



# Municipal Administration of Cities in Crisis

July 2013

**Author**

Vinay Gupta

The Institute for Security & Resilience Studies (ISRS) at University College London (UCL) provides a hub for scholars and practitioners to address the challenges of resilience and security in the 21st Century. We bring together the public, private and third sectors to seek out ways to catalyse innovation - so that we can all better cope with, and flourish in, increasingly uncertain times.



This paper was first published in July 2013.

Published by

Institute for Security and Resilience Studies
Gower Street
London
WC1E 6BT

+44 (0) 20 3108 5074

isrs@ucl.ac.uk

www.ucl.ac.uk/isrs

Institute for Security and Resilience Studies Limited is registered as a company in England and Wales. Registered office: 1 Beauchamp Court, Victors Way, Barnet, Herts, EN5 5TZ. Registered number: 06842634. VAT registration number: 103324470.

# Table of Contents

# MUNICIPAL ADMINISTRATION OF CITIES IN CRISIS

## The Challenge

1. In any stressed situation, certain municipal functions have to be maintained in order for healthier everyday life to persist. This applies equally to Haiti after its earthquake, Detroit in the face of an economic crisis, and Baghdad struggling to win the peace from protracted violence.

2. At this time, there is very little coherent work on managing the basic municipal administration of cities during times of scarce resources, rapid change, and recovery from shock. Lessons are learned again and again, without international repositories of know-how to enable municipal administrators (and their aides) to make the best possible adaptation to the circumstances they find themselves faced with.

3. The three most common challenge scenarios are political unrest, natural disaster and economic collapse. Even previously prosperous cities, like Athens, now face urban infrastructure challenges due to deferred maintenance and plummeting budgets. What tools and technologies can be put into the hands of municipal administrators to help them understand the function of their cities better, enabling them to react and prioritise more effectively during hard times? Can big data help identify crucial interdependencies and efficiencies in vital underlying systems? What potentials exist to transform urban responses to crisis using new technology?

## INTRODUCTION

4. Cities are especially affected by a wide variety of risks and uncertainties because of the concentration of people dependent on elaborate production processes with many intermediaries, specialisms and long supply chains. As infrastructures have become more complex and essential, cities have become increasingly dependent on advanced technologies and social structures like the financial system and global logistics pipelines for their continued smooth function.

5. We will briefly examine some case histories, and draw out a selection of useful threads. These are limited by the scope of a mini-project but nonetheless indicative of the value greater work could achieve.

# THREE DISASTERS - *THE DEVILS WE KNOW*

## Hurricane Katrina

**New Orleans, America 2005,**

**2000 dead, $80bn damage**

*Broad profile*

6. Storm surge overwhelms flood defences in impoverished American coastal city. Disorganised Federal response starts long before the disaster (no warnings are given that levees may break) and continues long into the rebuild phase of operations. Large areas of the city are abandoned after the flood, leaving the city at roughly half the population it was at before the disaster.

    a. Failure to issue compulsory evacuation orders, commandeer school bus fleets etc. pre-disaster coupled with multi-day delay in authorising use of military assistance in logistics, evacuation and maintenance of public order. (Army Support During the Hurricane Katrina Disaster, James A. Wombwell, 2009).

    b. Reports giving an accurate assessment of a risk of catastrophic failure of the flood defences are ignored, including Army Corps of Engineers warnings over several decades, and no warning is given of flood defence failure although some sources estimate it was known up to 72 hours before the event.

    c. Inadequate provisioning of resources for large scale evacuation resulting in improvised responses, 25000+ population being warehoused in a stadium 500km from New Orleans, 55000 citizens eligible for payouts for formaldehyde contamination in FEMA-provided temporary trailer accommodation.

    d. Unusually high loss of life for a disaster in a developed world country, paired with a public perception of mass disorder and looting after the event, makes this a stand-out event in the history of US disasters.

*Notable* interventions

7. There are no identifiable positive deviations or stand-out reports of unusual intervention in this disaster, with the exception of individual stories of heroism and improvisation.

