JITTA
JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

THE LIMITED BUT INVALUABLE LEGACY OF THE Y2K CRISIS FOR POST 9-11 CRISIS PREVENTION, RESPONSE, AND MANAGEMENT

ELIA CHEPAITIS, Fairfield University
Information Systems and Operations Management, Fairfield, CT 06430, E-mail: echepaitis@mail.fairfield.edu

ABSTRACT

Although Y2K was neither an accident nor an unanticipated challenge, the millennium debugging was a watershed event for crisis response, prevention, and management, in theory and in practice. The simultaneity, high stakes, and ubiquity of the crisis permanently altered the circle of players with vested interests in and responsibility for emergency management (EM). Unfortunately, for political, socio-cultural, and strategic reasons, the legacy of Y2K was invaluable but limited: two steps forward and one step backward. Unlike 9/11, the Y2K crisis was anticipated, well-defined, and limited. Nonetheless, the Millennium project presents a model and methods that are germane to the a permanent but dynamic EM regime today. Y2K provided a coherent readiness and response model: an active matrix of players, protocols, and procedures. This matrix retains value even though post 9/11 challenges are more complex and require more agility than Y2K issues. The article first examines this model and other legacies, particularly in the private sector and in political culture; then the author describes why features dissolved and why. The author emphasizes investments, learning, leadership, and commitments to systems control that occurred as a result of Y2K, and recommends what can reasonably be done in the post 9/11 era to recapture cohesiveness and regimens that worked successfully in the Millennium Crisis. A brief literature review is included, and the author suggests areas for further research, especially in the area of leadership, collaborative intelligence, and security cultures after 9/11.

Murray Turoff and Bartel Van de Walle acted as senior editors for this paper.

Chepaitis, E., "The Limited but Invaluable Legacy of the Y2K Crisis for Post 9-11 Crisis Prevention, Response, and Management," *Journal of Information Technology Theory and Application (JITTA)*, 6:3, 2004, 103-116.

INTRODUCTION

Y2K left an invaluable legacy for emergency management (EM) after 9/11, but the contribution was limited in three ways. The first limitation was the unique and temporal nature of the well-defined Millennium Crisis. The second was the loss of popular and political interest in coordinated and extensive disaster preparedness post-Y2K. The third was the dissolution of common interests after the Millennium; stakeholders abandoned a shared vision of EM, and pursued separate security agendas with their own timetables

Nonetheless, the Millennium is relevant, both as an example of a well funded, inter-organizational success of unprecedented proportions, and also because attention to systems integration and reciprocity empowered a wide circle of stakeholders.

However limited, Y2K mandated the only widespread “walk-through” scenarios to date that simulated the expert and creative responses necessary after 9/11, especially in case of cyberterrorism or infrastructure failure. Although the Y2K crisis was not articulated with the long-term in mind and the regime was largely dismantled, its greatest contribution was probability this model: an active stakeholder-centered matrix of protocols, reviews, and procedures (Table 1). Information systems professionals, experts in other fields, and laymen accepted information and communication technology (ICT) management as their area of responsibility and accountability: before, during, and after the crisis. The matrix approach to stakeholder participation informed and facilitated cooperative alliances and synergies, and holds great promise for the post 9/11 era.

CONTRIBUTIONS

This paper’s research objectives are twofold. The first is to examine the impact of definition and articulation on long-term support for emergency management (EM) regimes. The second objective is to describe both the salient characteristics of successful Y2K multi-year projects, and also the major players or active stakeholders. The author proposes that the matrix model employed during the Millennium Crisis created synergies and numerous advantages that are germane for the post 9/11 era, especially these three: flexibility, robustness, and a high degree of self-organization. The article is intended for not only practitioners such as Chief Security Officers and academicians, but also policy makers who may gain insights from the thesis that effective EM models are, above all, social networks.

Y2K was a socio-cultural, economic, political, and highly public event. Through congressional hearings, Americans learned that we have created systems that we do not understand. Through the Securities and Exchange Commission, business partners and investors learned who was and who was not yet Y2K-ready. A conference of experts, hosted by the Center for International and Strategic Studies, described possible ripple effects from the Millennium Bug, from subsystems through supersystems. Hours of expert testimony were broadcast and re-broadcast on C-SPAN for months, and sold to viewers by request.

Y2K galvanized support for short-term cooperation: the problem was pressing,

Table 1. Matrix for Y2K preparedness assessment for each stakeholder, with intuitive horizons

	Reviews	Protocols	Procedures
Needs Analysis			
Resources			
Outcomes (e.g. fix, replace, work around)			
Assessment (e.g. compliance, readiness, failure)			
Subsystems (e.g. business partners)			
Supersystems (e.g. infrastructure)			
Oversight (e.g. Securities and Exchange Commission quarterly statements of readiness)			

predictable, and fixable with enough knowledge, time, money, and cooperation. Pressure spread vertically and horizontally across organizations: large companies exerted pressure on small companies and customers; the UN and the OECD monitored the level of preparedness in poorer countries; a Senate Subcommittee ranked the readiness of U. S. government agencies; in the United Kingdom, a superb report, *Realising the Benefits of Y2K*, was presented. Y2K became a cultural icon: an interesting, simple problem, broadly communicated and discussed, segmented into manageable parts.

