WHOLENESS IN COMPLEX SOCIO-TECHNICAL SYSTEMS

William J. Toth

100 Westview Ln

Oak Ridge, TN 37830

Saybrook University

wtoth@saybrook.edu

ABSTRACT

Highly complex social and technological systems are ubiquitous in the modern world. Many of these systems are associated with high levels of energy; potential, kinetic, and human. The consequences of system failure can be extreme. Observation of catastrophic technological failures such as two space shuttle disasters, the nuclear power plants at Chernobyl, Three Mile Island and Fukushima, and many others, show clearly that creators and managers of these systems must take great care with system design and operations. Human system failures such as those seen in espionage or mass killing cases also highlight the need for both responsible and humane organizational management and sustained attention to defensive measures.

Lack of attention to any of vast systemic issue both social and technical can result in organizational or defense system defects. These defects can be described as *holes* or *shadow aspects* and these pertain to the technical systems, the human systems and the socio-technical system interplay. Responsible technology and social system design requires addressing these holes and shadow aspects to eliminate them and therefore make the system complete or *whole*. Organizational *wholeness* is a continuous process of attention to and mitigation of these types of defects. *Sustainability* in this context is the continued focus on safe and secure operations and life affirming human dimensions to respond to environmental changes and adjust defenses accordingly. This paper will describe propose a model that may be useful for hole and shadow aspect identification and issues related to their management or mitigation.

Keywords: wholeness, socio-technical systems, sustainability.

INTRODUCTION

The structure of human civilization has undergone sweeping changes over the eons. Qualitative evaluations of what is emerging in recent decades in organizational life highlights unprecedented complexity. Human organizations are becoming larger and more interconnected. Technologies are increasing in capability and humans endeavor to do more economically and socially with them (Bar-Yam, 2002). Generally, these socio-technical endeavors are beneficial and add to the welfare and mobility of community members. Sometimes, however, systems fail and often, the consequence of failure can be quite high.

Systems that aid in the mobility of people include the most visible ones, like airplanes, automobiles, and trains. Because many of these involve the transportation of large numbers of people in the same vehicle, accidents can result in many deaths. Broadening the systemic view, the energy source for these transportation systems is generally produced by processing oil, coal, or natural gas. Acquiring these resources and delivering them as usable products also rely on complex systems involving drilling rigs, pipelines, seagoing vessels, refineries, and end-product distribution systems. Accidents such as explosions, spills, or fires at any point in this supply chain can have devastating effects on adjacent populations or the environment.

Supporting general welfare by providing environmental comforts, work productivity, and entertainment for people involves systems of power generation and distribution. Fossil fuel supply chains are also relevant here, but modern systems also include nuclear power generation stations. Nuclear power offers opportunities for accidents of a different type, potentially with even greater and more long lasting consequences to populations and the environment.

General welfare for humans also includes protections from naturally occurring events such as fires, earthquakes, tornadoes, and tsunamis. Protective elements such as weather prediction systems, communications systems, building codes and standards, public shelters, and emergency response systems, have generally improved our ability to cope with naturally occurring events, but they too sometimes fail, resulting in unnecessary death and economic impact.

Complex organizational systems are also employed in modern times for education, governance, service, and production. Independent of the product or service of an organization, complexity introduces new opportunities for high consequence failure. Organizing humans for harmonious and cooperative effort is a difficult thing to do. From a broad, worldwide perspective, one can observe a vast number of deaths from geo-political and tribal conflict over the last 600 years (Roser, 2012). These statistics illustrate the consequences of failure in human communities from the smallest to the largest. Government intelligence agencies playing high-stakes games with foreign entities, in hot or cold conflict, can experience organizational failures that have extreme consequences. Espionage represents one socio-technical system failure in this context. Release of intelligence information has resulted in many deaths and other costly consequences. This is objectively true, regardless of how one feels about the legitimacy of these games. The reality is that tensions and potentials exist that are driven by human nature's proclivity to conflict. As with the inevitability of natural disasters, human crimes and malevolent actions are also assured and how we manage our organizations and integrate protective measures, can determine the magnitude of the impact.

In a deceivingly more benign environment, we can observe organizational failures of high consequence. Educational institutions are examples of highly visible organizational systems where increasing complexity introduces opportunities for different kinds of tragedies. Individuals who make up these organizations are heterogeneous and community leaders must be on guard for those individuals who become disaffected by consciously designed organizational forces, or less conscious structural dynamics. Because so many people in the U.S. have access to destructive weapons, the disaffected

community member may act out in violent ways. Organizations must be concerned with both the failures that result in disaffected, violent community members, and the failures of the protective systems, given the inevitability of certain events.

In a scenario that played out at the intersection of geo-political conflict and normal urban life, planes were hijacked to destroy buildings. In arguably the most dramatic and feared terrorist scenario, improvised nuclear devices might be detonated in major metropolitan areas. Thankfully this postulated threat has not been realized, but the fear of it remains the justification for billions spent on nuclear nonproliferation efforts worldwide (Schwartz & Choubey, 2009).