*Conclusion*

8. Very close to a worst possible case response failure to a predictable disaster. Hurricane Katrina is a veritable repository of irresilience anti-patterns.

## Haiti Earthquake

**Port au Prince, Haiti, 2010,**

**2-30000 dead, $5 - $15bn damage**

*Broad profile*

9. Extremely severe 7.0 earthquake, coupled with extremely poor quality concrete construction in a newly-high-rise city decimates an entire country. Unusually efficient international response spearheaded by the US Army in the wake of the crisis maintains social order even though most of the government's buildings have been levelled with enormous loss of staff lives. Long term management of reconstruction is proving problematic, however.

*Specific lessons*

a. Building codes were responsible for most of the deaths: Pisco, Peru suffered a larger earthquake (8.0) and - for a city of 130000 - lost only 500 lives. The crucial difference is that the majority of concrete construction was to earthquake-appropriate codes, and buildings did not "pancake" with entire floors crashing down flat on each-other resulting in total loss of life as was common in Haiti.

b. International community response more-or-less ran Haiti in the immediate post-crisis period because the government had been shattered. Surprisingly, this worked during the immediate crisis, with objections limited to objections about US control of the airport and air traffic control.

c. Long-term control of the assets raised by NGOs becomes a major factor as local capacity to responsibly spend the money in accordance with NGO standards of accountability is inadequate to the funds allocated to the crisis. Governance issues that had not caused severe problems during the crisis phase reassert themselves with teeth. Problems persist to this day.

*Notable interventions*

10. Cell phone services prove to be amazingly resilient, with some providers offering continuous coverage through the crisis while nearly all other modes of civilian communication failed. Landlines fare extremely poorly in comparison. (Why Haiti's Cellphone Networks Failed, Anne-Marie Corley, 2010).

11. Pre-existing digital maps of Haiti are inadequate. However, post-disaster satellite and drone imagery is used by an international volunteer team (CrisisMappers, Open Street Map etc.) to provide high quality maps, roadint etc. to responders. These maps become heavily used during the relief phase of operations. This is generally heralded as a great success for civil society helpers.

12. Civil unrest is widely viewed as a major risk factor. The US Army largely solves the problem by importing and making it widely known that there are adequate food supplies on the island, although local unrest around food distribution remains an issue for some time.

13. Deep difficulties in NGO coordination are largely forestalled by military lead, and resume as the military withdraws from the situation.

14. UN Peacekeepers allegedly bring cholera with them, causing an epidemic some time after the disaster. Reports blame inadequate sanitation in their barracks. (Haiti cholera epidemic caused by UN, say experts, Mark Doyle, BBC News, 26 July 2013).

*Conclusion*

15. **Network resilience was completely unexpected** - in a mostly-collapsed city, some cell providers continued to provide uninterrupted service. As noted, international "swarm cooperatives" provided much-needed digital maps, and coordinated person-finder and other services as required by international agencies, with the UN coordinating. Most commentators evaluated these services as very successful. The sheer scale of destruction was unprecedented, but (all things considered) cleanup went well, although later rebuilding has been extremely troubled, with access to land and property rights being key issues.

## Hurricane Sandy

**New York/New Jersey (mainly), America, 2012**

**300 dead, $70bn damage**

*Broad profile*

16. An enormous hurricane system sweeps through the Caribbean and US, but most areas impacted are relatively well prepared - Jamaica, for example, suffers only one casualty from the hurricane even though 70% of the island loses power. New York and New Jersey are hit unusually hard, with the New York subway system flooding, large scale persistent power outages, a breakdown of food distribution systems and more. However, rapid and heavy use of troops to provide essential services is efficient and successful, and loss of life - given the circumstances - is surprisingly low.

