Building resilience in virtual and physical networked operations

Jennie Phillips MA
PhD Candidate, University of Toronto, Toronto, ON, Canada
(corresponding author: jennie.phillips@mail.utoronto.ca)

Alexander H. Hay BSc (Hons), CEng, PEng, FICE, FinstRCE, CRM
Principal, Southern Harbour Ltd, Etobicoke, ON, Canada

As society becomes increasingly networked, both physically and virtually, so do human operations. This change exposes a unique subset of challenges and risks associated with the intersection of systems and the potential for cascading failure. Yet existing risk and resilience dependency models fail to accommodate these complexities, potentially exposing the capabilities that infrastructure systems enable to catastrophic failure. This paper builds on operational resilience (OR) theory, to develop a theoretical framework for developing resilience in physical and virtual networks, the networked OR framework. The authors argue that risk tolerance and resilience are developed through the concept of a projected tableau which is well situated in the broader network context. An overview of resilience, networks and OR is provided, with an explanation of the networked OR concept, a revised framework for developing resilience in networks and application to an emergency services network.

Introduction

Technology concentrates value and therefore densifies networks in both time and space. The consequence of failure increases in magnitude and complexity. As high-rise vertical communities continue to populate urban centres, the value of operations is concentrated. This increased demand and dependency on enabling systems implies increased vulnerability when these same systems fail. Further, the interconnectivity between these systems means that failure affects parallel operations that previously would not have been affected. The net result is that the cost of loss goes up in terms of lives, livelihoods and financial burden. Consider the Calgary floods in 2005–2013, for example. Following a threefold increase in rainfall, the floods in 2005 led to the displacement of 1500 Calgarians, 14 municipalities declaring a state of emergency and C$275 million (1 CAD = 0.76 USD) in insurances loss (Anon, 2013; Calgary Public Library, 2014a). The 2013 flood waters rose above previous records with a flow rate three times the 2005 floods; 110 000 were displaced, 32 municipalities declared a state of emergency and C$1.7 billion was reported in insurance loss (Calgary Public Library, 2014b). The increasing impacts of climate change, combined with an increasingly connected society, means that society cannot buy itself out of bad planning and disruption management. Infrastructure systems need to be planned and designed to cope with the increasingly complex demands of socio-economic survival and recovery in a catastrophe.

Through resilience planning, these challenges can be addressed. Different disciplines recognise this potential from infrastructure to business and from organisations to communities to individual psychology. Yet existing models fail to address the intersection between these systems. Specifically, they do not accommodate the complexities associated with operations that are increasingly networked across different systems. A need exists to identify mechanisms to develop resilience for what an operation must do and the eclectic blend of systems it depends on in a distributed context so that what infrastructure must be capable of can be specified better.

This paper presents a theoretical framework for developing resilience in networked operations, the networked operational resilience (NOR) framework. The study involved contrasting network theory and resilience theory across infrastructural, organisational and community domains with the operational resilience (OR) framework. The analysis involved revising the OR framework specific to complex networks (NOR). The NOR framework is distinct in that it (a) situates the operation in the network and (b) builds on the tableau concept to build network resilience along a continuum. The concept and application of NOR is explained through an infrastructure (hard and soft) lens, specifically infrastructure networks (built, natural and virtual) and the networked operations (physical, virtual, hybrid) that they enable. The discussion provides an overview of networks, resilience and OR theory and explains NOR by distinguishing this concept from OR, providing a step-by-step framework and applying NOR to examples of emergency services throughout. The results of how the theory is applied will be explored in more depth in subsequent papers, where the authors will closely examine the application of NOR to specific case studies.
Networks
From physical networks – for example, traffic networks or oil pipelines – to virtual ones – for example, the Internet or a coffee franchise – a network is ‘any collection of objects in which some pairs of these objects are connected by links’ (Easley and Kleinberg, 2010) and is characterised along different dimensions. First, the traditional study of networks focused on the structural dimension – that is, the spatial arrangement and composition of networks. The attributes include (a) the topology, typically a random (Erdős and Rényi, 1959) or scale-free structure (Barabási, 2003; Watts and Strogatz, 1998), such as a road network against a flight network; (b) boundaries, open or closed access through active measures or naturally emerging boundaries – for example, gated communities or membership requirements against geographic, political or language boundaries (Dunbar, 1998); (c) scale, the size of the network (Goldstein, 2012; McConney and Phillips, 2011); (d) scope, the diversity of nodes (Buckley et al., 2015; Hay et al., 2014; Seville et al., 2015; Weick and Sutcliffe, 2011); (e) centrality, the distribution and leadership structure (Borgatti, 2005; Freeman, 1979; Powell, 1990; Siebeneck et al., 2009; Stein et al., 2001); and (f) connectivity, the density of the network (Easley and Kleinberg, 2010; Granovetter, 1973). Yet as networks increase in complexity, traditional methods lack the depth of analysis required. Thus, networks are also analysed as naturally emerging systems, such as vitæ systems of systems (Bristow, 2015; Hipel et al., 2011; Okada, 2004; Okada, 2006), or federations of systems (Krygiel, 1999; Maier, 1998; Sage and Biemer, 2007), with analysis along a dynamic dimension (Norriss et al., 2007). Attributes include (a) the state or health of the network, links and nodes (Piraveenan et al., 2013; Podofillini et al., 2015); (b) the evolution of the network; (c) the exchange, the commodity (entity being exchanged), spread and transmission (Barabási, 2003; Borgatti, 2005; Stein et al., 2001); and (d) culture, leadership and governance – for example, trust, leadership style, benefits, agreements, rules and regulations, conflict or plans and policies. Finally, network components cannot be characterised in isolation; they must be understood in relation to the larger system at multiple levels (Boon et al., 2011; Bronfennbrenner, 1977; Phillips, 2015; Rose, 2004; Sun and Stewart, 2007). As such, the authors will classify networks along three system level dimensions: the macro level (network or system level), meso level (clusters and relationships) and micro level (nodes ranging from individuals or assets to organisations to subnetworks). Table 1 outlines an example of a network grid showing how all three dimensions can be used to characterise a network.

As applied to infrastructure, networks are considered as complex systems of hard and soft infrastructure. Hard infrastructure consists of the physical systems that enable the soft infrastructure (operations) – for example, road or telecommunication networks – spanning three primary domains: built, natural and virtual. Soft infrastructure includes the institutions and/or virtual networks spanning education, healthcare, emergency services, online and offline communities and so on.

Resilience
With roots in ecology, resilience is traditionally defined as the ability to absorb change, adapt and persist without modifying the traditional structure (Holling, 1973). When conceptualised for complex networks, resilience applies to the intersection between hard systems (infrastructure) and soft systems (human systems) described earlier.