The interdependence of government, healthcare, utilities, transportation, services, and communications through information systems was perceived as self-evident and critical for crisis prevention, response, and management. Emergency preparedness and broad approaches to disaster and contingency planning were enhanced incrementally in the ubiquitous multi-year Y2K effort. Perhaps most significantly, the tacit responsibility of EM leaders not only for the health of their own organizations, but also for the general good marked a watershed in preparedness. A quiet shift in context, away from self-interest and intra-organizational responses, may have been the most seismic development in the long run.

The crisis was a gateway to future global regimes, but not a bridge. On the whole, the leadership, vision, and resources necessary to sustain systems-wide EM evaporated and, unfortunately, were not resurrected after 9/11. After few millennium problems surfaced, the focus on the common good, such as the infrastructure, waned. Ironically, if more failures had occurred, interest in extensive EM regimens may have been bolstered. The greatest long-term impact on crisis response and management was probably within the business sector. Although leaders and stakeholders lacked the vision, creativity, or leverage to parlay the campaign into a permanent inter-organizational regime, it is germane to search for lessons that are of EM after the 9/11 attacks.

The article will examine first the multi-year effort to correct the millennium bug and the circle of stakeholders. Then, the author will discuss the loss of political and popular support for EM after Y2K. The study contrasts Y2K and the post 9/11 era, and recommends what models and lessons can be utilized reasonably. A brief literature review precedes suggestions for further research.

Y2K

A Unique Event

The Y2K crisis was unique: not an accident or an unanticipated event, and with global reach. The project was "largest coordinated worldwide activity to address a shared technology problem" (McDermott 1998, 42); "the first global challenge caused by information technology" said the United Nations-sponsored International Y2K Cooperation Center Final Report. The price of the fix was unprecedented: the Gartner Group estimated the cost of Y2K at $600 billion, although that price includes upgrades to replace or improve legacy systems (McDermott 1998, 41). In *ComputerWorld* in 1997, Peter Keen noted that that price tag was but part of the cost, and that the time- and people- resources devoted to Y2K were even more significant; that Y2K was more of a management problem than a technical challenge (Hyatt 1998, 16). Since no one knew just how many systems and embedded chips were vulnerable, Y2K forced organizations and individuals to perform unprecedented system-wide analyses and to fix or replace unreliable systems in a timely manner. Many organizations brought their ICTs and software under control, inventoried their information technology (IT), and learned about their dependencies on other parties, for the first time. Supply chains were evaluated and the reliability of key suppliers and customers was evaluated. Y2K provided an occasion for much needed pruning and organizing for systems and relationships.

National contingency plans were created, tested, and altered. Governments at all levels attempted to understand and connect with public and private suppliers of critical services. Although organizations were often reluctant to share data, and government agencies fell short of their targeted compliance deadlines, the Y2K campaign was truly pervasive and persuasive. Robust problem definitions, cogent imagery, and graphic projections helped stakeholders to visualize multiple levels of investigation and remediation. Although Y2K was not a security problem *per se*, but a maintenance issue, security planning and EM investments were deep and far-reaching not only within organizations, but also across cultures. From government agencies to households, users accepted a public responsibility for information systems reliability, for the common good. President Clinton's Council on the Year 2000, a Senate Subcommittee, and the Government Infrastructure Protection Center held public hearings and press briefings, not only for progress reports and reassurance, to prevent panic and to garner support for sizeable EM budgets. The IT-driven productivity surge of the late 1990s drove the U.S. stock market to unprecedented heights, although over-investment in IT produced a novel but dangerous business cycle. Economically, Y2K readiness could not be assured through domestic efforts alone. Outsourcing gathered steam--from SAP in Germany to Israel to shops throughout Bangalore, India. Economically, IT investment trends from 1995 to 2000 seem to show that over-investment in Y2K contributed to the bubble in the stock market and post-2000 the recession. Two factors probably reduced employment after 2000, from services to manufacturing: increases in productivity because of IT installed during the Y2K crisis, as well as expanded outsourcing that originated with Y2K projects.

A Defining Event in Crisis Management

Y2K's resemblance to 9/11 is limited for several reasons. Y2K campaigns preceded the Millennium moment, whereas 9/11's challenges followed a tragedy. Also 9/11 left us with much more complex and open-ended problems, and these require more agile solutions than the Y2K bug did. Yet Y2K enhanced best practices through inter-organizational brainstorming in five distinct stages: anticipating failure points and preventing crisis; planning crisis responses; establishing contingency plans; training and rehearsing; and, finally, evaluating EM performance evaluation (Table 2). Information systems acumen spread across a broad range of players, from Chief Information Officers (CIOs) to congressional committees to United Nations' task forces. Peter deJager intoned before a congressional hearing: "We have created systems we do not understand" (Yourdon and Yourdon 1998, 384), and ICT consumers at every level struggled to understand not only the systems they bought into, but also their vulnerability as subsystems.

Table 2. Multiple impacts of Y2K

Professional	• an enforced deadline • surge in outsourcing • replacement of legacy systems • teamwork and accountability • humility
Economic	• $600 billion invested [Gartner Group] • surge in upgrade funds • tech stock market bubble • competitive advantage
Sociocultural	• consistent, dramatic newsworthiness • ongoing debate about risks • popular stake in preparedness • subject for humor, hype, and skepticism • a global event
Political	• oversight and responsibility • executive, SEC, legislative • hearings, judiciary • both non-profit and commercial command & control regimes
Intellectual	• unprecedented attention to ICTs • acknowledged dependence on overlapping systems • debate on the general good and IT

Y2K propelled stakeholders to leap into multi-party risk analysis, data quality control, and contingency planning. Moreover, the campaign coordinated expertise, resource allocations, and commitments that were truly global. Nationally, critical linkages extended the reach of Y2K projects: from government to transportation to communication, banking, military, healthcare, educational, and utilities, and through local restaurants, dentist's offices, retailers, and libraries (Table 3).

