Building resilience in virtual digital response networks: a case study

Jennie Phillips MA
PhD Candidate, University of Toronto, Toronto, ON, Canada
(corresponding author: jennie.phillips@mail.utoronto.ca)
(Orcid:0000-0002-4924-4394)

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

The evolution of technology is creating a more complex, connected society of interdependent networks and processes. As connectivity increases, so does the concentration of value. This increases the consequence of failure and the scale, scope and complexity of potential risks causing these systems to fail. These systems are made resilient by making the physical and virtual networks resilient in isolation and intersection. Yet existing resilience practices fail to address the complexities of virtual networks and their dynamics with the physical environment, specifically the requirements of physical infrastructure networks to enable resilient virtual networks and vice versa. This paper aims to address this gap through a simulated case study of resilience development within and between a physical network and a virtual online network. The networked operational resilience framework is applied to an emergency services network partnered with a digital response network (DRN). DRNs are virtual networks of crowdsourced volunteers that respond to the virtual layer of crisis. Building situational awareness to aid decision-making, they have become an essential tool of crisis response. Findings address the context of virtual online networks in isolation and partnership, enabling infrastructure requirements, the risk environment and resilience capability and development.

Introduction

All infrastructure is defined by the purpose it serves, whether to support a particular operation or enable a capability. Consequently, the infrastructure is bound within systems and networks that include both the enabled operation and the neighboring operations and infrastructure systems. The ability to plan infrastructure development amid such complexity will depend on what is required of it in the future and a changing risk context. Tableaux projection is a tool that allows an infrastructure planner to project the operation-enabling requirements to a new context, spatially and temporally. However, with the rapid evolution of virtual networks, it has become less clear what those future enabling requirements might be. Nonetheless, recognizing what is required of infrastructure over its life is essential to the design of efficient structures and systems. As physical infrastructure enables virtual infrastructure, it is necessary to understand what is needed to enable resilient virtual networks and so define physical infrastructure in terms of performance and capability parameters. At no time is this more challenging than in evaluating what is required of infrastructure during a crisis. Incident sequencing (Hay, 2016) provides a way of relating physical infrastructure requirements to business performance through an incident, but it does not fully address the complexities of the virtual domain that similarly influences requirements on physical infrastructure.
The discussion introduces the concept of networked resilience and explains the theory of NOR as distinct from OR. Virtual networks are described, followed by introduction to DRNs and their applicability to ESNs and links with resilience. The four-step NOR framework is then applied to the DRN concept as a case study demonstrating how resilience can be developed in the virtual infrastructure connecting and enabling a virtual resource (the DRN). Discussion is provided regarding study findings, and the paper concludes with a summary of the study and suggestions for future research.

**Networked resilience**

Resilience, as applied to networks, involves understanding the nature of what must be made resilient (the basics of networks) and what resilience implies (the resilience capability). Whether virtual or physical, simple or complex, networks are a collection of nodes and links. Drawing from key literature on networks (Barabási and Bonabeau, 2003; Easley and Kleinberg, 2010; Erdős and Rényi, 1959; Watts and Strogatz, 1998), they can be characterised along three dimensions, including (a) structural (e.g. network topology and distribution), (b) dynamic (e.g. evolution, exchange and culture) and (c) system-level (macro, meso and micro) (Phillips and Hay, 2017). Resilience in complex networks applies to static (physical systems) and dynamic elements (human systems). It is the ability to absorb impact while also learning, adapting and bouncing forward. It is ‘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). Literature on resilience including publications by McManus et al. (2009), Walker et al. (2002), Rose (2004), Zolli and Healy (2012), Seville et al. (2015), Abraham et al. (2013), Bronfenbrenner (1994) and Holling (1973) suggests that a network is capable of resilience when it is unified, coordinated, connected, engaged, reliable, resourceful, agile and autonomous (Phillips and Hay, 2017). This capability is developed by assessing what already exists (inherent resilience), what must be developed (adaptive resilience) (Rose, 2004) and the integrating measures. This can be achieved through the NOR framework.

**Networked operational resilience**

NOR is achieved using the tableau concept to capture, project and amplify resilience in a network (Phillips and Hay, 2017). The tableau is the discrete definition of an operation or function independent of context, such as a shared communication function in an ESN. It outlines what the operation must do and what it depends on to achieve its purpose, as well as the associated risk, risk treatment and resilience development strategies. A communication function will depend on communication protocols, hardware, social network and physical communication network. Risk may be the loss of connectivity through physical failure of the communication network or loss of power or virtual failure of relationships between network stakeholders. Treatments such as
alternate communication channels, diversified power supports and ongoing tabletop exercises between responders to strengthen relationships will ultimately make this operation more resilient. Together these requirements form the tableau. The transition from a resilient operation to a resilient network is through the concept of tableau projection. Once the tableau is defined, it is projected to parallel/shared operations and systems. Those with the capacity to meet the operational requirements outlined in the tableau import and enable it as a subfunction within their own larger operation. The parent operation assimilates the inherent resilience embedded into that tableau, thus building the inherent resilience of their own operation. Health support within an ESN may be delivered through paramedic and hospital services in partnership with an informal community-led first-aid network. By importing the communication tableau shared between paramedic and hospital services, the community network becomes more resilient through enhanced interoperability and the inherent resilience embedded in that tableau. As these operations, and others, import, develop and project their own ‘resilient tableau’ to other operations, the amplification of resilient tableaux continues to a point where a critical mass of resilient nodes (operations) is achieved, thereby making the network resilient (Figure 2).

To ensure that the tableau is captured properly and that it effectively builds resilience in the broader network, operations must be situated in the network prior to projection. This ensures that requirements are generalisable to other operations in different contexts but within the same network system. The operation is initially situated by identifying any pre-existing imported external tableau (from the operational context and environment) as the operation is defined like the shared communication function described earlier. The operation is further situated through development of a network profile, a risk profile and a resilience profile. The network profile relates the operation to the bigger picture (Bronfenbrenner, 1977) to gather better understanding of the operational requirement. The community first-aid network, for example, may rely on a local car share company for service delivery, follow a low-carbon dioxide emission policy and use only green energies for their operations while ensuring compliance with first-aid certification. Each will have associated physical and virtual dependencies and influences on how the operation is defined. The risk profile captures expected (inherent and applied) and unexpected risk for the operation and broader network. Dependency on compliance may be higher than the local power grid; thus, inherent risk may lie in the resourcing and leadership of the network. The resilience profile consists of three levels of resilience based on the publications of Home and Orr (1998), Mallak (1998) and Rose (2004), including inherent, adaptive-operational and adaptive-networked resilience (Phillips and Hay, 2017). The emergent, voluntary nature of the community network enables cultural capacities such as social capital, building inherent resilience while also exposing the need for resilience development between the informal and formalised networks to ensure sustainability of membership. Once the tableau is projected, intelligent resourcing is fundamental to ensure that dependency relationships are tuned to local resource availabilities. This does not change the nature of the dependency, just how it is represented. Without intelligent resourcing, projection is unworkable in anything but the same organisation/environment/culture.