*Specific* lessons

a. In only 10 years, US disaster response had transformed from the bureaucratically incapacitated Katrina example to a more-or-less model response. Very nearly every lesson that could have been learned from Katrina was applied: early evacuation, rapid integration of military resources into the relief effort, and efficient cooperation with civilian volunteerism.

b. Power grid fragility was, by far, the most severe problem in the entire situation. Major loss of life was entirely possible, with millions of people without power for an extended period, and temperatures dropping far below zero only days after power was restored. Longer delays or worse weather could have had catastrophic consequences. Transportation fuel supply would also have been a severe issue had it not been for the extensive use of US military fuel supply infrastructure by civilian responders.
c. The subway system, although extensively flooded, was back in service within weeks.

Notable interventions

17. On the order of 10000 national guard and regular military deployed, with millions of gallons of fuel and millions of meals being run through military logistics, and power being provided by military generators and mobile power plants (DOD Provides Hurricane Sandy Response, Relief Update, American Forces Press Service Nov. 3, 2012).

18. The Occupy Sandy group - a literal descendant of the Occupy protest group - used pre-existing social networks and technology to organise response. Their experience with grass-roots self-organising systems proved highly effective in the crisis, and has been noted as a possible model for future large scale relief efforts, in particular their use of the internet to broker specific personal relief needs ("nappies and baby formula needed in Crown Square", "car needs a jump start in Brooklyn Heights") which more institutional responders have trouble with in conventional relief management frameworks. (Occupy Sandy: A Movement Moves to Relief, New York Times, November 9 2012).

19. Notable absence of command-and-control problems throughout the operation.

*Conclusion*

20. Absolutely spectacular example of institutional learning minimised loss of life in a potentially very nasty situation indeed. Luck with weather still a major factor in preventing loss of life: if the cold snap had arrived a few days earlier, disaster. First major use of volunteer networks coordinated by internet for small-needs and door-to-door services for vulnerable populations, and an excellent division of responsibility between military, first responders and civilians managing logistics, emergency response and local needs.

## Broad threads and lessons learned

21. Firstly, network infrastructure proves to be amazingly robust: even under enormous load, with extensive physical infrastructure damage, it frequently stays up. It is far from perfect, but on several occasions network infrastructure has completely outperformed expectations and proven to be a critical backbone to relief efforts. In particular, persistent problems with interoperability of radio standards are getting solved by consumer technology digital systems (even if that

is as simple as cell phones and Excel spreadsheets of relevant phone numbers). The implication appears to be "build on success."

22. One irony is that in many cases, the electrical grid goes down while the communications network keeps working up, because in network backbones often stay up on diesel generators. While the end-user devices like phones are good for a day, they then lose power. Expedient charger infrastructure, probably running off diesel, seems like a natural fit for many situations. This pattern recurred in Haiti and Sandy, and is also seen in Africa where rural areas often have cell phone service, but people walk for miles to charge their phones.

23. Furthermore, software used in crises is largely cobbled together by volunteer efforts and a few small software charities like the Ushahidi Foundation. There is a clear role for a State-provided "decentralized 999" service which could help people in a broad-scale, whole-systems crisis identify their resources and needs, and connect people together to solve their problems. For example, running out of nappies is a major inconvenience, and even a small supply chain disruption could cause that problem. Having a friendly neighbour locate and bring around supplies can make a huge difference to the comfort of old people in a crisis-stricken area, and in extreme cold or heat could easily be life saving. In situations which call for extremely broad response, how can the State assist civilians to help each-other? Occupy Sandy has shown the power of grass roots networks - how can the State cooperate with and empower such networks further?