Because the response to Y2K was unprecedented and a multi-year event, the effort was unique not only in scope and investment, but also in the types of players involved in damage control. Government at all levels, banking regulators, transportation authorities, and local militia and health organizations not only joined in the cooperative effort, but were themselves forced to demonstrate Y2K readiness. Although special teams and committees were disbanded after the event, Y2K was an invaluable experience.

The aggregate effects of coordinated attention in areas such as utilities, transportation, banking and finance, healthcare, and government were extraordinary. Y2K accelerated and coordinated systems development with multiple impacts: billions of dollars spent on testing; a plethora of outsourcing partnerships; massive investment in debugging and upgrading; and productivity increases in the short and in the long term. In the U.S., corporations were compelled to certify their compliance with the Securities and Exchange Commission. Technologically, the crisis accelerated systems upgrading and platform choices, upgraded 1997-2000 IT budgets for control and maintenance, strengthened major global software players and partnerships, and mandated public financing for the ICT infrastructure. Y2K accelerated the development of Application Service Providers and Enterprise Resource Planning, and paved the way for the emergence of Chief Security Officers (CSOs) to manage disaster preparedness for business enterprises.

Although few systems actually crashed during the millennium, and elevator passengers could relax their fear of embedded chips, Y2K mattered. Y2K's effects were: intellectual, financial, technological, economic, socio-cultural, and, above all, educative (Table 2). The event enlarged the criteria for sound information systems practice, and extended the arena of responsibility, accountability, and liability away from small circles of systems professionals: to manufacturers, chip designers, industry analysts, management at every level, users, socio-cultural gurus, economic analysts, and political leaders. From systems forensics

Table 3. Millennium projects: critical linkages, from prevention through emergency management

Prevention	• preparedness and oversight: • command & control regimes • documented Y2K readiness, certification, compliance. • a deadline: ease of definition
Communication	• multidirectional, dramatic, dynamic inter-organizational cooperation & collaboration; • accountability, responsibility , & liability established
Response	• risk analysis • multilevel ripple effects • contingency planning • flexibility • informed oversight • massive IT investments
Emergency Management	• multi-level • political & commercial leadership

to desktop information responsibility, the campaign promoted widespread understanding: of dependence on information systems, of vulnerability to attack or sabotage, of the costs of downtime and disruption.

Y2K educated policy makers, the public at large, and business leaders about risk as no other event before or since. Scenarios were investigated and replayed across the world: the impacts of systems failure were quantified and the ripple effects fully described—sometimes to excess, with socio-cultural as well as technological impacts. Information systems reliability was seen as a strategic national necessity for the first time, especially in advanced economies. Numerous programs ended after Y2K, but a prototype had been developed for future reference. The World Bank funded a United Nations-based International Cooperation Center that advised 170 countries how to fix the Millennium Bug, and reported on the progress of Y2K campaigns globally. Numerous organizations sought and found competitive advantage through Y2K readiness. People's Bank of Bridgeport printed handsome fliers and distributed buttons proclaiming: "We're Getting Ready for the Year 2000", and hosted conferences on readiness for local businesses and universities. Numerous software houses and hardware providers boomed because of Y2K One ICT guru, Peter de Jager, published a list of organizations that benefited most from Y2K contracts (McDermott 1998, 43). Command and control centers were set up and tested. All of these formal efforts were disbanded, but a sea change had occurred. Richard Clarke was appointed as a special advisor to President Clinton for cybersecurity during the Y2K crisis, and advocated a logical segue from Y2K to cyberterrorism. Particularly in view of the 9/11 Commissions recommendations, it is evident that Y2K's probably contributed more strongly to collaborative enterprise development in the private sector, in contrast with the lack of integration and extension across government agencies, especially in the area of intelligence, in the early 2000s.

EM And Popular Culture: The Y2K Boomerang And Backlash

By 2000, C.P. Snow's hypothesis (Snow 1959), that modern technology creates an unbridgeable chasm between professionals and laymen, seemed to have lost credence, given the mass market for ICTs and the vast publicity given to Y2K fixes. However, after Y2K, the public swiftly lost interest in readiness, and the regime imploded (Table 4). Perhaps, recalling Snow's observation, both the content and the context of preparedness had not been sufficiently appreciated by laymen. Even though the Y2K problem was well defined and visualized, and inter-organizational collaboration was

Table 4. Why Y2K readiness imploded

Professional	• success but embarrassment • collaboration and cooperation ends • new IT foci: ASPs, ERP
Economic	• budgets exhausted • IT bubble • competitive advantage elsewhere
Sociocultural	• loss of interest • Inability to imagine future vulnerability • sharp decline in newsworthiness • credibility issue: was the crisis overblown?
Political	• lack of political will, expertise & imagination • divorce of Y2K from issues, especially in regard to cyberterrorism • regimes dismantled: difficult communication • poor definition & problem articulation • separation of public & commercial priorities • atrophy of cooperation • dismantling of command & control regimes
Intellectual	• splintered & competing views of responsibility for the general good

unprecedented, the broader implications for long-term crisis management across organizations were not well articulated.