Virtual networks

Virtual networks depict the conceptual layer of the operation. Considering examples such as the community first-aid network to the Internet, economy or social networks in general, they consist of physical nodes (human and organisational and infrastructure) much like physical networks. Yet they are distinct in that...
relationships are metaphysical. Virtual networks provide the structure and culture of an organisation and the connection and collaboration extending past physical boundaries. Relationships can exist for the exchange of information, currency or knowledge; for social connection; or as a product of affiliation with a shared culture or purpose. This intangibility enables operations to occur online, offline or between the two. Yet virtual networks cannot exist without the enabling physical infrastructure. From built telecommunication systems and power grids to natural systems enabling human congregation, the virtual infrastructure is a product of complex relationships and dependencies with the physical system. Linked with these complexities are a new subset of risks and resilience needs, specific to the virtual context as well as the influences that it has on the physical one.

Virtual is not to be confused with the cyber dimension. Cyber is part of the built domain. It has substance – it physically transfers data. It requires both the virtual domain and the physical interface with the built domain. Together, the balance between natural, built, virtual and human domains define civilisation in a vitae system of systems and when in synergy represent resilience.

The study of virtual networks in the context of applying NOR offers specific benefits. First, application addresses the pressing need to fully understand risk and build resilience in virtual environments. The growth of information and communication technology (ICT) through smart cities to the Internet of things is rendering virtual networks more prevalent and increasingly complex. Yet innovation is moving faster than it can be understood, and therefore the capture and mitigation of associated risks lag behind. Furthermore, these advances are changing the way society functions. The value of operations is becoming more concentrated, and so the exposure to and consequence of loss is exceeding the value of the enabling infrastructure. Second, the interconnectedness between physical and virtual systems implies that risk is not restricted just to the virtual environment. Applying NOR to a virtual network will lend important insights into risk and resilience of physical systems.

**DRNs**

Extending previous research (Phillips, 2015, 2016; Phillips and Verity, 2016), DRNs were selected as the virtual network (unit of analysis) case study for this paper. Similar to the community first-aid network described earlier, DRNs are citizen-driven volunteer networks that emerge and/or activate to provide support during crisis (Figure 3). They provide service to communities and responders directly. The primary distinction is that virtual relationships and operations are online. In terms of composition, they are ad hoc assemblies of individuals and organisations physically distributed but virtually connected under a common cause. At the high level, their cause is to assist, mostly remotely, affected communities (local and remote diaspora) through response...
capabilities enabled by technology. They do so in three ways: 

(a) provide direct support to affected communities, 
(b) provide indirect support through collaboration with response agencies (e.g. humanitarian response agencies (HROs) and first responders) and 
(c) advocate support from the broader response community. At a low level, this may imply managing the information overload in a disaster context as a digital humanitarian or advocating human rights violations in a complex crisis as a digital activist.

A DRN serves as a critical case for study, offering rich and unique insight on the opportunities, challenges and complexities associated with virtual networks that function solely online. Membership is voluntary, demanding a strong sense of purpose. The scope of members is vast, ranging from software developers to emergency managers, and the scale of operation is global. They can provide capabilities on a 24/7 turnaround through an uninterrupted global workforce even in the face of localised disruption. Their ability to provide situational awareness and aid decision-making in a timely and accurate fashion is unprecedented. These networks are emergent and fluid. Most collapse after the peak of crisis and few are sustained. Relationships are often formed online and remain online. Leadership and decision-making are collaborative. The operational environment is a virtual one composed of online tools designed to mimic offline interaction. They are also uniquely vulnerable. The contexts in which they operate and the nature of their work place them at high risk, and the volunteer, fluid nature of the network makes it difficult to invest in measures to mitigate these risks (Phillips, 2015).

Beyond the value of the DRN as a virtual network case study, DRNs provide important insight on resilience development and transference in complex networks.

**Resilience transference in complex networks**

The integration of a DRN into an ESN demonstrates how a virtual online network can build the inherent resilience of a virtual offline and a physical network. Figure 4 depicts the DRN relationship with an ESN. Much like risk can be transferred to other portions of a network, resilience can also be transferred and shared across operations. In a crisis situation, the delivery of timely, accurate and concise information is critical to both decision makers and the communities affected. ‘People need information as much as water, food, medicine or shelter’, the International Federation of Red Cross and Red Crescent Societies (IFRC, 2005: p. 12) reports, ‘… information can save lives, livelihoods, and resources. Information bestows power’. There is a vast amount of information generated and shared prior to, during and post crisis situations. For example, 16 000 tweets were shared per minute during Hurricane Sandy (Meier, 2015). Yet in many cases, timely and actionable information fails to reach the affected populations in need. Similarly, those with the mandate to disseminate information also face information hurdles. Either they lack the capacity to manage it (Lovrics and Verity, 2014), or they do not receive it at all (Wall, 2012). Conversely, DRNs possess the capacity and capability to address these big (crisis) data challenges (Meier, 2015) among others. They do so by leveraging digital volunteer networks, often crowdsourced, to provide ICT-enabled capabilities such as crisis mapping, translation and the filtering, analysis and visualisation of data.

DRNs can directly support ESNs in many ways. Through the geolocation of event-based/citizen-generated social media data and map generation, they can assist emergency managers with faster decision-making by alerting to areas most affected and/or vulnerable. They can inform first responders on the best ingress.
and egress routes by identifying road obstructions and infrastructure damage and assist public works by highlighting regions prone to fail. They may deconstruct, verify and relay calls for help reported online to local dispatch (Canadian Red Cross, 2012) or provide situation reports to the local hospital on the nature of outbreaks around a city or the breadth of civil society involvement in the provision of localised healthcare. DRNs have become an essential tool of crisis response and increasingly planned for in urban design and regional development.