## CASCADE FAILURES - *FINANCE, POWER AND NETWORKS*

24. The disasters we have examined so far are simple large scale natural disasters - events which occur in a relatively localised region, with spike event impact and subsequent recovery. These spike events occupy a relatively small portion of the possible space of events. Systemic risks, such as flu pandemics or some of the worst-case cyber contingencies are in a completely different category of risk. The swarming behaviour, where aid streams into an affected area from the outside, may not be possible in a catastrophe which has no border. A pandemic particularly is everywhere at once almost by definition, and one which is severe enough to put stress on critical infrastructure due to absenteeism is unlikely to be even remotely contained. While we cannot address the full complexity of such a scenario here, we can observe that systemic risks and cascade failures have a few things in common which may make current sophisticated and successful approaches to disaster management substantially less successful.

    a. Systemic risks and cascade failures prevent resources moving into the crisis area from outside. All approaches which use centralise resources, including deployment of the military, will be limited to addressing the areas which have the most severe problems, or attempting to maintain a few specific systems (like power or backbone communications).

b. Systemic risks and cascade failures tend to be cross-system: electricity grids are required for communications grids and sewage systems, and logistical systems are dependent on both. Logistical systems is affected by a situation like quarantine have extremely long-reaching and unpredictable impacts: consider the loss of years of medical research because lab animals could not be predictably fed on schedule, for example. These kinds of risks are minor individually, but they increase the social cost for even a minor logistical or grid disruption exponentially. *This is a key argument for resilience and against senseless irresilience*.

c. Cascade failures in interconnected grids often make an entire co-existent system of grids as weak or weaker than the weakest subsystem involved. This counter-intuitive results shows just how clearly the devil is in the details. (Catastrophic cascade of failures in interdependent networks, Gene Stanley, Nature 464).

d. Systems which are extremely reliable tend to wind up without redundant backup systems, stockpiles to act as buffers, and similar resilience measures. The combination of card payments and ATM machines means that most people do not have a substantial cash reserve at home. Many companies have a single connection to the internet at each location, because business-class network connections have so little expected downtime. In all cases, an extremely reliable system tends to result in redundant systems being defunded as time passes. Manufacturing relies on just-in-time delivery, cloud providers like Amazon are generally-speaking more reliable than the power grid in many cases, and the result is systems without a second are now commonplace.

e. Some trigger points for systemic risks and cascade failures are common and well-understood: pandemic flu, financial crisis, cyber attacks. However, extremely complicated networks may have entirely new modes of failure - positive feedback loops across connected subsystems in different jurisdictions, or fragility like a cyber-attack on one grid causing catastrophic issues in connected computer systems.

25. As we have not seen large scale cascade failures in practice since the Spanish Flu of 1918 - although some might suggest the financial crisis is a near-failure - the general consensus is that responders are ill-prepared for any everywhere-at-once event. Certainly within the pandemic flu community, the awareness is that society is more-or-less completely unprepared for an event of any severity, and that most flu planning is wholly inadequate to the level of risks presented. But because the frequency of events is less than once or twice a generation, there is very little public awareness of the need to prepare. The same may be true of the financial crisis: safeguards erected after the 1929 crash were gradually repealed until many of the same high-risk behaviours entangled the system and brought the world to the brink of a serious lockup. Although the 1918 flu killed 3% to 5% of the global population at the time, at nearly 100 years ago, cultural and institutional memory has faded, and those in the field attempting to raise awareness of the risks and implement mitigation procedures for the expected,

upcoming, overdue pandemic flu event are often marginalised within their respective fields.

26. The lessons learned from Hurricane Katrina clearly had a huge impact on response to Hurricane Sandy. But those lessons will be lost over time unless there are frequent refresher courses from real world events. Is it possible that carefully targeted historical education could preserve of previous events and keep the necessary perspectives alive for longer?

## WICKED PROBLEMS

**"You know it is a whole system when the costs show up in one place and the benefits show up in another."**
**–** *Gupta's Law of Whole Systems*

27. The costs of preventing or managing systemic crisis or cascade failure do not typically show up where the worst impacts will be. Like climate change, the worst-affected areas are essentially random: any given emitter of carbon is unlikely to be affected proportionately to the carbon they have emitted. Fragility is not tightly coupled to the origin of the risk. Perhaps redesigning airports could change the pattern of pandemic spread in a way which could prevent the collapse of medical systems - but can hospital managers pool funds to pay for the redesign of airports, against the risk in some future scenario? We lack the ability to map cause and effect accurately enough to do mitigation, and even in the cases where we strongly suspect a relationship, institutions generally lack the ability to assign budget to mitigate risks which are strongly affected by the complex interrelationships which define systemic risks and cascade failures.