This paper presents a discussion about disasters from the organizational systems perspective. This is distinct from the post-disaster, root cause analysis approach that seems to be most common for government regulated organizations. For example, a mass-killing at an elementary school often elicits intense investigation into the perpetrator and his or her motive. Less emphasized are the organizational factors that might have driven the person to the act of violence, or the warning signs that went unheeded. Considering the high profile shootings of the past 20 years, these organizational issues are sometimes discussed, but investigations often focus preferentially on seeking relatively limited root causes such as violent video game playing (Bushman & Anderson, 2002) or the psychopathology of the perpetrator. In a similar way, the public seems to want to find singular or limited root cause failures for high profile technological disasters. This is evidenced by media coverage that is "event centered" (Anderson, 2002, p. 8) such as in the case of the Exxon Valdez disaster where the focus of attention was on Captain Joseph Hazelwood and his drunken state. "Event centered" is another way of describing the focus on a single root cause, without seeing broader systemic issues. Often the root cause is selected because it is familiar and thus an acceptable explanation, or it is one for which mitigating action can be taken to satisfy a fearful public (Leveson, 2011). True systemic understanding of causes of failure can become overwhelming as one can always add contributing factors to earlier stages in the causal chain.

Background

Many years of professional experience with socio-technical systems and significant academic study of organizational effectiveness has lead me to questions about organizational phenomena described in this paper. My focus is on high consequence failures of complex socio-technical systems. Though this discussion is about dark and tragic events, it is important to help raise awareness of systemic issues. The events of interest represent high consequence failures and include disasters, crises, crimes and tragedies. In the development of a theoretical model, I propose metaphors that describe the system defects that contribute to failure or the lack of protections to inevitable catastrophes. One metaphor is that there are *holes in the systems* that contribute to failures, if not their direct cause. These holes relate to myriad defenses that provide protections for people and the environment. Holes also represent the lack of other features that render a system incomplete for safe, secure, and responsible operation. I will use the hole metaphor to describe socio-technical system defects, but there may be literal holes in technological systems as well. In this respect, a hole is an effective metaphor because it describes a defect or a gap in defenses. A hole represents a place

where a perpetrator could penetrate a security system or energy could escape and injure people or hurt the environment.

The other useful metaphor is that there are *shadow aspects* to the systems that may obscure critical systemic elements, or important organizational dynamics. Shadows may also represent forces that are hostile to humanistic values. Organizations are often not conscious of these forces. Shadows may also be organizational characteristics that are inconsistent with espoused values and are therefore suppressed. Technologically, shadow aspects may represent neglected parts of complex systems, both in design and operation. From a human systems perspective, shadows represent the undeveloped or unrecognized human dimensions for which we have no resources or competency to confront.

The shadow metaphor is influenced by Jungian psychology and is my application of a modified definition of shadow to socio-technical systems. Shadow helps describe dysfunction that can have serious consequences. The shadows from Jung's perspective are intra-psychic forces that can have individual or collective forms. Shadows are described as "…our dark side, the inborn collective predisposition which we reject for ethical, aesthetic, or other principles" (Jacobi, 1973, p. 110). Applying Jung's ideas to the organizational setting, these "other principles" could be aspects that are not in keeping with the public image of the organization. For example, shadow aspects could be reflected in a felt sense of institutional racism, despite outward proclamations about a commitment to workforce racial diversity. Shadow forces could manifest in workplace or community incivility, subtle hazing, or bullying. Individuals could be victimized and become disaffected by these forces. Some individuals may retaliate, even violently, against the organization.

Shadow aspects might also describe a lack of competence for responsible holistic system design and therefore, a lack of attention to required protective elements. One example of many is the Champion paper mill near Canton, North Carolina that discharged effluents into the Pigeon River, effectively killing the river biologically, for nearly 100 years (Coombs, 2004). Despite their persistent lack of attention to environmental protections, Champion maintained a very positive company image as a local employer that even boasted helping North Carolina communities through the Great Depression (Bell, 2006). This characteristic of a bright, wholesome public image with darker destructive aspects is common, and is a fitting expansion of Jung's idea of shadow.

From a human perspective, organizing people for work, education or community life is a complex and important task. If one does not consider human system dynamics with great care, people can become lost and disaffected. Shadow aspects in this context represent the organization, poorly designed and managed, that does not allow for natural human development, and therefore encourages anti-social behavior including the possibility of violent backlash. The shadow example of Champion paper described in the preceding paragraph manifested physically. In other words, the image of the company was belied by lack of attention to environmental protections, and a river was killed. The social systems shadow manifests less tangibly. Rayner and Cooper use the celestial phenomenon of the black hole as a metaphor to describe how difficult it can be to identify organizational shadow aspects such as the perpetrators of workplace bullying (Rayner & Cooper, 2003). Organizational shadows of this type may contradict espoused values such

as a company's care for people. The lived experience of certain employees may include a felt sense of racism or that no one cares about them personally.

The antithesis of this dark perspective is that organizations can have awareness of these holes and shadow aspects and intentionally address them. In the theoretical model proposed, the organization's lack of attention to holes in defenses, or reconciliation with shadow aspects is described as dis-integrated. Integration of the many parts of a complex organization is required for an organization to be *whole*. This *wholeness* is important for all organizations but particularly so for those where systemic failure includes the possibility of tragic impact on individuals in the organization, the broader community or the environment. Recognizing systemic holes and shadow aspects and improving organizational design and functioning to accommodate them, fix them, or learn from them is but one way to move towards organizational wholeness. This term is proposed in opposition to the idea of organizational *perfection*, which implies a singular end state and a linear path to that state of perfection. Organizational perfection is a notional concept and any definition, even if attempted, would be incomplete. Respecting the complexity in socio-technical systems requires recognition that organizations develop on a number of fronts simultaneously, always respecting the generative nature of the process. Implicit in this unfolding process of becoming whole is that the end state cannot predicted with any accuracy.