Beyond the increased capacity and capability gained through the DRN–ESN partnership, leveraging a resource that is online, remote and digitally capable enables the ESN to assimilate inherent resilience. Embedding a resource that operates strictly online enables better accommodation of the digital challenges that arise due to existing and future behaviours and expectations associated with technology. They can supplement a capacity that is currently lacking or underresourced—for example, the capacity to manage the information overload described previously. Second, depending on resources that are distributed and remote from the disaster yields the benefit of distributed physical dependency on physical infrastructure. Although one part of the network may be located in a region that has lost power, the larger network can still continue to function. Third, leveraging remote resources also distributes virtual dependency—that is, the reallocation of demand to remote resources lifts the burden on the local ones in the affected area. By offsetting human resource demands for select response activities away from a disaster area, local resources are freed to allocate to more local-specific response needs. The detail of how this resilience is developed is demonstrated in the application of NOR later in this paper.

To realise these resilience benefits, however, the dependency and connectivity to this resource must be resilient. More specifically, the virtual infrastructure that enables this partnership, as well as the resource itself, must be resilient. A resilient DRN, for example, will be able to absorb small events and adapt and bounce forward from the big ones. Yet literature on developing resilience in complex networks remains nascent. Current approaches develop resilience within each component system instead of across these systems. Failure to account for these intersections implies that the inherent resilience associated with connectivity is lost. Serious gaps in the resilience of the overall system also result. NOR can address this gap through the application of the NOR framework (Phillips and Hay, 2017). NOR examines networks for what they must do and what they rely on against individual parts of the system.

**Methodology**

This paper explores resilience development through application of the NOR framework to a simulated DRN supporting an ESN. This scenario was developed using not only past case studies of different DRNs (digital advocacy, cyber response and digital humanitarian), but also, most significantly, the Digital Humanitarian Network (DHNetwork) as the unit of analysis explained later (Figure 5). The qualitative case study approach was used to generate understanding and assist with developing the theory on the context of DRNs (Yin, 2009).

**The case study**

The DHNetwork is a network of networks that acts as focal-point and matchmaking service between humanitarian response organisations (HROs) in need of support and technologists and technology-based organisations capable of providing that support. It does so by forming and sustaining the DHNetwork, a consortium of member organisations able to provide technical surge capacity, local and remotely, during crisis response. Services include creating maps (geographic information system (GIS), crisis maps); filtering, analysing and visualising data; coding/hacking; emergency telecommunications; and translation. In terms of structure, the hub of the network (DHNetwork) consists of three to four coordinators, rotating annually, and member organisation representatives (hub members). Leadership and decision-making are horizontal, membership is open and voluntary and decision-making is transparent and collaborative. In the event of a crisis, HROs ‘activate’ the DHNetwork by submitting a support request to the network. The request is approved by DHNetwork coordinators, and decision-making and delegation to a DHNetwork member organisation occur between all hub members. At this stage, an activation lead is identified from the delegated organisation, and the DHNetwork connects the HRO with the activation lead. The DHNetwork-activated organisation then operates under the guidance of the HRO to fulfil requests.

**Research method**

The simulated DRN case study is built on case study data from previous studies (Phillips, 2015, 2016, 2018). The term ‘DRN’ is used to refer to the network hub connected to a larger network of digital responders (DRN subnetworks or members). The study of resilience development in the DRN and broader ESN is completed through application of the four-step NOR process (Figure 1) to
this case study. Each step is explained through description of the step and application to the case. Within this process, operational, contextual and risk analysis is completed, while risk treatment and resilience treatment strategies will be identified. Risk modelling and analysis is completed using the RiskOutlook software. This software is used to build a control framework, analyse dependencies and identify a pathway of exposure to risk (O’Neill, 2013). Entities are ranked in terms of likelihood and failure, and relationships are mapped between entities by ranking all direct dependencies (see Table 1).

Using mapped dependencies, relationships are analysed by looking at cumulative impact against cumulative failure and group against risk index and plotting the top 15 risk indices (O’Neill, 2013). Risk scenarios are used to characterise failure and identify most critical risks to treat. Key findings are presented throughout the following section.

Application of NOR

Step 1: mission and operation definition

Description

NOR begins with isolating what an operation seeks to achieve, what it must do and what it depends on to do so. This process starts with defining the operation. Boundaries (active or passive) and a common purpose are established, as well as the associated operations and functions to achieve that purpose. Dependencies are identified that enable these processes from three component groups: human, organisational and infrastructural (natural, built and virtual). The recovery sequence for an operation is then identified through the incident response sequence (Hay, 2016). Functions and dependencies are categorised for when they must be recovered as essential/critical (reaction period, \(t_0\) to \(t_1\)), sustaining (response period, \(t_1\) to \(t_2\)) and routine (recovery, \(t_2\) to \(t_3\)).

Application

The DRN aims to achieve the shared purpose of the ESN, ‘… to provide communities with protection and support from harm in an emergency’ (Phillips and Hay, 2017: p. 60), rendering it as a subfunction of the larger network. The individual purpose of the DRN is to leverage digital networks to assist emergency responders. It achieves this purpose by acting as a network hub between the broader ESN and DRN subnetworks bound through two key functions. First, the DRN provides service delivery (matchmaking), connecting ESN requests to DRN member organisations with the requested capability. Second, it provides coordination involving network building, sustainability and shared situational awareness.

Dependency and enabling infrastructure requirements vary and overlap with the ESN (see Figure 6 for a snapshot of the DRN operation). Human resource dependencies include hub coordinators, DRN member organisations and supporting volunteer members. Organisational dependencies such as guidance documents, policy and legal supports overlap with ESN functions. Yet the dependency on resources such as mobile devices and/or computer hardware may be higher given the criticality of connectivity for virtual online collaboration. The enabling infrastructure includes both physical and virtual components. Physical infrastructure includes power, telecommunications and the Internet. Virtual infrastructure is both soft (social) and hard (cyber). The social fabric of the network enables network membership, organisational cohesion and sustainability. Unlike the stringent requirements associated with membership in ESN subnetworks, DRNs adopt an open membership model. Fire services, for example, will require specific health and fitness capabilities, academic credentials and experience for membership (employment). In a DRN, eligibility is based on an organisation’s ability to engage in crisis response, either digital or physical. It must be available, reliable and capable of meeting requests on a volunteer basis. Trust, pre-existing relationships and reputation are used to assess member viability. Decision-making for member acceptance, among other operations, is achieved through collective decision-making between DRN coordinators. Network sustainability relies on cultural attributes including transparent and open communication, trust, collaborative decision-making and the horizontal leadership structure to be sustainable and interoperable. The hard-virtual infrastructure (the online operating environment) includes online tools for communication and collaboration.