28. This takes us into the domain of wicked problems, VUCA (volatile, uncertain, complex, ambiguous), goat rodeos and similar attempts to describe wrestling with uncooperative whole systems. Although there is plenty of discussion of these issues, at this point there is no decisive breakthrough in how organisations or individuals can address them. "Here be dragons" is, bluntly, as far as publicly available work has gone in the area.

### Network mapping for wicked problem management

29. There are basically two approaches to this terrain: a high-tech, largely unproven **risk targeting** approach, and a low-tech, unfashionable, brute-force and ignorance **stocks-and-buffers** approach. The high-tech approach is favoured in the US. The notion is to accurately map a critical infrastructure network. This map is then analysed using network analysis and risk contagion techniques to identify a limited number of areas of extreme fragility which can be systematically reinforced or have redundancy added to them to protect the network as a whole.

(Interdependency Modelling: A Survey of U.S. and International Research P. Pederson et al, Idaho National Labs 2006).

30. However, it is not clear, given what we know about complex systems theory and in particular sensitive dependence on initial conditions that such approaches can work, even under ideal circumstances. Unless both **the initial map and the analysis** are perfect there may be unmapped modes of failure and those modes can be arbitrarily severe. The analogy is the risk management approaches done by financial houses before the financial crisis, in which assumptions were made from historical data about asset classes whose movement was not correlated. In the past, they had not been. However, when entire markets shifted in never-before-seen ways, new correlations occurred between previously uncorrelated asset classes, and contagion leapt from system to system in unprecedented ways.

31. Infrastructure modelling and analysis is a new discipline with little real-world experience to highlight problems, but - given experience in other fields - it is likely to be vastly harder to model systems in a way which gives genuine insight into robustness than is initially thought. Another parallel case is static analysis of computer network traffic and resilience: maps are essentially perfect because all systems are digital and can be mapped by software, but new modes of failure are constantly discovered experience shows. Ruthless complexity control and plain old human expertise are critical assets for managing these kinds of risks - even in computer networks, software analysis of vulnerable network configurations is still not a substitute for redundancy and experience.

32. It may be logical and rational to use network analysis to **identify systems which are certainly not resilient**, or even to make an over-all estimate of the boundaries of system resilience. It is much, much harder to imagine a consistent, coherent practice of using network analysis and simulation to prove that a critical infrastructure network is resilient. This is directly analogous to finding bugs in software: automated tools can prove there are bugs. They cannot prove there are no bugs. But if a cursory scan produced a lot of bugs, there are almost certainly more the tools did not detect. Complex systems have a lot of very unhelpful properties in common: there is a (thus-far) irreducible aggravation in dealing with them, and that must be remembered at all times, but never more than when evaluating vendor or researcher claims of reliability.

33. We should also consider the possible abuses of such tools. Could a malevolent user **identify points of system fragility** using software to map and analyse the infrastructure networks, then strike? Certainly such approaches have been discussed for many years, although there are no reports of such attack methodologies in the wild. But the possibility of "weaponized cascade failure" particularly in electrical or financial systems must be held as a real threat. While there are some networks which, in a pinch, we can live without until a manual reboot is performed (up to and including cellular phone services) there are other systems, primarily the electrical grid, which in certain climates at certain times of year are simply necessary for substantial numbers of people to stay alive. Again, there is a mapping problem: it is not clear that accurate maps of the expected

impacts of various kinds of grid failures are available to most of the potential responders, either because the analysis has not been done, or because the analysis is classified. In either case, the municipal responders which would be the first line of defence in any such crisis are clearly, in the general case, under informed. **What people are not aware of, they cannot prepare for.**