The shared vision, disaster prevention regime, and imagery associated with Y2K did not survive the millennial event intact. When dire predictions did not come true, support for inter-organizational collaboration and a permanent IT-disaster regime evaporated. The quiet success of most Y2K projects created the perception that the problem had been overstated and hyped.

On one level, Y2K was a unique and defining event in crisis management but, on another, it was a passing diversion – at times, a circus. The Millennium Crisis was dramatic and riveting because no one knew what was going to happen, and the imagery was galvanizing. On public airwaves, experts confessed that they had caused the mess not out of stupidity but for efficiency; « More programming sins have been committed under the guise of efficiency than any other reason, including stupidity. » (McDermott 1998, xiv). Y2K bugs were compared to cancer, spreading silently throughout the organization (Hyatt 1998, 3) threatening ATMs, bank accounts, credit ratings, prescriptions, electronic doors, elevators, and security systems (Hyatt 1998, 32, passim; Spector 1999). The highly respected Peter Keen said, « The problem is far worse than even the pessimists believe. » (Hyatt 1998, 16).

The population was warned: « Computer systems all over the world will begin spewing out bad data—or stop working altogether ! When this happens, it will be similar to a giant hard-disk failure. It's inevitable, and it's going to be terribly ugly when it happens. The only difference is that it is going to be *a billion times worse* than the worst microcomputer crash you have ever experienced or could ever imagine. » (Hyatt 1998, 3).

Experts and pundits compared the impact of Y2K to the 1929 Stock Market Crash, and forecast a sustained decline similar to the Great Depression if all bugs were not found: « Keep in mind that even if the Year 2000 problems are severe…, if the company can't get access to its customers or to the funds in its corporate bank account, it may still be able to limp along for a month or two until it closes the doors. If it can't process orders and invoices properly…, it could find itself bleeding to death over a period of six months to a year » (Yourdon and Yourdon 1998, 39).

The scope, depth, uncertainty and ubiquity of the Y2K problem captured the public imagination: on the evening news, on the cover of news magazines, before Congress, the courts, and in the Oval Office. Political analysts warned that President Clinton would be remembered for the Year 2000 Crisis the way Hoover was for the Great Depression. Since Y2K had the potential for grave damage to vast super systems, to elevators, to air traffic control, to public utilities, to security systems themselves, the public's attention seldom wavered but the popular commitment to continuous EM investments was shallow.

To many laymen, the year 2000 crisis was overstated: a widespread patch job characterized by confusion, mismanagement, hyperbole, and over-investment. A typical, alarmist readiness list may have encouraged skepticism (Table 5) (Hyatt 1998, 210, passim).

Hyatt added, « I would suggest stockpiling : ammunition (especially .22 caliber), toilet paper. Bic lighters, coffee and tea, sugar. » (Hyatt 1998, 210). Buyers hoarded and stockpiled so much Spam before the Millennium that Hormel's earnings plummeted in 2000 and 2001 *(Different Kind of Canned Excuse, 2001).*

There were voices of moderation. McDermott reminded readers that disasters often benefited the economy, and he put the risk factor in Table 6 at a daunting (but accurate) 5.

ICT gurus and public officials sought to reassure the public, but a chasm developed between EM experts and other stakeholders in 2000 that still, to some extent, has not been bridged in 2004—three years after 9/11.

What Can Be Done Post 9/11?

Unprecedented cross-disciplinary teamwork, oversight, development and systems-wide assessment built Y2K ready systems and also contingency and continuity programs, alliances, and expertise. The

Table 5. “What to do” list for Y2K emergency preparedness

1	Secure copies of important documents
2	Build an emergency preparedness library
3	Evaluate your current location
4	Determine your self-defence philosophy …(If you are going to purchase a gun, make sure it is appropriate for your size and goals)
5	Find an alternate source of water
6	Stockpile food and common household goods
7	Purchase adequate clothing (because the Y2K crisis will start in the middle of winter)
8	Develop an alternate source of heat and energy if you don’t have a fireplace, you might consider putting in a woodburning stove
9	Prepare an emergency medical kit
10	Determine how you will dispose of waste
11	Secure an alternate form of currency
12	Acquire a basic selection of hand tools

Table 6.”How bad is it?” chart

Score	Assessment
0	It is a hoax perpetuated by vendors, consultants, and lawyers to make a lot of money
1	It is a minor problem that can easily be fixed
2	It is no big deal
3	The problem should be addressed, but it is not serious
4	It is a serous problem if not fixed, but it is well within the realm of what can be done
5	It is a serious problem that will require hard work, but it can be fixed without disaster
6	The problem can be fixed but will be very expensive
7	It is a serious problem that will have huge costs and cripple some large companies
8	The costs will be so severe as to cause major economic repercussions
9	The problem will cause severe economic disruptions to our way of life for at least several months
10	The problem will be the end of civilization as we know it, and we will never recover

important questions raised are: What did we learn and what did we not learn from Y2K that is useful after 9/11? Who learned? What concrete changes and contributions can be attributed to Y2K, however inadvertently, and which opportunities may have been missed? In the long term, media hype obscured numerous collateral benefits of the Y2K crisis—such as unprecedented system-wide understanding of IT possibilities and relationships that emerged or were at least accelerated by massive Y2K investments, contingency plans, and stakeholder empowerment. How can the expertise be developed to deal with catastrophic threats, and to foster a learning, security culture?