Using this understanding, the DRN develops their incident response sequence based on the incident response framework (Figure 7) (Hay, 2016).

Table 1. Risk criteria

<table>
<thead>
<tr>
<th>Criterion</th>
<th>2 (low)</th>
<th>5 (moderate)</th>
<th>8 (high)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale of impact</td>
<td>Capability down by 20%, able to remain within 24 h turnaround</td>
<td>Capability down by 50%, return to functioning within 48 h</td>
<td>Capability down by &gt;50%, undetermined time to recover functioning</td>
</tr>
<tr>
<td>Likelihood/chance of failure</td>
<td>Every 1–2 years</td>
<td>One per year</td>
<td>One to two times per year</td>
</tr>
<tr>
<td>What impact will failure of this entity have on the operational requirement?</td>
<td>Entity will experience low impact without the contingency plan (self-sustaining)</td>
<td>Entity will experience low impact with the contingency plan (need to redistribute/adapt) or medium impact without a contingency plan</td>
<td>Entity will experience high impact, with or without a contingency plan</td>
</tr>
<tr>
<td>Entity will experience low impact without the contingency plan (self-sustaining)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entity will experience low impact with the contingency plan (need to redistribute/adapt) or medium impact without a contingency plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entity will experience high impact, with or without a contingency plan</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 7
A service delivery (matchmaking) time frame $t_2$ is set to 24 h from the receipt of a request, with $t_1$ at 6 h. As depicted in Figure 8, from $t_0$ to $t_1$, the essential functions identified include processing incoming requests and decision-making (for matchmaking), with dependencies including one DRN coordinator, email, online decision-making tools, local by-laws and response mandates, effective leadership and timely communications. Critical dependencies include power, Internet and ICTs (mobile/laptop devices). From $t_1$ to $t_2$, sustainable functions include providing surge capacity, service delivery decision-making and delivery of capability. Dependencies include all DRN hub personnel (remaining DRN coordinators, DRN hub members, DRN activation coordinator and DRN-activated organisation volunteers), a focal point (the website), trust and online tools for network-wide communication, video and text chat. External dependencies include the web host and client requests.

Step 2: operational system and network profile Description
To understand the operation and associated risk better, it is situated in its operational system and network profile. The operational system includes the external social, natural and human-made systems impacting or impacted by the operation, as well as expected...
(inherent, applied) risk. It can be assessed through the operational context (interdependency relationships), operational environment (external influences) and all-hazards context (threat of natural, human-induced and technological harm). The network profile depicts the network context through modelling the structural, dynamic and system-level dimensions of the network. Network-specific inherent risk and resilience are also determined. Finally, unexpected risk is measured through a binary assessment of resilience characteristics.

Figure 7. Incident sequence (Hay, 2016). MOC, minimum operational capacity; MSC, minimum sustainable capacity

Figure 8. Incident response sequence

Essential (by $t_1$ – 6 h)
- Functions
  - Processing incoming requests
  - Decision-making – matchmaking (DRN hub to HROs)
- Dependencies
  - DHN coordinator (1)
  - Email for internal/external communications
  - Online decision-making tools (loomio)
  - International humanitarian law
  - Effective leadership
  - Timely communications

Critical dependencies
- Power
- Internet
- Devices (ICTs) – Mobile phone, laptop, desktop, tablet and so on

Sustaining (by $t_2$ – 24 h)
- Functions
- Process incoming requests
- Provide surge capacity
- Decision-making – service delivery
- Decision-making – general
- Network sustainability
- Provide capability to HROs (DRN to HROs)
- Dependencies (Internal)
- Personnel
- DHN coordinator (others)
- DHN hub members
- DHN-DHN/OCHA activation coordinator
- DHN available volunteers
- Operating environment tools including:
  - Group communications and data storage
  - Video/text chat
  - Secure video/chat
- Focal point
- IHW monitors
- Trust
- Dependencies (external)
- Web host
- Requests from HROs
across all system levels (macro, meso and micro dimensions) – resilience gap identification (a concept introduced by Phillips and Hay (2017)).

Application

OPERATIONAL SYSTEM

The ESN acts as an operating context for the DRN. Yet the dynamics of this relationship is unlike the shared interdependency between first responders. It is a client–supplier relationship where the DRN provides a service to the ESN. There are interdependency requirements, however, to enable this coordination. Emergency support functions may require specific capabilities, a set time commitment, level of reliability, trust and compliance with operating protocols, deliverables and timelines to clients. A DRN must fit into their local emergency response system. In exchange, the DRN needs compliance with collaboration guidelines set forth by the DRN, a formalised relationship detailing roles, responsibilities, communication channels and information sharing and broader integration in operational protocols.

The ESN and DRN also share an operating context. For example, they both share relationships with the local community. The dynamics of this relationship is slightly different for DRNs, however. The local community can act as a direct beneficiary (receive support from DRNs), an indirect beneficiary (receive support from organisations supplemented by the DRN) or a partner (engage as a member or organisation with a DRN providing digital support). Communities will impose time and cultural sensitivities, specific needs, expectations and response measures of their own on DRNs. Contrarily, the DRN may require the local community to be online and communicating in a timely and accurate fashion.

The DRN and ESN also share a similar operating environment with shared functions such as situational awareness, information collection and dissemination. The imported/shared tableaux for these functions may have resilient attributes embedded in them, building the inherent resilience of the DRN and ESN and the connectivity between (discussed later). The overlap in demand implies shared dependency on the broader operating environment. For example, physical infrastructure requirements may include a local telecommunication provider and regional power grid (for ESN and locally situated DRN members). Virtual infrastructure may include close ties with local media organisations for information dissemination and open unobstructed Internet for online information sharing nationwide. Operationally speaking, both parties must abide by the same by-laws, state and federal laws and ethics guidelines while fitting into established response systems in larger-scale disasters such as ‘the Cluster System’ (Ocha, 2016). They are also influenced by local authorities and broader political powers. DRNs may pay specific attention to local laws and regulations influencing drone usage (often used in DRN activities). State surveillance and information controls prescribe the level of digital and physical security required and the space for online collaboration. Cultural factors such as freedom of expression dictate the transparency of information sharing. Physical infrastructure condition will determine the dependability of online connectivity and the capacity it can provide for virtual operations.