## "Brute force and ignorance" risk mitigation

34. The flipside of this approach is the more traditional human approach to complex systems risk: Obey Murphy's Law. What can go wrong, will. All complex systems are assumed to be fallible, and the emphasis is not placed on improving estimates of 99.999% reliability. Rather, the focus is on **"when this fails, what else will break?"** This kind of approach is embodied in recent years by the US Ready.gov suggestion that all families should have a 72 hour kit including food, water, medicines, documents, pet supplies (!) and so on. The kit is also specified to include items necessary to survive in prolonged period without electricity, water, power or other essential services. Importantly, the suggestion is not limited to areas which have a clear risk like storms or earthquakes. It is framed as being a prudent precautionary measure for everybody regardless of visible exposure to risk, and as a baseline from which those in higher risk areas should build.

35. **Interestingly, history has shown that preparatory efforts of this kind are very difficult to adopt at an individual level.** Although the government recommendation is made, the actual adoption is very slow. In areas with regular crises a "culture of preparation" arises and people get better and putting plywood shutters over their windows when storms are coming in, have well-stocked basements and so on, but it appears to take regular exposure to change culture. There are subcultures which do manage preparation in the absence of regular disaster, most notably the Latter Day Saints ("Mormons") who are remarkably prepared for a population which does not see regular crisis, frequently having six months to two years of food per household member in dedicated storage areas of their homes. But there is no known method for moving this kind of thinking from subcultures and regularly-exercised capabilities formed by real challenges into the general population which is at-risk but does not believe itself to be so.

36. Organisations do better, but not much. Pandemic flu preparation, while theoretically a major priority, with near-miss events in recent memory (the Mexican scare of a few years ago, and before that SARS) is still notional in many organisations. Public perception of preparation - defensibility, rather than actual preparedness - is commonly found, with very few agencies indeed actually braced for the full possible impact of such an event.

37. The specific goal of preparation for systemic crisis is **decoupling**. Yes, there may be huge cascade failure problems in the medical supply chain, but if the hospital has 30 days of all basic supplies and a redundant diesel backup generator system, the risk of cascade failures in external systems affecting patient care are minimal. This kind of approach is easy to describe conceptually, but hard in practice - in fact, logistical and grid dependencies for large organisations are usually so poorly understood that during a time of crisis unexpected failures due

to external risks are the norm. Once again we are back at the analysis point: is it possible to use software to identify what to stockpile, what to make redundant, and what to back up? Or will we once again face the situation where inherent complexity and cost preclude building a clear-enough understanding of needs to produce reliability?

38. It might be gilding the lily in nations with stable infrastructure, strong states and manageable risk, but there's also the rest of the world to consider. In Namibia, for example, many factories have to provide all of their own electrical power because grid energy is so expensive and unreliable. The locals know it and get used to it, but one of the problems with internationalising business is managing the flakiness of the underlying infrastructure in many parts of the world.

39. In short, the stockpile-and-buffer approach to service resilience **does not work either.** People do not stockpile. Organisations can barely work out what to stockpile. It is extremely unclear who pays for the resilience measures required above the level of the individual household's emergency food/water/drug supply - is resilience a national mandate, or hospital-by-hospital? The fragility cannot be overestimated, and if a solution exists, it is likely going to be extremely dependent on novel uses of ICT, while at the same time we must face the facts.

**Even pure-software systems are unreliable. Expecting software to save us from the unreliability of other systems is double folly, even if it is the only viable path forwards.**

## Action in the Crisis

40. It is clear that communication networks and software to analyse risk are key areas of movement in disaster preparedness and urban resilience. Keeping the show going during the hard times is increasingly about network bandwidth, social organisations, smooth interoperability between actors of different classes and various other functions which are "stereotypically digital." The internet has shown, through examples as diverse as Wikipedia and Ushahidi, what massively collaborative projects can achieve. Some of this culture has bled through into cooperative models on the ground in the face of real disasters. Massive progress has been made in the US at keeping the bureaucratic systems on the same page - can the same be said in the UK, or anywhere else? However, even misconfigured bureaucracy is mitigated by readily accessible networks and appropriate software to help coordinate civilian response. This whole area is ripe to be professionalised. The extension of state and municipal services through the internet is well-advanced in non-critical areas, but it is clear that extending the approach to crisis scenarios is inevitable, given the success of amateurism in these fields.