After 9/11, crisis prevention shifted away from matrix models, toward more linear and vertical strategies focused on intelligence gathering and warfare—the identification and destruction of hostile agents, targets, and weapons. Since terrorist attacks cannot be predicted with precision and probability, the scope of prevention, preparedness, and crisis management is unwieldy. Effective ICT weapons have not yet been developed and deployed, such as data mining, decision support, coordinated digital surveillance, or back-up and control mechanisms. Also, numerous non-technical, soft factors affect the development of these factors : language skills, border controls, clandestine terrorist financing, cultural dissonance, diplomatic expertise, capable political leadership, and legal constraints.

Stark differences exist between the two crises—Y2K and 9/11, EM challenges after 9/11 far exceed Y2K’s, and the solutions are more elusive (Table 7).

In the Millennium crisis, remediation methods were obvious : fix, replace, work around, expand, encapsulate, compress, or abandon (McDermott 1998, *passim)*. It was easy to locate shareware patches, or tap expertise from offshore software houses to computer science majors. As noted above, some organizations avoided the problem altogether by accelerating the replacement of legacy systems. The responders to the millennium crisis were broad-based: government at all levels, representatives of all the professions, industry associations and self-regulators, infrastructure leaders, and local militia and health organizations not only joined in the cooperative effort, but were themselves forced to demonstrate Y2K readiness.

After 9/11, it was difficult to comandeer assets in the absence of a clear and well-defined, forecasted event. Perhaps because few stakeholders are included in the circle of active players, numerous programs were initiated, few direct or collateral benefits are apparent. Unlike Y2K, it will take years to develop and deploy expertise : from linguistics to backed-up communication systems. Unlike Y2k, avenues of attack and contagion are not restricted to ICTs, and threats are broad and open-ended.

Counterterrorism, unlike Y2K projects, is top-down, isolated and secretive, and has not adopted this effective model: a broad-based, self-organizing, flexible social network that breaks complex tasks down through nodes of individuals following simple rules (Bonabeau and Meyer, 2001). In fact, secretiveness may produce a culture of "Group Think" and tunnel vision—a problem emphasized by the 9/11 Commission. Fragmented and unstructured stakeholder responses and also divergent government-commercial priorities make it difficult to coordinate and assess ongoing improvements in crisis prevention and management. Y2K and the years after 9/11 illustrate not only that the

Table 7. Y2K campaigns and the post- 9/11 challenge

Y2K	Post 9/11
Broad, Unified Stakeholder Circle: Lay and Professional Top-Down and Bottom-Up Continuous Input and Assessment	Fragmented Stakeholders, Often with Diverse Priorities
IT-centered problems	Problems not only IT-centered: Myriad Avenues of Attack and Contagion
Anticipated, overt, possibly overstated threat	Continuous Threat
Well-Defined, Articulated, and Justified	Isolated and secretive counterterrorism: the danger of Group Think" and tunnel vision
Broadly Communicated	Poorly Communicated
Enmeshed in Popular Culture	Massive, Diverse, and Ill-Defined Needs
Temporary, A Management Challenge and a Technological Task	No Specific Timetable
Collateral Benefits of Fixes	Difficult to Define
Technological and Managerial Issues: Socio-Cultural Impact Transitory	Fear of Pandemic of Panic
Empowered Leadership and Oversight	More Difficult to Respond to Systemic Failures than to Prevent Them
Assessment Methods and Measures	Lack of Assessment, Measurement, and Collateral Benefits (Including Learning)
Damage Estimates Exaggerated	Ill-Defined, Difficult to Articulate, Choices Difficult to Prioritize
The Advantages of Prevention: Shared Solutions and Containment	Less Mutual Trust and Empowerment
	Political Rather than Technological Issues: Socioeconomic Context
	Ongoing, Perhaps Growing Threats
	Difficult to Coordinate, Lead, Assess, or Measure Preventative Measures
	Probable Cause: Deliberate Human Agents

public and private attention span is short but also that leadership's appreciation for complexity and patience can be limited. Ideally, a balance can be achieved between sensationalizing a crisis and informing and empowering stakeholders. It appears that, if the size and scope of a scheduled and manageable challenge such as Y2K is communicated and understood, stakeholder trust and collaboration is, in fact, intuitive. A major lesson of YK appears to be that a crisis and solutions must not only be defined but well-articulated, and involving as many stakeholders as possible through appropriate imagery, creative problem-solving, walk-throughs, and trust.

To date, cyberterrorism appears to be the threat that most closely resembles Y2K, especially in the form of information warfare—an increasingly common form of attack. Through military, corporate, intelligence think tanks, and academic sources, scores of incidents of information warfare are documented on the website for the Institute for the Advanced Study of Information Warfare (http://www.psycom.net/iwar.1.html). Although these skirmishes in this form of guerrilla war may well precede « an electronic Pearl Harbor », some threats resemble the Year 2000 crisis in several areas : the danger to a broad range of targets, including infrastructures ; the unknown depth and breadth of the attacks ; the huge amount of investment not only in ICTs but in cooperative expertise that is required to prevent or contain damages ; and the need for public, educative forums to clearly articulate and define this ubiquitous problem. What is clearly different from Y2K, is that stakeholders do not know *when* attacks may occur or what they should do. In the absence of both a linear timetable and deadline, and also an ongoing popular debate focused on milestones and measurements, it is difficult to build upon the squandered legacies of Y2K.