The DRN context distinctly includes a relationship with the digital response community as a key interdependency. The digital response community and DRN may share compliance requirements regarding the open exchange of data (open data standards), minimum technology and connectivity requirements and leadership rules. They must also mutually adhere to a code of conduct and share situational awareness including the serviceability/condition of physical infrastructure networks.

The relational dynamics between DRNs and broader DRN members uniquely impacts how much they are dependent on and influenced by the local context and environment. Specifically, the more DRNs engage remote DRN members, the more dependency on physical infrastructure shifts beyond the boundaries of the affected region. This implies that the loss of power or connectivity in a major area of a city may hinder the interoperability of that portion of the DRN but not disable broader DRN operations. The broader the remote distribution, the lower the dependency on local resources. Conversely, as the geographic distribution of membership broadens, the portfolio of environmental influences – for example, legal, social and cultural norms – and regulations also expands. Compliance becomes more complex, exposing opportunities to bypass restrictions in some portions of the network while repressing operations in other portions of the network.

NETWORK PROFILE

The structural and dynamic attributes of the DRN and DRN–ESN relationship overlap and vary across virtual and physical domains. Like the ESN, the DRN has a scale-free topology in both domains, making it resilient to random attacks but vulnerable to targeted ones (Medina and Hepner, 2008).

The physical domain of the DRN may see a concentrated distribution of members in the densely populated area of the city affected by a crisis, including most network hub members, with a large contingent spread across the region, the country and around the world. Physical infrastructure demands correlate with this distribution. As earlier, although the centralised placement of many nodes may render a physical network vulnerable, geographic dispersion builds inherent resilience of network connectivity. In the event that one part of the network goes down, another part of the network remains uninterrupted, thus allowing the network to continue to function. When ESNs partner with DRNs, they build their inherent resilience by assimilating the reliability of this resource.

The virtual domain of the DRN follows a hub-and-spoke structure (see Figure 3). This reflects that members have stronger relationships with the hub than with one another, implying the
lack of interoperability between them. These weak ties between members render inherent vulnerability to network sustainability as well as increased dependency on the hub, yet inherent resilience of the networks’ ability to grow and adapt and thus build a more diverse network (Granovetter, 1973). This plurality builds the inherent resilience of a DRN in its capacity to problem-solve, learn and adapt and, subsequently, the inherent resilience of partnering ESNs. It enhances their ability to supplement any lack of technical skills and knowledge while lifting the burden on local resources to manage and capitalise on the digital aspect of disaster response. In the event this first-response network is in the developing world, however, a resource network situated in the developed world may operate under technical and connectivity capabilities different from those in an area that is underresourced and/or with poor Internet connectivity. Revisiting boundaries, the organisation-based membership approach used by DRNs builds resilience to the fluid participation of volunteers. Some members are also hybrid members – that is, they are affiliated with a DRN and an ESN. These members build resilience in terms of partnership between ‘client’ and ‘supplier’. Looking at the culture and leadership across dimensions shows that the DRN approach follows a collaborative, horizontal leadership model with a strong sense of purpose and space for emergence – embracing many of the characteristics associated with resilience.

Table 2 outlines the full network profile for a DRN.

**RISK PROFILE**

The DRN assesses expected risk further for each network level, identifying overlaps and distinctions with the ESN. As described by Phillips (2015, 2018), DRNs face digital (from cyberattacks to failure of communication infrastructure), natural (flood, earthquakes, hurricanes) and sociopolitical risks (e.g. social unrest, legislative change); legal and financial risk (e.g. fines, lawsuits) at the organisational (hub) level; and psychological (trolling, threats to family) and physical risks (physical attacks to murder) at the individual level. Most of these risks are shared with the ESN, yet some at the organisational and individual level may be felt more acutely in DRNs. For example, DRNs are more likely to face targeted psychological risk such as trolling if their initiative is somewhat political. They carry higher legal and financial risk without the resource backing likened to government bodies or large corporation. At the macro level, a failure of local telecoms companies or power interruption may not be detrimental to network connectivity, but it will have implications on the access and ability to share information with affected communities. Added inherent risk, common to the DRN and ESN, encompasses interpersonal, interoperability, reputation, leadership and psychological risks. Distinct to the DRN, damage to factors including trust, conflict, communications and transparency, external buy-in from clients, relationship strength or increased/unmanaged member fluidity can be detrimental to the existence of a network that is innately ad hoc and loosely connected. In structureless movements, Freeman (1972) warned of the dangers of any secondary leadership structures and power dynamics that emerge undermining the primary purpose of an initiative. The ability, strength and faith in leadership, combined with decision-making capability, can mean thriving or collapsing. Beyond post-traumatic stress risk associated with any crisis response, digital responders run the risk of digital burnout – the result of working conceptually in another place in an unregulated setting. See Table 3 for the full spectrum of DRN risk.

**RESILIENCE PROFILE**

At the last stage, a resilience gap analysis of a DRN isolates pockets of the network that may be at risk. As depicted in

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Network</th>
<th>Network hub</th>
<th>Member organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Scale-free network</td>
<td>Virtual relationships</td>
<td>Mostly human, organisational nodes enabled by infrastructure nodes</td>
</tr>
<tr>
<td>Boundaries</td>
<td>Local crisis responders engaged in digital response, open membership</td>
<td>Representatives from member organisations, restricted membership</td>
<td>Membership requirements – for example, must be able to provide service and follow ethics and mission</td>
</tr>
<tr>
<td>Scale</td>
<td>Spans local region, size varies</td>
<td>Spans local region; small, one or two more people</td>
<td>Spans local region, varies with popularity and affiliation</td>
</tr>
<tr>
<td>Scope</td>
<td>Heterogeneous, high diversity</td>
<td>Heterogeneous, high diversity between members</td>
<td>Homogenous, low diversity within member organisations</td>
</tr>
<tr>
<td>Centrality/distribution</td>
<td>Horizontal leadership/collaborative; distributed across the local region</td>
<td>Horizontal leadership/collaborative; distributed across the local region</td>
<td>Centrality varies with member organisation, distributed across regions</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Loose connections, virtual relationships</td>
<td>Dense within cluster, loose between clusters</td>
<td>Dense within organisation, loose between organisations</td>
</tr>
</tbody>
</table>