Table 1. Framework for characterising a network

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Macro</th>
<th>Meso</th>
<th>Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Structural</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology: structure (scale-free, random), links (physical, human face-to-face, human virtual), entities (human, objects)</td>
<td>Type of network</td>
<td>Types of relationships</td>
<td>Types of nodes</td>
</tr>
<tr>
<td>Boundaries: openness (open, closed), cause (induced, natural), types (functional, geographical, social, contextual), membership (compliance, fees, capability, trust)</td>
<td>Boundary of network</td>
<td>Types of clusters</td>
<td>Terms of membership</td>
</tr>
<tr>
<td>Scale: geographic/relational span, number of nodes and clusters</td>
<td>Size of network</td>
<td>Size of clusters</td>
<td>Size of nodes</td>
</tr>
<tr>
<td>Scope: diversity/plurality against homogeneity</td>
<td>Diversity of clusters</td>
<td>Diversity of nodes, relationships within cluster</td>
<td>Diversity of external nodes and relationships</td>
</tr>
<tr>
<td>Centrality/distribution: power distribution (leadership – directed or collaborative), geographical/contextual distribution</td>
<td>Distribution of network</td>
<td>Distribution of clusters</td>
<td>Node distance and nature of relationship with other nodes</td>
</tr>
<tr>
<td>Connectivity: dense against looseness, path length</td>
<td>Density of network</td>
<td>Density of clusters (within, between)</td>
<td>Strength of ties, number of relationships</td>
</tr>
<tr>
<td><strong>Dynamic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>States: healthy against unhealthy; affected against unaffected; binary, continuous, discrete</td>
<td>State of network</td>
<td>State of clusters and links</td>
<td>State of nodes</td>
</tr>
<tr>
<td>Evolution and lifespan: indefinite against definite time period, history (temporary, short term, long term)</td>
<td>History of network</td>
<td>History of clusters</td>
<td>History of nodes</td>
</tr>
<tr>
<td>Exchange: commodity (entity, relational), transmission (conserved, non-conserved), spread (broadcast, parallel, serial), flow (unidirectional, bidirectional)</td>
<td>Commodity interaction with network</td>
<td>Commodity interaction with clusters</td>
<td>Commodity interaction with nodes</td>
</tr>
<tr>
<td>Culture, leadership and governance: leadership style, autonomy against dependence, collaboration against isolation, polices and regulations</td>
<td>Culture, leadership and governance in network</td>
<td>Culture, leadership and governance in clusters</td>
<td>Influence of network on node and of node on network</td>
</tr>
</tbody>
</table>
Consequently, it encompasses the ability to sustain impact (elasticity) and bounce back after moments of instability (buoyancy) (Bruneau et al., 2003; Gunderson and Holling, 2002; Holling, 1973) combined with the ability to learn, change to a new set of conditions and bounce forward (evolution) (Home and Orr, 1998; McManus et al., 2009; Riolli and Savicki, 2003; Weick and Sutcliffe, 2011). Drawing from definitions of and capabilities for resilience across disciplines (McManus et al., 2009; Rose, 2004; Walker et al., 2002), resilience applies to four main principles: prevention, absorption, adaptability and retention of the same function/purpose. Drawing on these principles, the authors define network resilience as ‘the essential ability of an operation to respond to and absorb the effects of shocks and stresses and to recover as rapidly as possible normal capacity and efficiency’ (CRCI, 2016). And the authors define the capability for network resilience based on the literature highlighted earlier (Figure 1) through eight characteristics, moving from macro to micro system-level dimensions

- Unified: unified purpose, collective ownership, strong identity and commitment
- Coordinated: effective leadership and governance, faith in leadership, space for emergence and self-organisation and conflict management
- Connected: distribution of impact, minimised logistical burden, collaboration and resource sharing
- Engaged: situational awareness, ongoing communications, information sharing and openness
- Reliable: trustworthiness, reciprocity and technical capacity to deliver
- Resourceful: redundancy, diversity, learning, experimentation and innovation
- Agile: rapidity, fluidity, flexibility and adaptability
- Autonomous: robustness, islanding and psychological resilience

All networks possess a level of inherent (pre-existing) and adaptive (to develop) level of resilience and risk, which varies depending on the nature of the network and surrounding system (Home and Orr, 1998; Mallak, 1998; Rose, 2004). A scale-free topology, for example, may be resilient to random attacks but vulnerable to targeted attacks to the hubs (Barabási and Bonabeau, 2003; Siebeneck et al., 2009; Wang and Chen, 2003). The identification and management of inherent and adaptive risk and resilience at the operational level is accomplished through the OR framework, the topic of the next section.

**Operational resilience**

The OR framework provides a useful foundation for the development of resilience in networks, as it focuses on the synergy between the component parts of a system instead of the individual risk and resilience of each in isolation. This framework is based on the ISO 31000 standard risk management process (ISO, 2009), with overlaps described at the end of this section. The aim of OR is to develop resilience, not based on the anatomy of an operation, but more on what it must achieve. Infrastructure, for example, can be robust but not resilient as it cannot self-recover. It is made resilient by strengthening the systems that it enables and that can allow it to recover. In turn, resilience is developed for the operation, in part by understanding the roles of individual components in enabling the operation. By understanding the role of infrastructure, for example, the design brief can be defined by both performance and capability criteria. Drawing on previous works (Bristow, 2015; Bristow and Hay, 2014; Hay, 2013a, 2013b, 2014; 2016), the concept and process of OR is primarily described briefly in the next sections through an iterative four-stage process, with application to a fire service example throughout. The discussion concludes with the need for a networked approach to OR.

**OR framework**

**Step 1: mission and operation definition**

This stage involves defining the operational requirement – that is, what the operation must do and what it depends on to achieve its purpose, as well as how it must be restored to continue to meet that purpose. This stage begins with defining the operation – that is, isolating the part of the system that needs to be made resilient (bounding the system). The central purpose between subsystems (to a unified purpose) and what these must be able to do to achieve that purpose (associated operations) are identified. Each operation is studied through its enabling functions and each function is analysed through its associated dependencies, categorised into human, organisational or infrastructural