To date, unlike Y2K, 9/11 has neither educated nor mobilized stakeholders, and the absence of candor or reassurance may have eroded trust. Immediately after the Millennium, the cyberterrorism czar, Richard Clarke, noted the need for continuous preparedness - before cyberterrorists could emulate hackers and attack the infrastructure (Clarke 2000). Yet three years after the World Trade Center Disaster, Stephen Flynn's *America the Vulnerable* describes the lack of cogent planning or preparedness (Flynn 2004). On August 14, 2004, Gabriel Wieman reported on CNN that Al Qaida and associated groups have more than 4,000 Websites, expertise with embedded messages using steganography, and their own third generation computer language for propaganda, training, and fund raising. In 2004, Clarke's *Against All Enemies* criticized Bush Administration's handling of events both before and after 9/11 (Clarke 2004). The failure of the electrical grid in the eastern United States in August, 2003 illustrated the vulnerability of the most basic infrastructure services, even *without* a human agent. In the autumn of 2003, editorials asked how public health officials could handle a bioterrorist attack, if the government failed to provide sufficient supplies of flu vaccine (Davis 2004). As late as October 2004, intelligence agencies lacked an integrated and shareable terrorist watch list.

A lack of stakeholder involvement not only wastes resources, but also increases fear and reduces credibility. For example, residents of New London, Connecticut have yet to be informed if, in the three years since 9/11, any plans exist to protect any or all of four strategic facilities clustered near the mouth of the Thames River: the Waterford nuclear power plant, the Groton submarine base, Electric Boat's naval shipyard , and the Coast Guard Academy. Public petitions to restrict fly space over the power plant and the other facilities have been denied.

After 9/11, in contrast to the public sector, some individual organizations developed contingency plans. For example, the New York Stock Exchange established alternate sites in Brooklyn and New Jersey. Morgan Stanley constructed a backup trading facility 35 miles from its mid-Manhattan headquarters, but not on the same power or telephone grid (CNN Money 2001) . However, unlike Y2K, coordinated and system-wide prevention, responder, and backup systems were not mandatory and little or no oversight has been established. In fact, the American Management Association, in annual Crisis Management and Security Issues surveys, found that fewer businesses had contigency plans in 2004 than in 2003: only 61% of executives said that their companies had a crisis plan in 2004, down from 64% a year earlier. 54% of the companies had established a crisis management team in 2004, down from 62% in 2003 (American Management Association 2004).

Building upon and improving Y2K's legacy, some measures could be initiated swiftly and simultaneously : the development of expertise and intelligence, infrastructural improvements, and coordinated stakeholder participation, with oversight. (Table 8) . Many of these strategies convey collateral benefits.

In hindsight, the Y2K experience indicates that in anticipation of grave crises, such as a cyberterrorist attack, a matrix model works well that coordinates stakeholder activity and encourages self-organization and flexibility. In *Swarm Intelligence*, the efficiency and interconnectivity of social insects is discussed and efforts to capture the rules that make matrix strategies succeed are described (Bonabeau and Meyer 2001). However, matrix strategies and stakeholder empowerment will not work without distributed responsibility and top-down, as well as bottom-up, accountability.

LITERATURE REVIEW

A plethora of material on Y2K emerged from 1995 up to 2000: monographs, articles, congressional hearings, the Securities and Exchange Commission's compliance documents, and trade publications Three monographs were prominent, and their titles are instructive: *The Millennium Bug: Survive the Coming Chaos* (Hyatt 1998), *Time Bomb 2000* (Yourdon and Yourdon 1998), and *Solving the Year 2000 Crisis* (McDermott 1998). The author used McDermott as a supplementary systems analysis and design textbook, since his emphasis was on computer engineering and Y2K fixes: replace, expand, window, compress, work around, encapsulate, or abandon. In addition, he thoroughly investigated costing, staffing, strategies, failure points, and testing. In his first four chapters, McDermott presented not only the Y2K crisis, but also a balanced description of the context in which solutions were sought. The Yourdons' *Time Bomb 2000* was a bestseller, and described potential Y2K problems in numerous areas: employment, banking and credit, transportation, food, utilities, news and information, health and medicine, government, education, telephone and mail services. Also, in each chapter the authors included fallback advice for two-day, one-month, one-year, and ten-year failures or disruptions. Hyatt's *The Millennium Bud: How to Survive the Coming Chaos* was both the most alarmist and also the most informative book for anecdotes and quotes that illustrate the fear and hype that contaminated Y2K's legacy (Hyatt 1998). In addition, his footnotes are a gold mine for researchers looking for popular, trade, or obscure articles on the millennium bug.

Hyatt's book was not only a survival guide, but also contained estimates of the costs of software fixes and the potential costs of institutional breakdowns if there were still software glitches because of Y2K. Unfortunately, these books are dated, and of limited value for an assessment of the significance of Y2K into the millennium.