**Table 2. Network profile for a DRN**

- **States**
  - Dependant on operation and surrounding environment
  - Emerge in crisis, lifespan ranges from temporary to long term

- **Exchange**
  - Information exchange, non-conserved, multiple forms of spread, bidirectional flow

- **Culture, leadership and governance**
  - Collaborative decision-making, open communications, transparency

- **Evolution and lifespan**
  - Collaborative decision-making, open communications, transparency

- **Variation**
  - Varies with member organisation
Figure 9, risk pockets lie in the unification of the network, coordination and engagement at the macro and meso levels of the network. Vulnerability is also shown in terms of connectedness at the macro level, and autonomy at the micro level. These findings reinforce risk profile findings presented earlier.

Table 3. Risk profile of inherent and adaptive risks for the DRN

<table>
<thead>
<tr>
<th>Network level</th>
<th>Risks/hazards</th>
</tr>
</thead>
</table>
| Macro Network | **Inherent** Administration<br>Unclear membership<br>Out-of-date membership<br>Loss of faith in leadership<br>Loss of trust in leadership<br>Reputation damage<br>Voting power may not be representative<br>Relationships with risky nodes e.g. rogue volunteers<br>Financial<br>Lack of funding loses member interest<br>Funded nodes may create power imbalance over others<br>Interpersonal<br>Relationships too loose (relationships formed ad-hoc in crisis, fail after)<br>Relationships with hub stronger than between organisations limiting interoperability<br>Communications<br>Echo-chamber effect – risk of spread of ‘contagion’ (misinformation, gossip, etc.)<br>Online tool constraints (no. of connections) limits participation in calls<br>**Applied (All hazards)**<br>Digital<br>Internet failure<br>Power failure<br>Online environment may fail<br>Hardware failure<br>Surveillance<br>Information controls<br>Internet disconnect<br>**Meso Hub, organisations**<br>Inherent Administration<br>Passive leadership/information leadership<br>Conflicting mandates/conflict of Interest<br>Conflicting ethics/breach of ethical<br>Breach of ethics (humanitarian principles)<br>Breach of legal mandate/liability<br>**Applied Digital**<br>Social engineering<br-DDOS attacks<br>Website attack<br>Trojan<br>Data stolen<br>**Micro Individual, relationships**<br>Inherent Psychological<br>Burn-out<br>PTSD<br>Loss of incentive/time to contribute<br>Self-censorship<br>**Applied Digital**<br>Computer virus/malware<br>Hacked account<br>Hardware seizure<br>Psychological<br>Threats to family/self<br>Harassment<br>**Service delivery**<br>Insufficient capability/capacity to deliver<br>Resource mismatching<br>Interoperability<br>HRO<br>Solution may be organisation focused versus tailored to needs on the ground<br>Humanitarian initiative could become political/activist in nature<br>HROs exploiting DHNetwork capacity beyond acceptable<br>Members may form own relationships and bypass DHN in future deployments<br>**Community**<br>DRN members serving in a digital response sense may be pulling resources away from the physical response of their own community<br>Request may be not a short-term solution – may require long-term involvement<br>Lack of/conflicting relationships with partners on the ground<br>Socio-political<br>Social unrest<br>Legislative change<br>Political<br>Natural<br>Earthquake<br>Tsunami<br>Typhoon<br>**Financial**<br>Loss of funding (if applicable)<br>Communications<br>Lack of knowledge/information sharing<br>Legal/Financial<br>Fine<br>Law suit<br>Psychological<br>Social network compromise<br>Trolling<br>Smear campaigns<br>Interpersonal<br>Internal conflict<br>Breach of trust/anonymity<br>Physical (if local OR deployed)<br>Arrest<br>Kidnap<br>Murder

Step 3: situate operational requirement, risk and option analysis

**Description**

Risk is treated and resilience is developed while isolating the fundamentals that can be captured in the tableau. This is
completed, first, by contrasting the operational requirement and risk profile with the findings from step 2. Requirements are removed, added or changed; inherent risks become mitigated, transferred or more vulnerable; and the control cost of risk is calculated (Hay, 2016). In contrast, applied risks are prioritised through all-hazards analysis and fall under shared virtual risks and operation-specific virtual and/or physical risks. Finally, unexpected risks are analysed by contrasting resilience gaps with one another or with the detailed network profile. Risk is treated as the resilience profile develops. OR is built through a portfolio of crisis management strategies along each stage of the incident sequence. Treatment options are proposed and deemed viable for selection where the whole cost of risk (including residual risk) is less than the control cost of risk. The final stage of the resilience profile, networked resilience, is developed in the next section through the tableau.

Application

Situating the DRN within the ESN sheds new insight on the ESN’s perceived vulnerabilities, identified risk and selected risk mitigation and resilience measures. As stated by Phillips and Hay (2017), an ESN may deem their vulnerabilities to be interoperability, infrastructure limitations (roads and traffic networks) and public utility overload. Selected risk treatment measures may include implementing a traffic management system to enable faster travel times for emergency vehicles, resituating stations to a scale-free distribution and increasing exercising and simulations to build diversity and internal capacity and strengthen relationships across functional boundaries. Incorporation of a DRN into the ESN can change these findings. Vulnerabilities change as a DRN may lower interoperability risk by generating broader and timely situational awareness while also smoothing the information flow between functions. Conversely, interoperability risk may increase between the ESN and DRN if the relationship is weak, clear lines of responsibility are not established and/or volunteer fluidity is too high. Cascading failure linked to infrastructure damage could be mitigated by leveraging DRNs for drone damage assessment, synthesis and reporting on areas impacted in correlation with remaining infrastructure – for example, damage to structures from an earthquake that could be prone to fire. For risk mitigation and resilience development strategies, they can further assist with traffic management through public alerting or leveraging crowdsourced traffic tools such as Waze or Google Maps that use a human sensor approach to gathering and disseminating traffic data in real time. To assist with resource sharing agreements, they can relieve the burden on human resources to manage information overload to focus on other tasks while also drawing in remote resources from like-minded communities to scale up the response. Using these findings, an ESN may modify their vulnerabilities to include virtual online interoperability (between DRN and ESN) and telecommunications (due to the increase in demand to enable and connect with DRNs while also enabling the local population to share pertinent information online).