---

**Figure 1. Eight characteristics for network resilience capability**

<table>
<thead>
<tr>
<th>Unified</th>
<th>Coordinated</th>
<th>Connected</th>
<th>Engaged</th>
<th>Reliable</th>
<th>Resourceful</th>
<th>Agile</th>
<th>Autonomous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified purpose</td>
<td>Effective leadership and governance</td>
<td>Impact is distributed</td>
<td>Situational awareness</td>
<td>Trustworthy</td>
<td>Redundancy</td>
<td>Rapidity</td>
<td>Robustness</td>
</tr>
<tr>
<td>Collective ownership</td>
<td>Faith in leadership</td>
<td>Minimised logistic burden</td>
<td>Ongoing communications</td>
<td>Reciprocity</td>
<td>Diversity</td>
<td>Fluidity</td>
<td>Islanding</td>
</tr>
<tr>
<td>Strong identity</td>
<td>Space for emergence and self-organisation</td>
<td>Collaboration and resource sharing</td>
<td>Information sharing</td>
<td>Technical capacity to deliver</td>
<td>Learning, experimentation and innovation</td>
<td>Flexibility</td>
<td>Psychological</td>
</tr>
<tr>
<td>Commitment</td>
<td>Conflict managed</td>
<td></td>
<td>Openness</td>
<td></td>
<td></td>
<td></td>
<td>resilience</td>
</tr>
</tbody>
</table>

**Macro**  
**Meso**  
**Micro**
components, and component demands. Recall that infrastructure consists of three domains (built, natural and virtual), so while moving towards applying resilience to built infrastructure, it must be ensured that all domains are accounted for. Second, a dependency analysis is done to construct a causal chain of the operation. This involves determining the effects of each enabling function on the operation and prioritising according to tolerance and impact of disruption. Functions are classified as essential or critical (high-priority; operation would fail if compromised), sustaining or routine (low-priority) internal and external functions. Dependencies are identified for each essential function, exposing critical functions out of the organisation’s control. Third, prioritised functions and dependencies are aligned along the incident sequence (Figure 2) to establish operating thresholds and tolerances and construct a recovery sequence. Starting with routine functioning (pre-incident), the incident sequence begins at $t_0$ (the incident) with a reaction where performance drops to zero, or close to it, and essential and critical functions must be restored to minimum operational capability by $t_1$. Response (from $t_1$ to $t_2$) involves situation-specific restoration to minimum sustainable capacity. And recovery (from $t_2$ to $t_R$) is the restoration of full functionality and, ultimately, to a new routine.

Each of the functions and dependencies along the incident sequence will either be enabled by infrastructure or be infrastructure itself. Establishing a sequence for how an operation must be restored will prioritise different infrastructures and their components, and inform the capability and performance required to support recovery. Yet it is not about standby systems and so on; it is about understanding the diverse and dynamic changing role of infrastructure in enabling an operation in a dynamic and unforeseeable risk context. The aim here is to understand failure truly. And by doing so, society can prepare for various unknown hazard risks, by understanding how hazard effects influence operation (covered in step 2).

**APPLICATION**

With an overall purpose to protect the community from fire and other risks, a fire service may perform three main operations: fire education, inspection and emergency response. The emergency response operation may have internal essential functions, including home visits, fire suppression and rescue. Each of these functions will rely on the internal and external infrastructure (built, natural and virtual) to enable operations. Internal requirements may include a fire hall for coordination and housing equipment and personnel (built). It must be geographically situated to serve a set percentage of the population within mandated response times under different conditions. It must be placed within a portion of the city with no cellular interference (natural) and possess a reliable internal communication system (virtual). Externally, it will require access routes – for example, road networks – and systems for water distribution such as municipal water treatment and supply systems (built), mobile communication systems (virtual) and a fire suppression agent – for example, water (natural). This operation will require internal personnel to manage the response (fire chief) and suppress a fire (firefighters); organisational provisions, including an incident management system for coordination and communication during an incident; ongoing training, liability and legal rights; and supplies, including fire equipment and vehicles. Externally they may rely on dispatch 911 services and an uninterrupted traffic management system to enable quick travel to a site. Following dependency analysis and the construction of the incident sequence, fire suppression may be identified as an essential function, with dispatch, traffic control and water supply as critical functions. Essential dependencies will most likely include firefighting personnel, an incident management system, fire equipment and vehicles and road networks, communication and water supply networks. It may also be found that fuel is a critical dependency to enable use of vehicles.

---

**Figure 2. The incident sequence (Hay, 2016)**
Step 2: operational system analysis
The dependency analysis and incident sequence is developed using the risk criteria and appetite of the organisation as the operational system. In context, it captures the external social, natural and human-made systems and entities that impact or are impacted by the operation, as well as risk associated with the operations surroundings. This context is conceptualised through methods such as the PESTLE (political, economic, social, technological, legal and environmental) or STEEPLE (social, technological, environment, economic, political, legal and ethical) process (Makos, 2015) or by examining the operating context (interdependent relationship), operating environment (influential but independent) and all-hazard context (external threat of natural, human-induced and/or digital harm). Together, these findings are used to characterise the baseline inherent risk to the operation – that is, risk that exists in commonplace – as a control framework to calculate the control cost of risk (cost of risk before treatment when only compliance measures are applied). All-hazard risks are analysed for applied risks in step 3.

APPLICATION
The operating context for the fire service will include the local community. They will depend on the fire service to help them prepare and protect themselves and their homes, as well as respond to incidents. In exchange, fire service will depend on the community to build and maintain facilities according to fire codes and ensure that all occupants are trained on fire safety and evacuation. The operating environment will include the local municipality, which must establish and enforce fire by-laws, provide a legal mandate, fund and endorse fire operations and ensure that public utilities are provided and maintained to enable fire operations. Fire service will also depend on developers and construction companies to integrate fail-safe systems – for example, wet risers for high-rise buildings within carrying capacity. Inherent risks could range from internal operational risks, including equipment failure, funding cuts or physical/mental health risk to personnel, and external risks such as lack of human or fire regulation compliance or building failure beyond carrying capacity. The position of the fire hall and how its response is affected by anticipated events, such as flooding, school drop-off/pickup times and other impedances, will associate the inherent risks with the capability that the (built) fire hall enables, typically described as the percentage of the population that can be provided with fire response within, say, 10 min. This approach is increasingly used in operational audits of municipal emergency services to determine whether the built infrastructure enables or impedes efficient emergency response capabilities. All-hazard risks for the region may include floods and earthquakes (natural), a rise in active shooter activity (human induced) and power/telecommunication failure and cyberattacks (technological).

Step 3: risk and option analysis
Risk and option analysis consists of two stages. First, the applied risks – that is, the directed hazards (potential forms of harm) that may pose risk (chance of harm) to an operation – are identified. All-hazard analysis is the analysis of a hazard in context, rather than a consideration of all possible hazards. When a hazard manifests, it changes the likelihood and severity of other hazards, as well as the ability of the operation to adapt, absorb and respond to other hazards. In effect, all-hazard analysis is an evaluation of the true risk profile of the operation for a given hazard. Second, risk treatment and resilience strategies (options) are identified to allow operations to respond, recover and adapt within operational tolerances and thresholds. For each applied risk, each treatment option is assessed by contrasting the whole cost of risk against the control cost of risk (the product of step 2). As each option has its own residual risk, the whole cost of risk is the sum of the costs of treatment, residual risk and security requirements. If the option has a lower whole cost of risk than that of the control, it is viable. If the cost is higher, then the option is not viable. Critically, this is the point at which the operation owner selects the strategy to pursue. Only once a strategy is selected can tableaux be built (the next step).