The dominant Y2K question on January 1, 2000 was, "Was the crisis exaggerated?" However, from 2000 to 2004, little research on the Year 2000 crisis has been conducted in information systems or in other disciplines. No,

Table 8. Using and improving Y2K's legacy

Expertise: Well-funded Training and Education
Intelligence: Improved Predictions
Infrastructure improvements, Including Feedback, Control, and Contingency Planning
Continuous Top-Down Coordination, Oversight, and Assessment
Active Participation and Input by a Wide Circle of Stakeholders

researcher investigated the collateral benefits unintended consequences, and new directions in information systems because of the millennium crisis. It is not only interesting but also germane to the hypothesis that after the millennium, almost nothing of substance was published on Y2K. No scholarly monographs or articles were published. It was as though the Y2K crisis was a huge embarrassment, a trick that is best forgotten. The few Y2K failures did not have disastrous consequences, were speedily repaired, and were not reported at length. The long-term effects of Y2K on emergency response, back-up systems, auditing and oversight are discussed in a cursory fashion here and there, in engineering, retailing, healthcare, and information systems trade literature, but not in refereed articles (e.g., Elliott 2000; National Underwriter/Life and Health Financial Services Editorial 2000; Harrington 2000; Henderson 2000; Childress 2004; Moran 2004). Significant material can be gathered and extrapolated on the surge in IT spending during the crisis in statistical abstracts or data from the Commerce Department. Finally, isolated comments and case studies, such as *Nestle Struggles with Enterprise Systems* (Laudon and Laudon 2003) tangentially document the deleterious impact of diverting funds needed for projects such as ERP development to the Y2K crisis. These and other small accounts in the aggregate offer important clues on the opportunity costs of Y2K funding. Three fine reports published in 2000 document the collateral benefits of Y2K: the International Y2K Cooperation Center that was funded by the World Bank (International Y2K Cooperation Center 2000), Beckett's Report to the House of Commons (Beckett 2000), and Eleni Martin's Silver Linings Report (Martin 2000). This report notes that, after Y2K, governments were ideally positioned to take advantage of more integrated and responsive systems.

Except for the *9/11 Report* (2004) by the National Commission on Terrorist Attacks Against the United States, and Clarke's *Against All Enemies* (Clarke 2004), definitive studies have not yet been conducted. Hulme, Garvey and Rendelman summarize the tension between government and business in their struggle to balance security and privacy concerns (Hulme, Garvey and Rendelman 2002); Sobel's report, *Securing our Infrastructure* (Sobel 2002), before the Senate Committee on Government Affairs also discusses this tension. Stephen Flynn criticizes the Bush Administration's policies against terrorism before and after the 9/11 attacks in *America the Vulnerable* (Flynn 2004). A chapter by Warren and Hutchinson in *Information Security Management: Global Challenges in the New Millennium* surveys types of cyberterrorist attacks against ICTs, but not attacks on other targets using ICTs (Warren and Hutchinson 2001). Finally, Bonabeau and Meyer wrote a landmark article for the Harvard Business Review on swarm intelligence, forecasting the development of expert systems that recapture the collaborative intelligence of social insects; this is how the matrix model should work, and their research suggests that tools for improving group intelligence are forthcoming (Bonabeau and Meyer 2001).

Conclusion: Research Opportunities

The thesis of this paper is that stakeholder participation and skillful articulation are both critical for EM post 9/11. The scope, depth, and ubiquity of both the Y2K problem and 9/11 challenges remain unprecedented. Both had the potential for grave damage to vast super systems, to the common good and public safety, but the public's attention seldom wavered before Y2K, yet the public has yet to be engaged post 9/11

The author also addressed these questions: why did Y2K lack agency for the post 9/11 era, how could better balances be struck between a well-communicated campaign and a sensationalized event, and what benefits may be derived from successful EM outcomes? History never repeats itself, but it does resemble itself. It is doubtful that C.P. Snow's assertion, that laymen are "tone deaf" in any debate about technology, is true. However, persuasive arguments require appropriate channels, rich messaging, and impressions management—the right melody, so to speak, to resonate and stimulate participation.

Numerous additional research opportunities are embedded in Y2K and 9/11: impacts on employment, the infrastructure, political discourse, the erosion of trust, decision making, or legal systems. Can patterns be discerned in the opportunity costs of EM funding, especially beyond IT? What are the consequences if resources are diverted for non-terrorist, emergent problems such as hactivists —politically-minded hackers who sabotage Websites and spread misinformation to manipulate public opinion?

Which global players and partnerships were most impacted by Y2K and 9/11, and to what macro-economic effect? Also, in which industries or institutions was compliance, resistance, or upgrading most typical, and why? What was the precise impact of the billions of dollars spent on testing, debugging, and upgrading with Y2K or enhanced continuation after 9/11: on productivity and on the business cycle--in the short and in the long term? How much does disaster prevention channel an economy into new directions, or dead ends? Trends in IT investment from 1995 to 2000 seem to show that heavy ICT investments contributed to a bubble in the stock market and eventual recession.

EM after 9/11 is replete with research opportunities, such as collateral benefits and collateral damage due from campaigns against terrorism. What has not been done, and why, is significant in salient areas: improvements to the infrastructure, agreements on IT platforms, and massive ICT investments in strategic areas such as multi-sensory robots, increased broadband, data mining, biometrics, and artificial intelligence for language translation.