Situating the DRN in the broader operational system reveals a series of changes to the operational requirement, subsequent risk and treatment measures. First, the operational system reveals the need for compliance with all stakeholders beyond the ESN, relationship building in local communities and security measures (both physical and digital) for remote and local deployments. These findings suggest the addition and/or reprioritisation of existing requirements. Second, the DRN observes changes to dependencies and risk perceptions when contrasting with the network profile. The lack of interoperability between member organisations (as shown by the hub-and-spoke structure) implies higher dependence on the hub and, thus, higher demand on hub members. This implies the requirements on personnel change, and, combined with scale-free vulnerability and the centralised geographic placement of hub coordinators, hub vulnerability

<table>
<thead>
<tr>
<th>Unified purpose</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 ownership</td>
<td>Collective leadership and governance</td>
<td>Impact is distributed</td>
<td>Impact is distributed</td>
<td>Impact is distributed</td>
<td>Impact is distributed</td>
<td>Impact is distributed</td>
<td>Impact is distributed</td>
</tr>
<tr>
<td>Strong identity</td>
<td>Faith in leadership</td>
<td>Minimized logistic burden</td>
<td>Minimized logistic burden</td>
<td>Minimized logistic burden</td>
<td>Minimized logistic burden</td>
<td>Minimized logistic burden</td>
<td>Minimized logistic burden</td>
</tr>
<tr>
<td>Commitment</td>
<td>Space for emergence and self-organisation</td>
<td>Collaboration and resource sharing</td>
<td>Collaboration and resource sharing</td>
<td>Collaboration and resource sharing</td>
<td>Collaboration and resource sharing</td>
<td>Collaboration and resource sharing</td>
<td>Collaboration and resource sharing</td>
</tr>
<tr>
<td>Conflict managed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 9. Resilience gap identification for the DRN
increases. Also, nodes situated mostly in the developed world means dependency is defined on developed world infrastructure. Requirements may need to change or scale to account for varied infrastructure conditions, whether designed to the lowest common capability or to ensure redundancies. Subsequently, risk increases the DRN’s capability to deliver. Third, contrasting the network profile with inherent risk shows the risk of fluidity and client buy-in is lower priority. There is a chance of risk transference in leadership and decision-making. Although the DRN approach aligns with many precursors of resilience (Hay et al., 2014; Hipel et al., 2011; Okada et al., 2006; Seville et al., 2015), secondary leadership risk emerges with higher priority due to differing personalities to competing mandates. Without a formal leadership structure and protocols, Freeman (1972) explained that likely repercussions include internal conflict, inconsistent vision, loss of trust, an inability to deliver and reorganisation of the network. Fourth, the resilience gap identification most strongly emphasises risk linked to leadership, cohesion and sustainability of the network. The DRN weighs these findings, adding on the lack of funding to compensate member involvement, periodic engagement and ad hoc nature of relationships. They deem leadership, cohesion and sustainability as the largest vulnerabilities in the network.

As described earlier, a DRN can render an ESN more resilient only if it is internally reliable and resilient. Thus, subsequent study of the DRN alone involves assessing events that may trigger failure of the DRN. Three risk scenarios (natural, malicious and accidental) are used to analyse applied risk. (A natural scenario is a cyclone affecting the power grid, cellular networks and Internet service providers. A malicious scenario is a rogue DRN volunteer that leaks sensitive data (user identities) from their crisis mapping platform. An accidental scenario is an accidental breach of ethics by a volunteer causing tension in rival factions in a war zone.) Findings suggest that natural disaster risk is low for the network as a whole, as interruption in one portion of the network can be balanced through function in another. Although the likelihood of network failure is low due to natural hazards, ICTs, Internet connectivity and power remain critical for nodes and clusters to function. Thus, connectivity risk is high. The malicious and accidental scenarios proved most detrimental to the network. They impacted trust (both internal and external), faith in leadership, digital burnout, reputation and buy-in to the network and, ultimately, the cohesion of the network. Thus, the DRN identified that they must select treatment options that can address these malicious and accidental associated risks, combined with connectivity, to manage their vulnerabilities.

Using this insight, combined with earlier findings, the DRN can become a more reliable resource to the ESN by identifying options and treating their highest priority risks. For connectivity concerns, they consider mandating training and adoption of alternate connectivity approaches – for example, mesh networking for physical interruption. They contemplate adding power backup and ICT redundancy to operational requirements or the requirement for all members to have dual SIM cards for more reliable mobile connectivity. To address cohesion and sustainability risk, they float the idea of developing a not-for-profit arm that would act as a potential funding partner (among other things) for the DRN. (This initiative is currently being explored by the DHNetwork, through the development of a DHNetwork non-profit organisation (DHNetwork, 2018)). This would build hub members’ sustainability and create the space for broader network innovations. They also consider forging relationships with local telecommunication providers to co-develop and implement a short messaging service for disaster information and reporting capability during disasters (Meier, 2010). This would increase connectivity options and build relationships at the local level. Another consideration is to build engagement through a three-stage model of engagement (pre-engagement, initial engagement and sustained engagement) (Robinson et al., 2016). For malicious and accidental events, the DRN considers adding digital security compliance to the operational requirement. In addition, they contemplate mandating training and minimum competency in digital security and standard data. They also require that all data storage and communication (email, chat) should be encrypted, and a no-email attachment policy may be implemented. They recognise that new members may need to be assessed in more detail prior to joining – for example, through a double-vetting process – and audited more regularly. (One DRN studied uses a double-vetting process, where members are added only if they are known and received approval through two members.) To manage interoperability risk identified by the ESN, the DRN may choose to run simulations regularly between the two networks. As the DRN is an unfunded network, treatment options are selected not in terms of costing but more so in terms of available and motivated personnel to lead changes, access to donor funding, time and resource commitment, perceived impact and/or general interest. Based on these criteria, the DRN selects implementing a local DRN as one of the risk treatment and broader resilience development options.