Organizational wholeness should start at the earliest stages of conception and design and continue through the operational and divestment stages of an organization's life-cycle. Stakeholders generally consider benefits and costs for economic viability. A focus on wholeness would require other considerations such as the probability of safe operations, and acceptable impact on organizational members, the general public, and the natural environment. Some of these concerns are described in the literature broadly as issues of *corporate social responsibility (CSR)*. Judging by the myriad regulatory agencies and a cynical view of CSR as related by Arthur et al., (2007) one may conclude that companies are unlikely to consider anything other than profitability in their decision making. Considering the systemic impacts of a socio-technical endeavor is critically important, but unlikely in the face of economic drivers. One can only hope that regulations and normative forces such as CSR will work together to encourage broader consideration of human and environmental protections, but system complexity will likely leave many stones unturned. Organizational wholeness requires a self-motivated commitment to systemic understanding, which is not likely in the modern competitive environment. Government supported enterprises such as power stations or oil supply lines crossing government land stand a better chance for systemic analysis, but this comes at a cost of oppressive regulations that stifle productivity and innovation. The acceptance of the need for organization wholeness would manifest in organizations performing systemic analyses and providing for protections as their self-accepted responsibility with only minimal influence from supra-organizational authorities and their regulations. This seems unprecedented in the modern corporate environment.

Wholeness in human systems making up various organizational settings involves responsible social systems design and management based in humanistic principles. Returning to Jung's ideas, wholeness and health in the individual involves recognition

and integration of the disparate parts of the psyche. Jung calls this process *individuation* and it leads to the highest aspiration of individual life (Jacobi, 1973). I argue that socio-technical systems and modern organizations must have similar aspirations. Disparate parts of the individual human psyche are analogous to the vast parts of complex organizational systems. As with the individual, organizational health and high functioning requires recognition and accommodation of all systemic components. Tensions between the rational aspect of the individual psyche, or the ego, and unconscious aspects of the psyche can result in neuroses, that can manifest as depression, confusion, delusions, anxieties, and other disorders (Horney, 1950). In the organizational analog there can be similar tensions between rational aspects such as organizational definitions, company slogans, stated values, and other overt publications and proclamations; and unconscious organizational forces. These represent shadow aspects and can include strong normative forces, informal organizations, incivilities and hostility, peer evaluation and cliques, and other malevolent activities. A lack of reconciliation between these conscious and unconscious or shadow forces can create neuroses at an organizational level. Despite the tendency towards dysfunction, decades of organizational development (OD) literature has shown that organizations can attend to these tensions and function quite well. That same literature is helpful in explaining the dysfunction, though it generally does not use the term wholeness. OD and organizational psychology continues to evolve, but the literature shows that there are many organizations that still give little respect to human needs. Wholeness means that we hire well, train well, support employees or community members wisely, and make allowance for natural human development. Neglect of systemic wholeness can lead to complex system's defense degradation and ultimately to significant defense breakdowns that allow disasters, crises, crimes and tragedies to happen. Wholeness implies an adaptive system that is constantly aware of change. In this way, *sustainability* becomes an important concept and is defined as a constant commitment to wholeness despite constant change.

Defining Terms: Disasters, Crises, Crimes, and Tragedies

One often hears the word "disaster" coupled with the word "natural" and most definitions focus on natural events that cause loss of life and property. "Tragedy" is a word that is often used when describing mass killings of innocent people. Tragedy is also used to describe the aftermath of a terrorist attack. "Crisis" is a term sometimes used to describe hardship that plays out over time, such as "a period of economic crisis," but a period of crisis could be triggered by a disaster. A "crime" is typically an intentional malevolent act that may be the cause of a disaster, or usher in a period of crisis.

The term disaster is used by Taylor (1987) to create a taxonomy of all of the potential manifestations presented in Table 1. This is fairly large collection that includes most of the focus areas of this inquiry. Many items in Table 1 will not be addressed, but this taxonomy is useful for orientation. It shows the many frames within which undesirable things can happen. Implied are the impacts to people and the environment, so the taxonomy can be useful for starting the discussion about responsibility and stewardship.

Table 1 (Taylor, 1987 p. 537)

	Natural	Industrial	Humanistic
Earth	Avalanches	Dam failures	Ecological irresponsibility
	Earthquakes	Ecological neglect	Road and train accidents
	Erosions	Landslides	
	Eruptions	Outer space debris fallout	
	Radon deposits	Radioactive pollution	
		Substances	
		Toxic waste disposal	
Air	Blizzards	Acid rain	Aircraft accidents
	Cyclones	Chemical pollution	High jacking
	Dust storms	Explosions over and underground	Spacecraft accidents
	Hurricanes	Radioactive cloud and soot	
	Meteorite and planetary activity	Urban smog	
	Thermal shifts		
	Tornadoes		
Fire	Lightning	Boiling liquid/expanding vapor accidents	Fire-setting
		Electrical fires	
		Hazardous chemicals	
		Spontaneous combustion	
Water	Droughts	Effluent contamination	Maritime accidents
	Floods	Oil Spills	
	Storms	Waste disposal	
	Tsunamis		

People	Endemic disease	Construction accidents	Civil strife
	Epidemics	Design flaws	Criminal extortion by virus and poisons.
	Famine	Equipment problems	Guerilla warfare
	Overpopulation	Illicit drug making and taking	Hostage-taking
	Plague	Plant accidents	Sports crowd violence
			Terrorism
			Warfare

Missing in this taxonomy are explicit categories for espionage and sabotage, but they can be included in some of Taylor's broader categories. For instance, mass killings can be categorized under "terrorism." Also missing is an emphasis on information technology, clearly because Taylor's analysis was from a time where this was not as prominent.