Acknowledgment. An earlier version of this paper appeared in the Proceedings of *ISCRAM 2004*, the first *International Workshop on Information Systems for Crisis Response and Management* (Chepaitis 2004).

REFERENCE

American Management Association, “2004 AMA Survey: Crisis Management and Security Issues,” 2004. Available at: http://www.amanet.org/research/. Last accessed January 16, 2005.

Beckett, M., MP, *Modernising Governments in Action: Realising the Benefits of Y2K*, Report to the House of Commons, April 14, 2000.

Bonabeau, E., and C. Meyer, “Swarm Intelligence: A New Way to Think About Business,” *Harvard Business Review*, 2001, 80:5, pp. 106-111.

Chepaitis, E., “The Impact of Y2K on Crisis Management: Widening the Stakeholder Circle,” In *Proceedings of the First International Workshop on Information Systems for Crisis Response and Management ISCRAM2004*, Carle, B. and B. Van de Walle (eds.), 2004, pp. 111-113.

Childress, S., “Hactivists Log On: Police Are On Guard against Threats of Electronic Chaos,” *Newsweek*, 30 August, 2004, p. 43.

Clarke, R., *Against All Enemies*, New York: Free Press, 2004.

Clarke, R., “Promoting Cyber Security for the 21st Century,” *White House Document*, Clinton, W.J. and A. Gore, January 7, 2000.

CNN Money, “Morgan Stanley Eyes Backup,” 2001. Available at http://money.cnn.com/2001/10/30/companies/morganstanley/. Last accessed: January 16, 2005.

Davis, M., “Did We Prepare for the Wrong Biological Attack?,” *The Hartford Courant*, 12 October, 2004, p. A9.

“Different Kind of Canned Excuse,” *New York Times Business Diary*, February 18, 2001, p. C4.

Elliott, H., “No Bugs; Now What?,” *Electronic News*, 2000, 46:2, pp. 32-35.

Flynn, S., *America the Vulnerable: How Our Government is Failing to Protect Us From Terrorism*, New York: Harper Collins, 2004.

Harrington, R., “Lessons Learned from Y2K,” *Credit Union Executive Journal*, 2000, 40:1, pp. 6-10.

Henderson, T., “Retailers to Press On with Projects Deferred by Y2K,” *Stores Magazine*, 2000, 82:1, pp. 138-140.

Hulme, G.V., M.J. Garvey, and V. Rendelman, “The Right Balance: National Cybersecurity Plan Takes Shape but Raises Questions about Expectations,” *Information Week*, 16 September, 2002, pp. 22-23.

Hyatt, M., *The Millennium Bug: Survive the Coming Chaos*, Washington, DC: Regnery, 1998.

International Y2K Cooperation Center, “Y2K Center Says International Cooperation Key To Success,” Available at: Newsbytes.com. Last accessed: February 16, 2000.

Laudon, K.C., and J.P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise* (7th edition), New York: Prentice Hall, 2003.

Martin E., *The Many Silver Linings of the Year 2000 Challenges: Three Organizations Collaborate to Build on Unanticipated Benefits from Y2K*, U.S. General Services Administration GSA Report # 9647 (March 7), 2000.

McDermott, P., *Solving the Year 2000 Crisis*, London: Artech House, 1998.

Moran, J.M., “Crisis Preparations Lack 9/11 Urgency,” *Hartford Courant*, 11 September, 2004, pp. A1, A9.

National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: W.W. Norton & Co, 2004.

National Underwriter/Life and Health Financial Services Editorial, “Now That It’s Over, Was the Y2K Effort Worth It?,” *National Underwriter/Life and Health Financial Services*, 2000, 104:9, 2/28, pp. 18-21.

Snow, C.P., *The Two Cultures and the Scientific Revolution*, New York:Cambridge University Press, 1959.

Spector, L., “2000: The Year of Living Dangerously,” *PC World*, January, 1999, pp. 90-110.

Sobel, D., “Securing our Infrastructure: Private/Public Information Sharing,” *Report of the Electro-nic Privacy Information Center before the Senate Committee on Government Affairs*, 8 May, 2002.

Warren, M., and W. Hutchinson, “Cyber Terrorism and the Contemporary Corporation,” In *Information Security Management*, Dhillon, G. (ed.), Idea Group Publishing, Hershey, PA, 2001, pp. 53-64.

Yourdon, E., and J. Yourdon, *Time Bomb 2000*, New York: Prentice Hall, 1998.

AUTHORS

Elia Chepaitis is an associate professor of information systems (IS) and operations management at Fairfield University, in Fairfield, Connecticut. She holds advanced degrees in industrial engineering, economic history, Russian Studies, and international business. Her research interests include international information systems, information ethics, the impacts of IS in developing economies, crisis management, and information access for those with disabilities. Dr. Chepaitis worked as a consultant in Kemerovo, Siberia in 1991 and 1992, and received three Fulbright fellowships to teach in Russia and Morocco in 1994, 1995, and 1998. She has invented an alternative to Braille, Elementary Imprint Assistance (ELIATM), that has been granted numerous national and international design and utility patents from 1987 to 2004. Information systems theory and practice , as well as contemporary ergonomic principles, strongly influenced the development of the new code. This easy-to-use tactile language is designed for the 92% of the blind who are unable to read Braille, and has been successfully tested at the State University of New York’s School of Optometry, for ease-of-learning, tactile acuity, and superior reading speeds. The results of this research are forthcoming.