APPLICATION
All-hazard risk analysis may reveal that flooding, earthquakes and telecommunications outages are the highest risks to the fire service. Contrasting inherent and applied risks, the risk treatment and resilience strategies may include moving the fire hall away from flood-prone areas or fault lines and ensuring an alternate site is available and widely recognised by the community as a backup focal point. They may build redundancy into communication systems such as ensuring that two-way radios are available or by using third-party communication applications for alternate mobile communications in the event of email failure with a local Internet service provider. They may ensure that a minimum number of personnel are available at all times for set periods, vehicles are refuelled regularly and fire education is increased to minimise fire risk and increase the speed of citizen response times. In partner with the city, fire service may request installation of hydrants, diversification of water pipelines to low-risk zones and by-laws for mandatory embedded wet riser systems in high-rise buildings. It is the combined application of these treatment options that builds resilience into the overall operation. In an operational audit, it was found that it is better to install defibrillator stations on each floor of a high-rise office building above the ground floor due to the paramedic response capabilities during periods of stress. The office complex was outside the emergency response times from the ambulance station for most hazard situations. In this case, an equipment and training solution was used to compensate for an inadequacy in the ability of the built infrastructure to enable timely emergency response.

Step 4: define, refine and project the tableau
The tableau (plural ‘tableaux’) captures the foundation of an operation which is used to enable and replicate operations across the larger system. Consisting of the minimum requirements – that is, the core capabilities and capacities to enable an operation – it acts as a roadmap outlining the essential functions and dependencies required to fulfill the operational requirement. Risk treatment or resilience strategies for inherent and applied risks to the operation (ensuring that the whole cost of risk is manageable...
within target operations) are also included in the tableau. It is the basis for building resilience in networks, elaborated on in the next section. Once defined, the tableau is projected to neighbouring/parallel operations. If the recipient possesses sufficient capability and capacity to enable it, it is imported as a function of the larger operation. Every operation consists of one or more tableaux, and as every context has different constraints, requirements and risks, every applied tableau becomes unique to that context. These properties explain why homogeneity may be observed between operations but each one can function, and fail, very differently.

APPLICATION
As fire service locations replicate across a city, the need for continuity between operations is required for seamless interoperability as well as the combined ability to achieve the overall purpose. This is where the tableau becomes particularly useful. Although each fire station operates within different contexts and constraints, all share the same purpose and, consequently, require the same capability and capacity to achieve that purpose. At this stage, the fire headquarters may establish a common foundation for all fire service stations to follow across a municipality – a tableau. First, it will outline what each station must be able to do, such as respond to house calls within a set time frame with set capabilities (e.g. fire suppression and rescue). Second, it will outline what the operation requires to do so, establishing the baseline capacity (personnel, equipment, vehicles etc.). Third, it will outline the risk treatment and resilience development strategies that must be implemented for that operation. And, fourth, the tableau is projected to existing and new fire stations across a municipality. Those that possess the capability and capacity to enable the operation will import the tableau. As an urban fire station will differ from a local volunteer fire station, the way a tableau is applied will differ across contexts. Demand will be different in densely and sparsely populated areas, for example; thus, the scale and scope of resource requirements will differ, but requirements will remain the same. The risk and resilience requirements will ensure that resilience across operations is achieved. The city may mandate that all stations ensure redundancy in their communication systems, for example. How each operation meets this requirement may differ between stations. One site may use two-way communications, whereas another may use a mesh network system. As long as the whole cost of risk remains below the control cost for each fire service, importing the tableau will ensure that each station will meet this requirement. Applied to a recent operational audit, it would have clearly shown the efficiencies in repurposing two municipal facilities to relocate existing emergency response resources for optimum coverage and efficiency of operations, rather than expanding the existing facility and adding new crews.

Figure 3 outlines the different stages of the OR cycle.

OR and International Organization for Standardization risk management standards
The alignment between the OR process and the ISO 31000 standard risk management process is presented in Figure 4. Step 1 overlaps with establishment of the context; step 2 overlaps with risk identification, step 3 overlaps with risk analysis, evaluation and treatment; and step 4 is a new application for risk treatment.

Need for a networked approach
As applied to Networks, OR is used routinely to evaluate multiple infrastructure domains and dimensions but fails to account for complexities between these domains. As depicted in the fire service example, for infrastructure to enable resilience, it must be recognised that a community’s response and recovery will coincide with that of their neighbours. The fire service department relies on collaboration with the local municipality and compliance from developer and construction networks and shared infrastructure providers. If the community does not take a system-of-systems view, they risk competing with their neighbours for scarce single-source resources. As such, the distribution of operations is not an issue, but defining the boundaries in large-scale complex systems that are common to multiple users is. For example, a national infrastructure model will be used by multiple communities in different ways. After a major incident, each community will be self-recovering. Their actions will directly affect the abilities of their neighbours to recover due to the allocation and access to necessary resources. This is precisely what NOR can address across infrastructure domains.

The remainder of this paper provides a framework for applying OR to networks through NOR and discusses an application of this framework through case study.

Networked operational resilience
NOR uses the tableau concept to synergise operations and develop resilience throughout a complex network, as well as to provide a mechanism to situate the operation. It is explained in the next sections by introducing theoretical concepts, outlining the step-by-step NOR framework and applying the theory to a multistakeholder multipurpose emergency services network.

Theoretical concepts
The tableau and NOR
The tableau is the keystone to the process, as it defines the risk treatment and resilience strategies to be replicated across operations and into the larger network. Drawing on the OR foundation, the authors propose that a network can be made resilient along a continuum in four stages (Figure 5)

- single operation
- neighbouring/parallel operations sharing a similar operational requirement and/or operational system
- critical mass of risk-tolerant/risk-resilient operations being reached to make the network resilient
- new operations (nodes) achieving resilience through affiliation and tableau import.

As the continuum suggests, resilience starts with the operation and replicates outwards until the entire network is resilient. With the tableau being central to this process, the initial tableau is
designed for the operation and external operational system and is projected to other operations performing the same functions, operating in the same operational system or both (Figure 6).

