3. A. Alfred Taubman Center for State and Local Government, John F. Kennedy School of Government, Harvard University. May 2007. Accessed online at http://www.ksg.harvard.edu/taubmancenter/pdfs/peril_new.pdf
40. Lundquist, Susan (ed.). "Remote Sensing Information Matrix". U.S. Environmental Protection Administration. 2007. Accessed online at http://pugetsound.epa.gov/images/d/d0/Matrix_v4_Print.xls
41. Marcus, Leonard J., Barry C. Dorn, and Joseph M. Henderson. "Meta-Leadership and National Emergency Preparedness Strategies to Build Government Connectivity." In, Working Papers 2005. Center for Public Leadership, John F. Kennedy School of Government. Accessible online at <http://www.ksg.harvard.edu/leadership/Pdf/MarcusDornHendersonWorkingPaper.pdf>
42. May, Ernest R. "Lessons" of The Past: The Use and Misuse of History in American Foreign Policy. New York: Oxford University Press. 1973.
43. The Markle Foundation. "Part Two: Working Group Analyses." Protecting America's Freedom In The Information Age: A Report of the Markle Foundation Task Force, October 2002. Accessed online at http://www.markle.org/downloadable_assets/nstf_part_2.pdf
44. Matzler, Kurt, Franz Bailom, and Todd A. Mooradian. "Intuitive Decision Making" MIT Sloan Management Review 49 (1): 13-15. 2007. Accessed online at <http://sloanreview.mit.edu/smr/issue/2007/fall/08>
45. McAfee, Andrew. The Impact of Information Technology (IT) on Businesses and Their Leaders. "The 9x Email Problem". Blog entry, September 29, 2006. Accessed online at: http://blog.hbs.edu/faculty/amcafee/index.php/faculty_amcafee_v3/entry/the_9x_email_problem
46. McLuhan, Marshall. *Understanding Media: The Extensions of Man*. Cambridge, MA: The MIT Press, 1994.
47. Mechling, Jerry. "Back-Office Transformation: Why and How," paper written for the National Association of State Auditors, Comptrollers and Treasurers (NASACT) and the National Electronic Commerce Coordinating Council (ec3) NASACT Symposium paper, and presented at the ec3 Annual conference, Sacramento, California, December 2006. Accessed online at http://www.ec3.org/symposia/white_paper.pdf.
48. Mickelson, Erik, Zachary Tumin, and Jerry Mechling. "Varieties of Shared Services in the Public Sector." Leadership for a Networked World Program, John F. Kennedy School of Government Harvard University. Working Paper 06-2007.

49. Mittu, Ranjeev. "Unclassified Information Sharing and Coordination in Humanitarian Assistance and Disaster Relief." Presentation given at Collaborative Expedition Workshop #63, Towards Stable Meaning and Records Preservation in Information-Sharing Building the Way Forward Together. July 17-18, 2007. Accessed online at http://colab.cim3.net/file/work/Expedition_Workshop/2007-07-17_TowardsStableMeaningAndRecordsPreservation/Mittu_InfoSharing_HumanitarianAssist_200717.ppt
50. National Weather Service, National Oceanic and Atmospheric Administration. "Situation Awareness and Decision Making in a Warning Environment." Advanced Warning Operations Course, IC Core 2, Lesson 3: Team SA. Accessed online at <http://www.wdtb.noaa.gov/courses/awoc/ICCore2/Lesson3/player.html>
51. Plato. Laches & Charmides. Rosamond Kent Sprague, translator. Indianapolis: Bobbs-Merrill, 1973.
52. Program Manager, Information Sharing Environment. "Information Sharing Environment Implementation Plan." 2006. Accessed online at <http://www.ise.gov/docs/ise-impplan-200611.pdf>
53. Royal Aeronautical Society/Human Factors Group (RAES-HFG). "Situation Awareness Definitions Collected During the JAA ESSAI Project." Accessed online at <http://www.raes-hfg.com/crm/reports/sa-defns.pdf> (2000?)