Another model for understanding high consequence, undesirable events comes from Ian Mitroff (1988). He uses the term "crisis" in his writings about crisis management. His organization of various crises, in a model is also quite useful for the understanding of these events, their distinguishing features, and the suggestions for mitigation efforts. Mitroff offers his own taxonomy and typology that adds a beneficial dimension. This model is shown in Figure 1 (Mitroff, Pauchant, & Shrivastava, 1988).

Using an application of Jungian typology, Mitroff differentiates crises that arise from within, or internal to, an organization and those that arise external to it. Mitroff sees likeness between this categorization and Jung's introvert/extrovert and sensing/intuiting classifications. Mitroff's work emphasizes the differences in approach in mitigation and response to the various crises types.

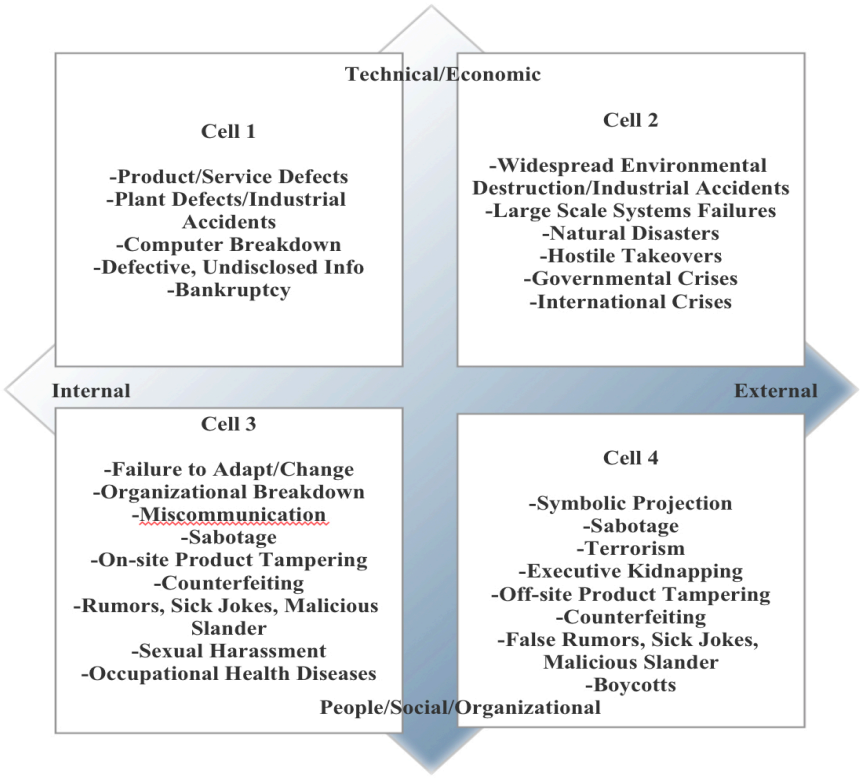

Figure 1: Mitroff's Crisis Management Model

One characteristic that might distract from attention to the importance and systemic nature of these crises, disasters, tragedies, and crimes, is the postulated event's probability. Imagination can produce endless possible threats, and one may become overwhelmed by possible risks with any endeavor. Which of these events are worth considering for mitigation plans or protective measures? It is a difficult question. United States intelligence agencies were considering a number of attack scenarios including ones related to attacks on the homeland (National Commission on Terrorist Attacks upon the United States, 2004) prior to the September 11, 2001 (9/11) attacks. Mitigation plans that may have included some defenses for airplanes being used as bombs to destroy buildings, and other attack scenarios would have been infeasible. Prior to 9/11 the very low probability of these events likely allowed them to be dismissed. Despite this, organizations cannot use the low probability of the postulated threat as cover for neglecting more basic protective measures. Regardless of the probability of an internal attack such as a mass killing in a workplace or school, there is no excuse for managing organizations in a way that disaffects or exiles employees or community members.