Recipient operations with the capability and capacity to enable the operation will import the tableau and thus adopt the risk treatment and resilience strategies outlined in the tableau. As more nodes import this tableau, as well as develop their own tableau for suboperations, the network will achieve a critical mass of resilient nodes rendering the network resilient. At this stage, new nodes or operations achieve resilience simply through affiliation (as well as through imported tableaux). And old nodes exiting the network will have no impact on the overall resilience. This bottom-up approach for resilience development is echoed in the literature on community resilience (Brewin et al., 2002; Goldstein, 2012; Norris et al., 2007), organisational resilience (Harford, 2012; McManus et al., 2009; Weick and Sutcliffe, 2011) and terrorist networks (Siebeneck et al., 2009) among others. The continuum, however, can also be followed from a top-down perspective. The network can also be analysed as an operation, and the tableau developed is projected down into the clusters and nodes within the network, similar to business franchises.

The composition and transformation of the tableau as it moves through the system can be explained by moving from the micro to meso to macro levels of the network. For this explanation, micro

Figure 3. Detailed OR cycle

<table>
<thead>
<tr>
<th>OR process</th>
<th>ISO risk management process</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Missions, operation definition</td>
<td>a. Establish the context</td>
</tr>
<tr>
<td>b. Operational system analysis</td>
<td>b. Risk identification</td>
</tr>
<tr>
<td>c. Risk and option analysis</td>
<td>c. Risk analysis</td>
</tr>
<tr>
<td>d. Define, refine and project the tableau</td>
<td>d. Risk evaluation</td>
</tr>
<tr>
<td>e. Risk treatment</td>
<td>e. Risk treatment</td>
</tr>
</tbody>
</table>

Figure 4. Alignment between OR framework and International Organization for Standardization risk management process

Figure 5. Continuum of resilience development
is deemed to be the operation, meso is a cluster of operations and macro is the network as a whole. Note that, whether a network or a single provider, NOR analysis always involves analysing each as an operation.

First, the tableau is defined at the micro level for the operation. As explained in the OR framework, each operation identifies an operational requirement, situated within its specific operational system. It outlines what the operation must be able to do, what it depends on and what risks exist with doing so. Risk treatment and resilience-building strategies that are deemed viable (whole cost of risk being less than the control cost of risk) are integrated into the operational requirement to manage these risks. The operational requirement is used to create the tableau (Figure 7). Portions of the tableau may be specific to the operation itself and remain within the operation. Another portion may be specific to the operational system and is projectable as a suboperation/

function to other operations within the same operational system, independent of functional similarity. In other cases, a portion may be operation-specific and projected to operations with functional similarity. Portion sizes will be unique to each operation projection. Risk and resilience measures are integrated within the projected tableaux.

At the meso level (cluster level), each operation will also have a tableau customised to its context. It will have portions that may be projected to suboperations that are functionally or contextually similar operations (Figure 8). It can also import projected tableaux and embed them as a function within the higher operation or already possess imported tableaux from other operations or the operational system. As the tableaux continue to be refined, projected and imported, operational tableaux across the network become an eclectic blend of custom and shared tableaux. In some cases, these tableaux may even be co-constructed between clusters of operations.

At the macro level (network level), the network will also have its own tableau. As depicted in Figure 9, much like the meso and micro levels, it will contain portions imported from its external environment or context, customised to the network level and projectable to all operations within the network. Within the network, operations will import the network tableau into their own tableau and project their own tableau between one another based on functional and/or contextual similarity.

Resilience is achieved in a network once a critical mass of nodes (or operations) have constructed, shared and imported tableau with embedded risk and resilience requirements. Critical mass will vary with each operational system. As an aside, risk and resilience capabilities built at the network level tableau can ensure
that widespread resilience is injected into the network (from a top–down perspective, as described earlier). Similarly, once the network has achieved a resilient state, new nodes gain resilience through affiliation and exiting nodes have no impact on the overall resilience of the network. Yet for the tableaux to build risk and resilience capability effectively, they must be defined from operations that are well situated within the broader network. In response, NOR builds on the OR framework to also include the development of a network profile, build on the risk profile and create a resilience profile.

**Network profile**

First, the network is conceptualised as an additional context to the operational system. By situating the operation, better insight will be gained into the operational requirement and risk and there will be greater ability to create a more universal tableau. By using the network framework or any network modelling tool (e.g. social network analysis, mental modelling and graph theory), the structural, dynamic and system-level dimensions of the network are characterised and a network profile is created.

**Risk profile**

Risk is categorised and classified differently in NOR to better suit the tableau concept and network context. Recall that OR classifies inherent risk as a product of internal operational risk and applied risk as directed all-hazard risk. The NOR framework generates a risk profile where it distinguishes risk into two broader categories of risk. The first, *expected risks*, are the foreseeable risks with foreseeable consequences. They include inherent risk and applied risk consisting of all-hazard risk for the operation and network and network-specific inherent risk. Network-specific risk is assessed during construction of the network profile, identifying any vulnerabilities associated with network dimensions, attributes and the external surroundings (all-hazard). Some risks identified during this process may propagate the entire network, ultimately impacting each operation. In contrast, as described by Weick and Sutcliffe (2011: p. 2) ‘expectations can get you into trouble unless you create a mindful infrastructure’. Thus, there must also be preparation for *unexpected risks*, or ‘predictable surprises’ as colloquially labelled. Thus, the second risk category, unexpected risks, is the unforeseeable risks with foreseeable consequences. They are those which cannot be prevented by planning but can be managed by building resilience. It is important to note that, whether risks are expected or unexpected, failure mechanisms are ‘reasonably foreseeable’ if one understands one’s own operation.

**Resilience profile**

As attributes that render one network fragile may render another resilient, a resilience profile for expected risks is created. Two types of resilience for expected risks are distinguished. The first, *inherent network resilience*, is the resilience that is innate to the system – for example, a leadership culture that promotes self-organisation and emergence is naturally more resilient (Handy, 2007; Home and Orr, 1998; Johnson, 2012; Mallak, 1998; McManus et al., 2009; Weick and Sutcliffe, 2011). Second, *adaptive resilience* is resilience that must be developed for expected risks. It addresses aspects of crisis that can be planned for, specifically the prevention, absorption and recovery aspects of
resilience definition. In essence, adaptive resilience I is developed by addressing all stages of the incident sequence (Figure 2). This is done by implementing a portfolio of crisis management strategies ranging from incident management and emergency management (during the reaction and response stages) and business continuity during recovery (from the planning point).

For unexpected risks, the resilience profile is built on to include a third type of resilience, adaptive resilience II. It covers the learning, adapting and transforming aspect of resilience. It can be developed by doing resilience gap identification (Figure 10), which aims to identify segments of the network that may lack resilience capability. This can be done by contrasting the system-level dimensions (micro, meso, macro) with the eight characteristics of resilience (unified, coordinated, connected, engaged, reliable, resourceful, able, autonomous). A comparison table such as the example in Figure 10 can be used. One goes through each comparison by asking a simple yes/no question: ‘Does this portion of the network (e.g. cluster) demonstrate this characteristic (e.g. autonomy)?’ Intersections where the answer is ‘no’ may allude to vulnerabilities in the network.