54. Schein, Edgar H. Organizational Culture and Leadership. San Francisco: Jossey-Bass Publishers, 1992.
55. Schön, Donald A. Beyond the Stable State. New York, NY: Random House, 1971.
56. Schön, Donald A. Educating the Reflective Practitioner: Toward a New Design for Teaching and Learning in the Professions. New York, NY: John Wiley & Sons, 1990.
57. Seid, Michael, Debra Lotstein, Valerie L. Williams, Christopher Nelson, Nicole Lurie, Karen A. Ricci, Allison Diamant, Jeffrey Wasserman and Stefanie Stern. "Quality Improvement: Implications for Public Health Preparedness." The RAND Corporation, Center for Domestic and International Health Security 2006. Accessed online at http://www.rand.org/pubs/technical_reports/TR316
58. Sparrow, Malcolm K. License to Steal: Why Fraud Plagues America's Health Care System. Boulder, CO: Westview Press, 1996.
59. Sparrow, Malcolm K. Imposing Duties: Government's Changing Approach to Compliance. Westport, CT: Praeger Publishers, 1994.
60. Stark, Mallory. "How 'Career Imprinting' Shapes Leaders: Q&A with Monica Higgins." Harvard Business School Working Knowledge for Business Leaders. February 7, 2005. Accessed online at <http://hbswk.hbs.edu/item/4610.html>
61. Taleb, Nassim Nicholas. The Black Swan. New York, NY: Random House, 2007
62. Toffler, Alvin. Future Shock. New York, NY: Random House, 1971.

63. Tolk, Andreas. "Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability." Presented at 8th International Command and Control Research and Technology Symposium, National Defense University, June 2003. Accessed online at <http://www.vmasc.odu.edu/pubs/tolk-beyond01.pdf>
64. Tumin, Zachary. Maritime Domain Awareness A Case Study in Cross-Boundary Information Sharing Among the United States Navy, Coast Guard, and Department of Transportation. Harvard University Teaching Case, 2007(a). Accessible online at: <http://www.lnwprogram.org/file-storage/view/0.229607251122/Maritime%20Domain%20Awareness%20Final%20Rev.10.19.07.pdf>
65. Tumin, Zachary. "The Strategy of the Executive Sponsor: Six Images". Class Note 06.2207. Harvard University 2007(b). Accessed online at <http://www.lnwprogram.org/file-storage/view/0.229607251122/Six%20Images%20of%20Executive%20Sponsors.pdf>
66. Tumin, Zachary. LA JRIC: The Los Angeles Police Department and the Global War on Terror. Harvard University Teaching Case, 2007(c) Accessed online at <http://www.lnwprogram.org/file-storage/view/0.229607251122/LA%20JRIC%20Final%20Rev.%2010.19.07.pdf>
67. Tumin, Zachary. MITA and Medicaid Transformation. Harvard University Teaching Case, 2007(d). Accessed online at <http://www.lnwprogram.org/file-storage/view/0.229607251122/MITA.pdf>
68. Tumin, Zachary. Iowa's Recovery Center. Harvard University Teaching Case, 2007(e). Accessed online at <http://www.lnwprogram.org/file-storage/view/0.437152769055/Iowa%20Recovery%20Center%20Ver%205.21.07.pdf>
69. Henricksen, Barry. United Nations Spatial Data Infrastructure Vision, Implementation Strategy and Reference Architecture Draft Discussion Paper. October 2006 .Accessed online at <http://www.ungiwg.org/docs/unsdi/UNSDI%20Draft%20Discussion%20Paper%2025-10-'06.pdf>
70. Wikipedia, The Free Encyclopedia.. "October 2007 California Wildfires". Accessed online at: http://en.wikipedia.org/wiki/October_2007_California_wildfires (2007)
71. World Health Organization. "WHO pandemic influenza: draft protocol for rapid response and containment." Updated draft 30 May 2006. Accessed online at http://www.who.int/csr/disease/avian_influenza/guidelines/protocolfinal30_05_06a.pdf