The taxonomies presented are extensive, but not exhaustive. They represent a wide variety of disasters, crises, crimes, and tragedies to illustrate common families of events and are used to guide mitigation or response efforts. My thesis is that, among high profile cases of disasters, tragedies, crimes and crises, there are common characteristics that describe archetypal organizational deficits. These deficits fit the proposed metaphorical description of holes and shadow aspects, and therefore represent a lack of organizational wholeness. This lack of wholeness can be described from two perspectives. The first perspective involves dysfunctional human interaction with an organization that results in a malevolent action such as theft, sabotage, espionage, or mass killing. This perspective breaks down further as organizational forces that contributed to the development of this malevolent human insider threat, or the organization's inability to see the insider activity at an early enough stage to avert the crisis. The second perspective focuses more on the technical aspects of the socio-technical systems. Specifically, this relates to the organization's responsible and ethical stewardship of large, high consequence technical systems, their support infrastructure, and the defenses necessary for the protection of the environment and communities. When things go terribly wrong, what were the organizational systems holes and shadow aspects surrounding this failure, and how were these holes and shadow aspects created? Was the complex system designed ethically and responsibly? Were the potential hazards considered and were mitigating measures included in the design? Given that with sufficient complexity, certain disasters and crises are inevitable, was the organization able to respond appropriately and was there sufficient resilience built in to the system to recover and return to productive and safe operation? Again, the focus is on design and awareness of the whole system's operation and potential failure modes. What was neglected?

Human Insider Threats to Socio-Technical Systems.

Both Mitroff and Taylor's typologies have clearly identified the human involvement in crises and disasters. Many modern, complex organizations create, process, or are otherwise responsible for assets of high value or high consequence if stolen or inappropriately used. Examples of these assets include dangerous chemicals, biological agents, nuclear materials, radiological materials, or explosives. An attack on a facility responsible for these materials would include theft or diversion, sabotage, or espionage. Security measures employed at facilities generally focus on attacks from the outside as evidenced by locked doors, fences and surveillance systems. Attacks by employees or other authorized personnel with privileged access to facilities and secure areas are more difficult to guard against. These *insider threats* are a focus area for organizations such as the International Atomic Energy Agency (IAEA), the U.S. Nuclear Regulatory Commission (Satorius, 2015), the U.S. Department of Energy (2014), and a growing number of information technology companies (Vormetric Data Security, 2015).

The IAEA defines an adversary as any individual performing or attempting to perform a malicious act (2008). These adversaries may be insiders or outsiders. The insider can be considered more dangerous than the outsider because they have authorized access to the facilities and can cause damage where organizations are most vulnerable. An insider colluding with an outsider is particularly dangerous as the insider can facilitate an

effective outside attack by disabling alarms or providing access to locked areas. From the information technology industry, this definition of the insider is offered; "…a trusted entity that is given the power to violate one or more rules in a given security policy…the insider threat occurs when a trusted entity abuses that power" (Wall, 2013, p. 108). The motivations identified by the IAEA include financial, ideological, or psychopathological. Though the IAEA definition represents a typical characterization of insider motivations, it is too simple and does not account for the individual and organizational interaction. It is difficult, if not impossible to separate individual's motivations from the larger organizational system. Therefore, it is only useful to talk about individual predispositions towards malevolent actions. Organizations should be concerned about how those so pre-disposed might react given particular organizational circumstances. These circumstances include a wide variety of organizational dysfunctions that are common in the workplace and in communities. These dysfunctions are characteristics of an organization that lacks wholeness and is the antithesis of a progressively managed, organization emphasizing humanistic values. No organization is managed perfectly and even the best organizations can treat people poorly. I propose that organizational wholeness can evoke the best in people and lack of wholeness can evoke behavior with tragic consequences. Counter-examples may be found on either extreme. A few individuals might thrive or perform heroic acts despite poor organizational circumstances, and some people may commit terrible acts or be negligent in the best managed organizations. In these latter type cases, the person's predisposition dictated the outcome. It is, of course impossible to determine how many people who were predisposed to malevolent action decided not to act out. If this is a large number, we can hold some hope for humanity, but we cannot allow that idea to distract from the responsibility, given high consequences if systems fail, to organize responsibly and treat people well. Organizations responsible for high consequence systems or materials must be designed and managed with OD and humanistic values accommodated. Failure to do so introduces shadow aspects into the human system where psychological predispositions can flourish.

Human Insider Threat to Communities

Attackers in other organizational settings may not have theft of high consequence materials as their aim; some simply want to hurt or kill people. People are vulnerable to murderous attack when they gather in workplaces, schools, churches, or other common areas. There is no broadly agreed to definition for *mass killings*, but one used by the FBI and other government agencies is "…incidents occurring in relatively public places, involving four or more deaths – not including the shooter(s) – and gunmen who select victims somewhat indiscriminately. The violence in these cases is not a means to an end such as robbery or terrorism" (Bjelopera, Bagalman, Caldwell, Finklea, & McCallion, 2013, p. 4). A U.S. federal law (112th Congress, 2013) updated the definition to three or more killed. If the insider can be defined as any trusted individual with access to sensitive facilities or communities, many of the mass killings that have happened in the United States were committed by an individual or individuals that can be considered an insider. The criterion is the individual's connection to the victims, and therefore inside the community of the victims. Data collected by Stanford Geospatial Center and Stanford Libraries (2015) shows that from 1966 to 2015 there were 154 events that fit the

mass killing definition of three or more killed, not including the shooter. Stanford's data coding indicates that 90.3% of the perpetrators had some connection to the victims by either being a part of their work, residential, school, or recreational communities. For this reason, they can be considered insiders to the community.