Afterwards, explanation of these gaps can be attempted through a second stage of comparison, a resilience gap analysis. First, a comparison between resilience gaps can be done. For example, a lack of trust (reliability) may be identified at the macro level, which is enforced at the meso and micro levels with a lack of collaboration (connectedness) and information-sharing (engagement). Also, observing a lack of autonomy and unified purpose at the micro level could suggest a need for a different leadership strategy to empower operations or build a more cohesive vision. Otherwise, the comparison table can be contrasted with the network profile for further insight (Figure 11). Contrasting the same trust gap against the network profile may reveal that the size of the network is very large and connected mostly by weak ties. This may also suggest a need to integrate relationship-building measures.

The risk and resilience classifications discussed are summarised in Figure 12. As described, expected risks (foreseeable risk and consequence) include inherent risk (associated with the operational requirement) and applied risks (all-hazard, network-specific inherent and all-hazard risk). Unexpected risks (unforeseeable risk, foreseeable consequence) are those that cannot be effectively predicted. Inherent resilience applies to expected and unexpected risks, adaptive resilience I applies to expected risks, and adaptive resilience II applies to unexpected risks.

To clarify the tableau concept further and demonstrate how the OR process is modified to accommodate these changes, the following section provides an overview of the NOR framework.

The NOR framework
The framework for NOR unfolds as described below. This explanation builds on the iterative four-stage OR process with the new concepts discussed in the previous section and includes an application to emergency services in every step.

Step 1: mission and operation definition
This first step remains similar to the OR framework, with outputs still including the operational requirement, recovery sequence,
inherent risk and control framework. Whether regarding an operation or a network, the following fundamental questions must be asked: ‘what is it that is aimed to make resilient?’ ‘what purpose is sought to achieve?’ and ‘what must it do and what does it depend on to achieve that purpose?’ The difference here lies in that three levels of a system are being assessed, the operation (micro level – node), cluster of operations/hubs (meso) and network(s)/subnetworks (macro). Although the NOR process can be used to assess individual operations, it may be done so through the shared operations and function. Focusing on the overlaps helps to address the challenge of developing resilience across different systems by co-creating resilience at these intersections.

**APPLICATION**

At the macro level, an emergency service network will share a common purpose of providing communities with protection and support from harm in an emergency. It will rely on first-response and healthcare operations (meso-level networks) to achieve this purpose. Each will have their own subpurposes, one focused on incident site emergency response and the other on the provision of acute and chronic healthcare. First-response operations will include fire, police and paramedic services (micro level); each will subsequently have their own subpurpose and associated functions – that is, police will focus on law enforcement and crime, fire on rescue and fire suppression and paramedics on emergency medicine. A healthcare network may consist of a regional hospital

<table>
<thead>
<tr>
<th>Unified purpose</th>
<th>Coordinated purpose</th>
<th>Connected purpose</th>
<th>Engaged purpose</th>
<th>Reliable purpose</th>
<th>Resourceful purpose</th>
<th>Agile purpose</th>
<th>Autonomous purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified</td>
<td>Collect</td>
<td>Collective</td>
<td>leadership</td>
<td>and</td>
<td>governance</td>
<td>Effective</td>
<td>leadership</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Figure 11. Resilience gaps against network profile for resilience gap analysis**

**Figure 12. Risk profile against resilience profile**

---

*Image and text content from the provided document.*
operation. Beyond specific functions to each operation, there will also be functions that are replicated or shared throughout the network. For example, many will possess a rapid-response function with mandated response period, guidelines, compliance measures and interoperability requirements. All first-response network operations will have a house call function and externally share a dispatch function. The paramedics and the regional hospital will possess a critical care function.

When dependencies are evaluated and the incident response sequence is generated, the role that infrastructure plays in enabling the operation is identified. And many aspects of the local infrastructure will provide the critical functions and dependencies required to enable the emergency services network. Aligned with the fire service example, the first-response network will rely on the same built, natural and virtual infrastructure. Although the specifics of how the infrastructure enables each operation may differ, criticality remains the same. The same applies for the healthcare network; specifically a regional hospital will rely on a facility capable of housing patients up to a specific surge capacity and depend on enabling resources including heat, water, power, security, ingress and egress routes and internal and external communication systems. Beyond infrastructure, dependencies for each operation will be consistent with fire services, including well-trained and available personnel, equipment and vehicles, a shared incident response system for emergency command and control and facilities and provisions for housing the injured population. Each of these dependencies is considered essential and critical for the purpose of this discussion.

For the purposes of this discussion, the shared functions and enabling components that are essential and critical for the network to achieve its purpose are focused on. It is assumed that the first-response network and the regional hospital are essential operations; the essential functions are rapid response and critical care; the critical functions are 911 dispatch, the telecommunication network, the transportation network and public utilities (water and power supply); and essential and critical dependencies include personnel, vehicles, fuel supply, communication devices – for example, smartphones – roads and public utilities (water, power).

Step 2: operational system analysis, network, risk and resilience profile development

The second step builds substantially on the OR framework. The first stage mirrors OR, where the operating context, operating environment and all-hazards context (the operational system) are assessed and contrasted with the operating requirement. Specific to NOR, any network or external tableau here that may need to be imported into the operation are isolated and analysed. The risk profile is also started, where any expected risks, either inherent or potential external risks (all-hazard), are added. Second, the network profile is developed to capture the structural, dynamic and system-level dynamics of the network and identify external network risk (network all-hazard). The same strategies for identification of external operational risks are used, and additional risks are added to the risk profile. The inherent network risk and resilience of the network are identified, which completes the expected risk portion of the risk profile and begins the resilience profile. Unlike other stages of this framework, the network is conceptualised once and reused for comparison to any operations within the network being assessed (Figure 13). Unexpected risks are assessed during this stage by using the resilience gap identification and analysis process. Resilience gaps are assessed by contrasting resilience capabilities with the macro, meso and micro levels and analysed by comparison with the network profile. At the end of this stage, a network profile, risk profile of potential expected and unexpected risks and the first stage of the resilience profile (inherent network resilience) is created.