This extension creates four questions which must be answered:

1. how do we make sure that the systems stay up?
2. how do we make sure the systems are, in fact, not the cause of the crisis?

3. how do we interface various bodies with the expedient response networks?
4. how do we manage trust and expectations on informal networks?

## The Reconfigurable City

41. The ability to optimise deployment of the resources a culture has to meet human needs is the core asset of civilizations. We currently solve this problem with a combination of government, markets and civil society responses. The addition of digital networks is adding some new capacities to these systems, and producing new modes of activity like commons-based peer production (the economic mode of Wikipedia or Linux).

42. In the city, smart buildings, grids, networks, and upcoming technologies like self-driving vehicles start to offer new options in managing natural disasters and other points at the edge of chaos. New risks come with these technologies, but the overwhelming direction of travel is towards resilience through enhanced situational awareness and dynamic reconfigurability.

43. Imagine how much easier coordinating an evacuation is in a city populated by driverless cars. All roads can be used optimally, and people collected in order of vulnerability. This kind of global optimisation of evacuation is previously unthinkable, and is just over the horizon. Smart grids offer the same kind of utility: selectively turn off power building-by-building as flood waters approach to prevent electrical fires and damage to grid equipment.

44. Actually implementing systems of this kind is probably going to take somewhere between ten years and four decades. The questions of incumbency, shifting of risk from one demographic to another, political control of software systems, and the ever-present spectre of irreducible complexity haunt all aspects of this work. But it's clear that the move towards smart cities is inevitable as infrastructure learns to dance, so the sooner work is begun on the policy and bureaucratic integration of flexible response to complex contingencies, the better. Simulation is hopefully going to be a good substitute for trial and error, even with all the difficulties noted with infrastructure and grid simulation approaches, but there is going to be no substitute for the gradual building of trust, experience and understanding between the blue light services and smart city engineers. This is predominantly a social problem, a question of building shared expectations, shared language and shared vision as an incubator for breakthrough capabilities.

45. Codesigning the smart city with responders may be key to its resilience.

## Conclusions

46. Conclusions specific to client.

# BIBLIOGRAPHY

Army Support During the Hurricane Katrina Disaster, James A. Wombwell, 2009.

Catastrophic cascade of failures in interdependent networks, Gene Stanley, Nature 464.

DOD Provides Hurricane Sandy Response, Relief Update, American Forces Press Service Nov. 3, 2012.

Haiti cholera epidemic caused by UN, say experts, Mark Doyle, BBC News, 26 July 2013.

Interdependency Modelling: A Survey of U.S. and International Research P. Pederson et al, Idaho National Labs 2006.

Occupy Sandy: A Movement Moves to Relief, New York Times, November 9 2012.

STAR-TIDES and Starfish Networks: Supporting Stressed Populations with Distributed Talent, Defense Horizons 70, Linton Wells II, Walker Hardy, Vinay Gupta, and Daniel Noon, December 2009.

Why Haiti's Cellphone Networks Failed, Anne-Marie Corley, 2010.

# BIOGRAPHICAL NOTE

**Vinay Gupta**

A software engineer by trade, later becoming an expert in energy policy and disaster relief, Gupta focusses on making complex problems simple enough to solve with COTS systems and components. He is best known for the hexayurt shelter system (for refugees and natural disasters), Simple Critical Infrastructure Maps (in use at US DOD STAR-TIDES project), CheapID (a proposal for cryptographically secure private biometric ID cards) and his practical work on voluntary cooperation in organizational design. Current and former clients include Council of Europe, UK MOD, US DOD (OSD-NII).