Socio-Technical Accidents

Given our increasing reliance on complex socio-technical systems, the issue of accident mitigation becomes ever more important. Most of the high profile cases of disaster, tragedy, crime, or crisis involve complex systems where incomplete design or neglectful management contributed to the ensuing catastrophe. Given the multiple events aligning with defensive system holes (Reason, 1997), one may rightfully question the categorization as "accident." Are these truly accidents or the results of negligence? Certainly it is the latter if systemic issues were known and ignored. Responsible design and management also includes the requirement that systems are understood to the fullest extent possible, and accommodation is made for protection of the workers, community members, and the environment. Might it also be contended that lack of systemic analysis and accommodation for high consequence systems is also a malevolent action? This would be a difficult area to say with certainty. Myriad product liability cases (Sundar, 2015) show that this is an active area of debate in the courts.

Anticipating and accommodating all possible failure modes is clearly not feasible. Excessive protections and redundancies can over-burden a system and possibly even introduce new complexities and unanticipated hazards (Reason, 1997). Required is a kind of design elegance that accommodates the most likely failure modes while still allowing for efficient operation. The passenger airline industry is inspiring in this respect. Each significant accident has contributed valuable lessons learned to the industry and improvements propagate throughout the worldwide fleet (Federal Aviation Administration, 2015). All of these improvements have been incorporated into a physically limited airframe as part of an elegant design with an impressive safety record. Of course the airlines are not without any incident, and they operate within a larger system that has its own flaws with respect to passenger comfort and overall security, but the long process of learning from failure modes and accommodating them in physical and procedural changes sets a worthy goal for other socio-technical systems.

Psychopathology of the Individual.

Undesirable actions by humans include espionage, sabotage, violent backlash, mass killings in the most extreme cases. Wholeness requires that we look at individual actions in the broader organizational context, but some individuals seem more psychologically predisposed to malevolent actions than others. Also concerning are predispositions to loss of attention and other types of human error. Personalities that might be more inclined towards accidents such as ones that are defiant, panicky, irritable, distractible, reckless, or arrogant (Hogan, 2016). The individual's predisposition to malevolent action is always of concern, but particularly so in organizations responsible for high value or high consequence assets. Organizational wholeness is critical from the humanistic value perspective so that those predisposed individuals are not encouraged on the malevolent pathway. It is, of course, impossible to prove a causal relationship between a predisposed

person's lack of undesirable actions and organizational functioning, but the lack of incident should not be used as an excuse for loss of commitment to wholeness.

Forensic psychologist Eric Shaw illustrates the pathway to malevolent behavior in the information technology industry with a pyramid (Shaw, 2011). Starting with the broadest level (1), and leading to the actual committing of the crime at the peak (5), he describes the following steps on the pathway.

1. Personal predispositions in individuals vulnerable to insider risk present prior to joining the organization such as: serious mental health problems, previous violations of the law, social skills problems or being a social or professional network risk;
2. Personal stressors such as: financial problems, relationship, marital or family difficulties, significant medical problems, legal problems or relocation;
3. Professional stressors such as: demotion or failure to achieve anticipated advance, loss of seniority or status, transfers, disappointing reviews or conflicts with workers;
4. Concerning behaviors such as: disruptive conflicts with coworkers or supervisors, violation of security policies, tardiness or missing work or violations of financial rules; and,
5. Maladaptive organizational responses to subject concerning behaviors such as: failure to detect the behavior, failure to investigate the concerning behavior, failure to appreciate the implications of and investigated or concerning behavior, failure to act or deal with the concerning behavior or reaction to the behavior that escalates risk (Shaw, 2011 pp. 7-8).

This pathway represents components building upon one another starting from personal predispositions compounded by organizational incompetency in dealing with the concerning behavior. The development of a malevolent actor given Shaw's pathway is a complex process that generally plays out over months or years before something terrible happens. The model shows opportunities for intervention in many places prior to the malevolent action.

Responsibility of the Organization to Their Human Community.

Relevant to technological accidents, lack of wholeness may discourage sustained attention, job competency, and continuous learning. Because of an event focused mindset and the tendency to seek a single point of failure in incident investigations, these myriad contributing causes will be obscured. What is our responsibility to organizational wholeness? The responsibility of organizations to the human community is to keep in mind that they are *part of* that human community. With respect to these critical issues and the high impact of failure to manage systems and people well, we see that OD and systems theory is not just for making more efficient organization; it may have impact a much broader sense of human welfare and possibly human survival. The responsibility prohibits the orientation that Martin Buber describes as "I-it" with respect to this new ontology that includes an ever increasing socio-technological reach (Buber & Kaufmann, 1970). Organizations will undoubtedly have to curtail the aggressive push for progress and product. Neither people nor resources should be seen as "its" in a productivity machine.

CONCLUSION

We endeavor to do more and more as the human community evolves. Our systems, be they technology based, human community comprised, or a combination of both, must be designed and managed appropriately to minimize the potential for disasters, tragedies, crimes, and crises. We should continue to hold question of whether we are acting responsibly when we attempt to harness the many energies associated with systems whose failure can have high consequences. Have we really considered these potentials? Consider the recollections of Dr. Robert Oppenheimer from an interview in 1965.