APPLICATION

Beyond the operational system identified for fire service, the operational context may include legal representatives and support networks, secure facilities for confidential operations and criminal storage, municipal security and surveillance systems and channels for secure communication (for police operations), public health programs and medical equipment and pharmaceutical distribution and storage systems (for paramedic and healthcare operations). Their network operating environment will be impacted by a wider array of by-laws, regulations and laws applying to individual and overlapping operations. Distinct from fire service, the network includes operations as subnetworks with specific functions that are mutually dependent on one another. Fire service depends on police services and vice versa. Similarly, police rely on paramedics, paramedics rely on a regional hospital and so on. Thus, an inherent interoperability risk is faced. In addition, each of these interdependent operations relies on the same infrastructure to enable them. This combined demand creates the inherent risk that operations may exceed the carrying capacity of their enabling systems. In contrast, an external tableau may be identified from the local government that outlines compliance requirements for citizen rights, which all emergency service operations must import and enable. Importing this tableau is a resilience development measure in itself, as it ensures that all operations minimise liability by following specific protocols. Finally, all-hazard risks will be congruent with fire service, with a larger geographical radius. Analysis of the network profile may reveal that the emergency service network follows a scale-free topology, rendering it resilient to random attacks or failures around the city, but vulnerable to targeted or centralised ones. The majority of first-responder sites may be clustered in densely populated areas throughout the city, but the regional hospital may be located on the outskirts of the city, rendering inherent risk of timely access to hospital services. The hospital may also be located along a fault line, increasing the vulnerability to earthquakes. Yet the hospital and the city itself are surrounded by farmer’s fields, rendering them inherently resilient to forest fires. Access routes in urban centres may be restricted due to pedestrian and one-way streets, challenging response times, yet in surrounding areas roadways are more diverse, thus building inherent resilience. Access routes to
specific pockets of the community may fall outside of the jurisdiction of different stations and leave the proportions of the community hard to reach within mandated response times. Connections are strong within functional groupings (fire, police, paramedics) but weak between them, creating vulnerability in the interoperability between departments but building strength within each function. Older fire and police stations on the outer proximity of the network have stronger ties with the community due to regular awareness-raising and outreach work, creating a culture of trust and collaboration with the community. The hospital may be located close to the major pipelines supplying oil to the city centre, which, being close to fault lines, may increase inherent risk to the hospital in case of damage or rupture to the pipelines. The all-hazard context may reveal the added risk of epidemic given the close proximity of how personnel must work with the sick and with one another.

The resilience gap analysis (Figure 10) used to identify unexpected risks may reveal that there is a lack of coordination at the macro level (which aligns with the observation in the network profile that there are weak ties between functional groupings). At the meso level, a lack of faith in leadership may be seen, as well as high logistical burden on first-response operations and enabling infrastructure in the downtown core. At the micro level, the regional hospital may lack connectivity with the larger network and related hospitals, limiting collaboration and resource-sharing across operations (also observed in the network profile). Each of these gaps reveals weakness in the overall resilience of the system. To understand lack of coordination further, analysis between resilience characteristics reveals that this may be due to a lack of faith in leadership at the meso/cluster levels. Comparison with the network profile (Figure 11) may also show that this gap may be related to the scale-free, uneven distribution of services across the city. Or the limited access routes within the downtown core may imply that each first-response function cannot arrive within the same timeframe, thus creating challenges for collaboration.

In summary, for expected risks, network vulnerability is linked to interoperability, centralised attack/system failure, meeting mandated response times and epidemics. The first-response network is vulnerable to system overload, infrastructure limitations (e.g. congested road networks) and inability to service full jurisdictions. And the hospital is vulnerable to earthquake and pipeline rupture. Unexpected risks – that is, gaps in resilience –
include a lack of coordination at the network level, low faith in leadership across all meso operations and high logistic burden for first-response network and, at the micro level, the regional hospital is weakly tied to the first-response network given path distance and strength of relationship.

In terms of resilience, the overall network is resilient to random attacks/failure and forest fires and gains resilience through the imported tableau, ensuring service compliance. First-response services in the urban core have strong internal relationships, and outside the city, they are resilient in terms of access channels and ties with the community. The hospital is resilient in its ability for islanding in the case of central failure.

**Step 3: situate operation and risk and option analysis**

Building on OR, this step begins with situating the meso and micro operations within the network to gather a more accurate assessment of inherent risk and control framework and analyse external risk (all-hazard analysis). This is done by contrasting the three profiles (network, risk and resilience) with the original operating requirement. Network analysis, for example, may suggest that shifting a dependency from a single node to distributing it across a capability cluster is more viable. Or parallel operations may be identified in geographically distinct contexts that may benefit from co-creating a portion of the tableau (described in step 4). Some nodes may experience more or less risk than anticipated when contrasted with the inherent risk of what/who they are connected to. The thresholds and tolerances in the incident sequence may change, as tightness of relationships, contextual constraints, size of the network and the cyber against physical distribution influence the speed of cascading failure. Risk at the micro level of the system may reduce when situated within a macro system that is inherently very resilient. Once the perception of inherent risk and control cost of risk is updated, analysis and prioritisation of all-hazard risk are begun.

Once network operations are situated, a bird's-eye view of the network (the macro level) will reveal pockets of risk and pockets of resilience across the network. As described earlier, the network is assessed through clusters and/or operations that may be functionally or contextually similar, and risk treatment and resilience-building strategies that can be applied across operations are identified and implemented, facilitating faster and more holistic resilience development.

Much like when an operation is situated, risk treatment and resilience development must be situated within the network. Option analysis is used to identify treatment strategies for expected and unexpected risks across the network. Treatment can be situated by co-identifying strategies between related operations and functions, or sharing and recommending treatment options. For any strategy to be viable, the whole cost of risk must fall below the control cost of risk. As the aim is to define and project a tableau including risk and resilience measures, it must be ensured that strategies are financially feasible across parallel operations. Adaptive resilience I is developed for expected risks, using complementary processes from emergency management, business continuity, critical infrastructure protection and so on. Adaptive resilience II is developed for unexpected risks, using the vulnerabilities and insight gathered during the resilience gap identification and analysis. For example, resilience capacity may be built in higher operational functions – for example, through relationship-building tactics (discussed earlier) or training exercises.

**APPLICATION**

By contrasting the operational system with the three profiles, first, the specific demands on local infrastructure are identified more clearly, as well as the scale of demand. For example, specific road routes that might be more used than others may be foreseen. The geographical proximity of response sites in the core of the city shows where increased demand on public utilities and fuel stations for vehicles may be experienced. Second, the regional hospital in situ reveals that it is less resilient than anticipated. It may have lowered risk of service interruption failure, as it is on a different power grid and removed from portions of the city likely to experience overload. Yet it is more vulnerable in terms of its ability to interface with the majority of the first-response network in a timely fashion, as well as its proximity to a major pipeline and a major fault line. The overall resilience of the network may lower, in this case, based on the premise that nodes can be only as resilient as what they are connected to. The first-response network may become less resilient because one of its critical dependencies, the hospital, is more vulnerable. Third, it is identified that certain sections of the city are outside the coverage area of the combined response sites. The inability to access these areas creates added vulnerability to the first-response network to not being able to fulfil its central mandate to the sites linked to the communities with these service gaps.