> *"We knew the world would not be the same. Few people laughed, few people cried, most people were silent. I remembered the line from the Hindu scripture, the Bhagavad-Gita. Vishnu is trying to persuade the Prince that he should do his duty and to impress him takes on his multi-armed form and says, "Now I am become Death, the destroyer of worlds." I suppose we all thought that, one way or another." - Robert Oppenheimer* (Giovannitti, 1965)

Dr. Oppenheimer was of course, instrumental in the creation of the atomic weapons that were later dropped on Hiroshima and Nagasaki, Japan at the end of World War II. My impressions from watching the short film clip are of a man who was deeply concerned, nearly moved to tears, in the consideration of what he created. This interview, nearly twenty years after the event gave Dr. Oppenheimer time to reflect as an older man on the systemic consequences of this technological advancement. One can only wonder what his mental state was just 10 years earlier, when during a hearing, he said, "When you see something that is technically sweet, you go ahead and do it and argue about what to do about it only after you've had your technical success. That is the way it was with the atomic bomb" (United States Atomic Energy Commission Personnel Security Board, 1954, p. 81). One may wonder still, ten years prior to that, and caught up in the "sweetness" of this scientific and technical accomplishment, if there was any reflection at all, or were he and his team energized only by what was possible. It does not take much reflection to see similar advancements in technology and organizational complexity today that is accompanied by complex interactions with multiple systems affecting the human community and environment. Oppenheimer and his team felt a sense of urgency, driven by war planners, to achieve the technological goal of creating a nuclear weapon. One may argue that there was not time to slow down and consider collateral issues. More recent urgencies also drive decisions about socio-technical systems, disallowing the time for consideration of systemic impacts. Organizational wholeness may be an aspiration, but organizations may not feel that they have the time for this level of responsibility.

Relative risk to life data indicates that there are a few familiar circumstances that are killing most of the people in the U.S. Among these are heart disease, cancer, and accidents or "unintentional injuries," a category that includes automobile accidents (Centers for Diease Control, 2015). Compared to the top killers, industrial accidents, terrorist acts, and mass killings could be dismissed as misplaced concern, as the death toll is not as great. They should not be dismissed, however. High profile incidents like the Exxon Valdez disaster, and the Hurricane Katrina aftermath had wide reaching effect on communities and our national psyche. Terrorist acts like those on 9/11 changed

American of life significantly and permanently. Accidents like the one at the Three Mile Island nuclear power plant dramatically changed our public policy decisions and our energy strategy. Motivating organizations to be concerned with wholeness will be difficult; sustaining a commitment to wholeness even more so. This is particularly true of corporations whose main focus is profit, or stakeholder wealth. While fear is a motivating emotion, its use is dangerous because it typically demands very quick, linear responses that don't allow time for systemic consideration (Finkelstein, Whitehead, & Campbell, 2009). Fear, coupled with event centered risk analysis measures can drive results that we see typified by the Transportation Security Administration at U.S. airports. The "security theater" that is the result is criticized harshly by Schnier (2009) as being ineffective to counter any real threat. Emergency response and communication were weaknesses uncovered by the 9/11 attacks and were subsequently dismissed as the country shifted to a terrorist centered strategy (La Porte, 2005). Fear is a fickle motivator and unreliable for motivation to organizational wholeness. In the cases of the biggest killers in the U.S., it manifests as chronic fear and seems to motivate in only limited ways. For example, despite warnings about heart disease and cancer, obesity continues to rise, most disturbingly among children (Carroll, Navaneelan, Bryan, & Ogden, 2015). Acute fear can be used in questionable ways such as after the 9/11 attacks, the fear of which, if not the motivation for invading Iraq, then justifying the Bush Administration's actions and giving 9/11 new meaning (Krebs & Lobasz, 2007). The motivation towards organizational wholeness will require other energies. Of deep concern is from where the energy for these changes, and their sustainment will come from, given other motivators like greed and power. The answer is undoubtedly embedded in the philosophical discussions of ethics and responsibility, but the issues are too urgent for them to remain simply academic concerns.

The idea that technological advancement requires ethical consideration is obvious. There are, however other ethical dimensions based on systemic complexity that may not be as widely studied. These dimensions relate to responsibility for attention to all aspects of highly complex, high consequence of failure systems, not just end use. Aspects include consideration of safeguards and security measures that extend to all potential areas touched by the system whose failure has the potential for high consequence. Another aspect is responsibility for whatever legacy issues one may be leaving behind for others to contend with. The result of this inquiry may be to add to and complicate the ethical debate by uncovering areas of responsibility formerly unconsidered; the very definition of shadow.

In summary, because we have the ability to do something, can we resist Oppenheimer's "sweetness," and not do that thing, if it detracts from the overall world societal good? If there are compelling reasons to do the thing, do we have the intelligence and wisdom to do meaningful system analysis work and will we accept the responsibility for safeguards? In short, can we face the shadow aspects of our decisions? Unfortunately, we are far beyond the decision point for creation of many of these technologies. We already have them and the only thing that we can do is curtail their use or shut them down completely; an unlikely outcome given powerful entities that benefit from their existence. There may be some hope that we can retire certain things like nuclear weapons, but these opportunities are in the minority. Certainly we will have to re-think large issues such

generating electrical power by burning hydrocarbons, but the fundamental hunger for the fruits of progress will never be sated. How then can our systemic awareness motivate organizational wholeness and give us hope for survival? The question is urgent and it demands insight and courage. Is it possible that in our current state we have technologically outrun our ability to responsibly deal with the systemic effects and collateral societal costs? Systems thinking and analysis is one way of uncovering holes and shadow aspects. Unchecked socio-technical advancement seems always to be antithetical to organization wholeness. Systems analysis will take time and issues uncovered will require accommodation that run counter to technological ambition, power, and profit.