The risk profile is analysed for risks that are most likely to harm the operation. Inherent risks can be further prioritised by looking at recurring themes in the network profile and gap analysis. Reinforced risk linked to interoperability, infrastructural limitations (road and traffic networks) and public utility overload and/or failure is observed. Each risk contributes to the larger risk of inability to deliver within mandated response times. The all-hazard analysis for the larger network might also reveal that active shooters are of higher priority to the network, given the inclusion of police services.

Some examples of strategies to mitigate risks and build resilience in shared operations and functions are as follows. First-response networks can mitigate infrastructural limitation risk, specifically densely trafficked road networks, by working the traffic management system to revise emergency travel routes to enable emergency vehicles to pass through easier. They could minimise the risk of overloading public utilities by developing resource-sharing agreements, uptake of more green technologies or resituating stations across the city to follow a random instead of scale-free structure. Interoperability can be improved by...
increasing exercising and simulations between functional groups and training and embedding hybrid responders — for example, firefighters with paramedic certification — to build diversity in internal capacity as well as facilitate the bridge between communities. The regional hospital may address earthquake risk by reinforcing the facility to withstand higher-magnitude impacts or, at a minimum, protect the most essential sections of the facility to ensure ongoing function. They may address the risk of gas line rupture by working in tandem with the oil supplier to install sensors for early detection of seepage and enforce more frequent inspections and a shorter replacement cycle of pipelines near the hospital. For the broader development of resilience, first responders could develop resource-sharing capacity across the network by outlining guidelines for infrastructure usage as well as co-acquisition of backup systems and emergency supplies to share during a crisis. For areas that are hard to reach, outside of coverage or high above the coverage area (vertical communities), implementing community-building strategies will help build resilience capability into communities, specifically enabling them to be autonomous, collaborative, emergent and innovative.

Step 4: define, refine and project the tableau
After addressing the various pockets of risk throughout the network, for either individual operations (the hospital) or shared ones (first-responder network), resilience is further developed as a whole by filling the gaps between these pockets. This is done through the tableau. As discussed in the previous section, here aspects of the operational requirement will be segmented into those that are customised to the network/organisation, customised to the context and customised to operations (independent of the context). This will segment functions and dependencies specific to what can or cannot be projected and to where.

APPLICATION
Building resilience in the broader network is begun through the shared rapid-response operation. Drawing from the fire service discussed earlier, their rapid-response operation may be used as a foundation to define the tableau for projection to other emergency services. Fire service is selected in this case as they may exhibit the fastest service delivery, a low failure rate (well-managed risk) and resilience characteristics.

The existing rapid-response tableau for fire service may consist of four segments of capability. The first may identify the requirements customised to fire service — that is, rapid-response dependencies specific to the delivery of fire-related services. The second may be customised to the operating environment and context of a specific fire hall. The third is imported from the local municipality, outlining compliance requirements. And, finally, the fourth may describe elements of rapid response that apply to any emergency service provider. It will also include risk treatment and resilience strategies specific to the risk profile for that operation and service provider. As an example, it may address logistic burden by mandating capability for the green technology treatment option identified earlier. The fourth segment can be projected as a tableau to other emergency services. It would outline the core capability — for example, an operation must arrive to the site and provide emergency response service within a set time frame — their core capacity — for example, the minimum resource requirements and response protocols — and risk mitigation and resilience practices. Risk requirements may include the capability to follow specific emergency routes and perform ongoing community outreach. Once it is projected, the tableau is imported by other operations with a similar function. Whether police, paramedic or another service, they all must provide a rapid-response capability. Importing the tableau, they will enable the operation meeting the same capability, capacity and, most importantly, risk and resilience requirements. This translates into a performance and capability specification for infrastructure systems and specifically the design brief and operational requirement for built infrastructure.

As this process is applied to other individual and shared operations and functions, a shared tableau may be developed for essential and critical functions (critical care, dispatch) as well as within functional groupings (within fire, paramedics, police) instead of between. The more tableaux that are created, projected and imported, embedding treatment strategies for the expected and unexpected risks across all system level dimensions of the network will increasingly lower the overall network vulnerability and build resilience.

Figure 14 outlines the detailed NOR process.

Figure 13 outlines how the network profile is applied to multiple instances of NOR.

Future research
Further research is required to test the application of this framework. Specifically, the authors are currently applying the NOR framework to post-conflict rehabilitation of the whole of community infrastructure networks. There is a need to understand the social dynamic in the tableaux — that is, the perception, influence and judgement associated with community ownership of the systems reconstruction — in place of ‘aid’ solutions. In addition, further study is needed on the application of NOR to virtual networks. Building on previous works (Phillips, 2015; Robinson et al., 2016) on digital response networks (digital activist and digital humanitarian networks), the NOR framework offers vast potential for this context. It can assist governments and crisis response organisations to grassroots/community-based organisations and community networks operating online, to manage better the risk that they face due to what they do and how and where they operate.

Conclusions
In the preceding discussion, a framework is provided for academics and practitioners to explore and develop resilience in networked operations, the NOR framework. This framework consists of using the OR framework as a foundation, building on the tableau concept and adding a network analysis component to situate better the operation and subsequently the tableau. The tableau is described as being fundamental to capturing and spreading risk treatment and
resilience strategies across a network, and it is explained along a continuum of resilience development. An effective tableau is developed by situating an operation within the network, to understand the operation in isolation as well as from the perspective of the larger network operation. This approach is applicable to any form of complex network, whether transportation, communications, knowledge exchange, crisis response, advocacy, multinational or multistakeholder networks; the list goes on. Understanding these network resilience demands allows defining more efficiently infrastructure system planning and design requirements, as well as better defining what they can support.

As operations become increasingly networked, it must be ensured that a holistic approach to understanding the operation, effectively diagnosing and treating risk and building resilience customised to the needs of each network is adopted. As described by Dalziell and McManus (2004: p. 4), in systems ‘the whole is greater than the sum of its parts …’ and ‘… the emergent properties of a system cannot be understood by analysing the components of the system in isolation’. Through having a clear idea of the operation and its networked surroundings, what can or cannot be expected and to what must resilience be developed can be better articulated. Through frameworks like that described earlier, moving towards building resilience in increasingly complex and uncertain times can be done.

REFERENCES


How can you contribute?

To discuss this paper, please email up to 500 words to the editor at journals@ice.org.uk. Your contribution will be forwarded to the author(s) for a reply and, if considered appropriate by the editorial board, it will be published as a discussion in a future issue of the journal.