REFERENCES

112th Congress. (2013). Public law 112-265.

Anderson, A. G. (2002). The media politics of oil spills. *Spill Science & Technology Bullitin, 7*(1-2), 7-15.

Arthur, L., Cato, M. S., Keenoy, T., & Smith, R. (2007). Corporate social responsibility in your own backyard. *Social Responsibility Journal, 3*(2), 32-38. doi:http://dx.doi.org/10.1108/17471110710829704

Bar-Yam, Y. (2002). Complexity rising: From human beings to human civilization, a complexity profile. *Encyclopedia of LIfe Support Systems*. Oxford, UK: UNESCO Publishers.

Bell, J. L. (2006). Champion paper and fibre company. *NCPedia.* Retrieved from http://ncpedia.org/champion-paper-and-fibre-company

Bjelopera, J. P., Bagalman, E., Caldwell, S. W., Finklea, K. M., & McCallion, G. (2013). Public mass shootings in the United States: Selected implications for federal public health and safety policy. Washington, DC: Congressional Research Service.

Buber, M., & Kaufmann, W. A. (1970). *I and Thou. / Martin Buber*. New York: Simon \& Schuster.

Bushman, B. J., & Anderson, C. A. (2002). Violent video games and hostile expectations: A test of the general aggression model. *Personality and Social Psychology Bulletin, 28*(12), 1679-1686. doi:10.1177/014616702237649

Carroll, M., Navaneelan, T., Bryan, S., & Ogden, C. (2015). *Prevalence of obesity among children and adolescents in the United States and Canada*. Retrieved from Hyattsville, MD:

Centers for Diease Control. (2015). Leading causes of death. Retrieved from http://www.cdc.gov/nchs/fastats/leading-causes-of-death.htm

Coombs, J. A. (2004). Pigeon River Revival. *Wildlife In North Carolina*.

Federal Aviation Administration. (2015). Lessons learned from transport airplane accidents. Retrieved from http://lessonslearned.faa.gov/

Finkelstein, S., Whitehead, J., & Campbell, A. (2009). How emotional tagging can push leaders to make bad decisions. *Ivey Business Journal Online*, 1.

Giovannitti, L. (Writer). (1965). The Decision to drop the bomb [Video File]. In F. Freed (Producer), *NBC White Paper*. Wilmette, IL: Films Inc.

Hogan, R. (2016). The accident-prone personality. *People and Strategy, 39*(1), 20-23.

Horney, K. (1950). *Neurosis and human growth : the struggle toward self-realization*. New York: Norton.

International Atomic Energy Agency. (2008). IAEA Nuclear Security Series 7: Nuclear Security Culture, Implementing Guide. Vienna, Austria: International Atomic Energy Agency.

Jacobi, J. (1973). *The Psychology of C. G. Jung*. New Haven: Yale University Press.

Krebs, R., & Lobasz, J. (2007). Fixing the meaning of 9/11: Hegemony, coercion, and the road to war in Iraq. *Security Studies, 16*(3). doi:10.1080/09636410701547881

La Porte, T. M. (2005). Governance and the specter of infrastructure collapse.

Leveson, N. (2011). *Engineering a safer world : systems thinking applied to safety*. Cambridge, Mass.: MIT Press.

Mitroff, I. I. (1988). Crisis management: Cutting through the confusion. *Sloan Management Review, 29*(2), 15.

Mitroff, I. I., Pauchant, T. C., & Shrivastava, P. (1988). The structure of man-made organizational crises: Conceptual and empirical issues in the development of a general theory of crisis management. *Technological Forecasting and Social Change, 33*, 83-107.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton.

Rayner, C., & Cooper, C. L. (2003). The black hole in "bullying at work" research. *International Journal of Management and Decision Making (IJMDM), 4*(1).

Reason, J. T. (1997). *Managing the risks of organizational accidents*. Burlington, VT: Ashgate.

Roser, M. (2012). Global deaths in conflicts since the year 1400. Retrieved from https://ourworldindata.org/VisualHistoryOf/Violence.html - /7

Satorius, M. A. (2015). *Insider threat program policy and implementation plan*. Nuclear Regulatory Commission.

Schneier, B. (2009). Beyond security theater. Retrieved from https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

Schwartz, S. I., & Choubey, D. (2009). *Nuclear security spending: Assessing costs, examining priorities*. Retrieved from http://carnegieendowment.org/files/nuclear_security_spending_low.pdf

Stanford geospacial center and Stanford libraries. (2015). *Stanford mass shootings in America*.

Sundar, S. (2015). Product liability case to watch in 2015. Retrieved from http://www.law360.com/articles/602531/product-liability-cases-to-watch-in-2015

Taylor, A. J. (1987). A taxonomy of disasters and their victims. *Journal of Psychosomatic Research, 31*(5), 535-544.

U. S. Department of Energy. (2014). *Insider threat program*. (DOE O 470.5). Washington, D.C.: U.S. Department of Energy.

United States Atomic Energy Commission Personnel Security Board. (1954). In the matter of: J. Robert Oppenheimer. Washington, D.C.: Atomic Energy Commission.

Vormetric Data Security. (2015). *2015 Vormetric insider threat report: Trends and future directions in data security*. Retrieved from http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107-124. doi:http://dx.doi.org/10.1057/sj.2012.1