Step 4: define/refine and project the tableau

Description

The transition from operational to networked resilience occurs at this stage through tableau projection. The initial tableau is defined to capture the core requirements of the operation, risk and risk treatment and resilience strategies. It can be developed by one operation and projected or by a collection of operations and shared. It can apply to shared functions spanning different contexts, a shared context with different functions or situations where context and function are the same. In essence, it can be designed for any scale, context and/or function, from low to high granularity. It must, however, always be designed so that it is ‘universalised’ for the context in which it is to be projected. Once projected, the tableau is imported by operations with the capability to enable it. The broader network is made resilient through an iterative process of reusing the network profile for each NOR cycle until a critical mass of resilient tableaux penetrates the network.
Application
To implement and build a local DRN as a treatment strategy, the DRN begins by defining a tableau for that operation. Using the DRN tableau as a foundation and previous works on local DRNs (Phillips and Verity, 2016), they contrast the global with the local DRN context to identify overlaps and differences.

Overlaps exist between core functions of both networks. Echoing the global, a local DRN must (a) provide a focal point for contact in an emergency; (b) provide a matchmaking service between requesting organisations and DRN member organisations; and (c) ensure that capability is met through DRN member organisations. Dependencies, at a high level, stay the same. Personnel are required to perform the same functions, organisational procedures and guidelines must still be followed and ICTs are still required, as well as the enabling physical infrastructure.

In terms of differences, infrastructure condition is an important determining factor influencing not only connectivity but also the timeliness of response, which is fundamental to DRN capability. Contexts of application must allow for information sharing online and crowdsourcing of that information and response in support of civil power. This is distinct from the immediate response or reaction role of municipal first responders. The dynamics between the formal and citizen-driven response must be acknowledged, and a concept of operations must be established. In many cases, responders must shift their role from ‘saviours to enablers’ (Phillips, 2016) to support community leadership in an emergency and collaborate to accommodate the information needs during this time. Local DRN personnel will be a combination of local/offline and online members. Local relationships will be stronger with local authorities and community, increasing the capacity for situational awareness and collaboration with local authorities. Meanwhile, the local DRN and enabling infrastructure will be located in the hot zone of a disaster, facing higher likelihood of failure. Thus, redundancy and distribution of critical dependencies must be higher. In terms of operational system and risk, the local DRN must function in the local response picture and may need to coordinate requests from a broader scope of response organisations. Beyond risks to the global network, local all-hazards risks may be higher priority, and inherent risks may be more specific to the local context.

Among other differences, this insight informs the design of the DRN tableau so that it is general enough to enable the DRN operation at both the global and local levels. Functions and dependencies will remain the same, yet the specifics of the requirements are kept at a high level to allow for variance in how they are applied. Custom aspects of the global and local DRN are left for further tableau development. Once the DRN tableau is clearly defined and projected from the global DRN, the local DRN imports and enables it once it has achieved the capacity to enable the requirements outlined in the tableau.

Beyond the local DRN tableau, the DRN continues the process of tableau definition and projection. It co-develops a shared internal tableau defining basic requirements specific to DRN hub activation. They also developed a tableau for DRN activation and project it to the greater DRN.

The local DRN decides to develop at tableau to facilitate its relationships with external stakeholders. Between the local DRN and the ESN, they co-develop a shared surge capacity tableau for online deployment, as well as a tableau for the situational awareness function to ensure that both portions of the network can streamline information faster while meeting the needs of the responders themselves.

Discussion
Secondary application of NOR from the paper of Phillips and Hay (2017) to an ESN–DRN demonstrates the usability and generalisability of the framework, the context of virtual online networks and capabilities and requirements for collaboration. Initial application showed that NOR could be used to develop resilience in physical/virtual offline established networks, while application in this paper demonstrates that NOR can also be used for more complex networks such as DRNs – virtual online ad hoc networks. Deductively, NOR can be used to capture operational requirements, identify risk requirements and develop resilience in simple to complex networks, ranging from physical to virtual, online to offline and formal to informal networks across multiple infrastructure domains (built, natural, virtual). The insight gained from the adoption of the framework in the first paper is mirrored in this one – specifically, the use of a networked perspective, accounting for unexpected risk and inherent resilience yields different (more tailored) outcomes than an operation in isolation from its larger system. Situating an operation changes demands and dependencies, reveals new ones and reprioritises existing ones. Some risks are mitigated, some are transferred to other parts of the system and some emerge and/or become more vulnerable. Study of the DRN as a critical case study in partnership with an ESN generates insight on the operational requirements, risk landscape and resilience capability of a DRN in isolation, as well as the broader context and infrastructure requirements to enable this partnership. Beyond the specifics of the DRN–ESN case, much like the NOR framework is generalisable to varying complex networks, so are the findings. Understanding gained from the DRN context can be applied to other networks – that is, networks that are virtual, operating solely online and/or ad hoc and citizen driven, as well as complex networks that bridge infrastructure and operational domains. Some of these transformations and findings are explained in the review of the findings from the NOR analysis of the DRN–ESN simulated case study.

Through the lens of enabling physical and virtual infrastructure (both cyber and social), NOR analysis revealed insight on operating dependencies, inherent risk and resilience in virtual online networks. The criticality of dependency on telecommunication infrastructure and communication hardware (e.g. mobile phones, laptops) was identified. The loss of connectivity is immobilising when operations are strictly online.
Although the distributed nature of these networks renders them resilient – that is, the network can continue functioning in the event that one portion of a network goes down – risk lies at the individual and organisational level for connectivity. Measures must be put in place to ensure continued physical connectivity at all system levels to ensure the network’s ability to achieve its purpose. Without an offline physical location for collaboration, these networks must emulate and secure these environments online through their virtual cyberinfrastructure. Online tools create a virtual space for gathering, communications and decision-making and provide mechanisms to facilitate distributed collaboration – for example, online decision-making or online co-production. Combined with the loss of connectivity (virtual and/or physical), the scale of impact from digital attack renders a virtual online network unrecoverable. Integration and prioritisation of digital security measures into the operational requirement are fundamental to network survival. From the perspective of virtual (social) infrastructure, the hub-and-spoke structure of the network shows that relationships between members are weak, and the voluntary, virtual nature of how relationships are formed reinforces the looseness of interpersonal relationships. Dependency is higher on the hubs and, subsequently, on aspects of the social infrastructure including leadership, trust, culture and relationship building. The ad hoc citizen-driven nature of these networks implies a distinct relationship with community – these networks serve but also may be made up of that same community. Operation definition, risk treatment and resilience development demand strong integration of community input and relationship building along the process.

The intersection of physical and virtual operating environments exposes complexities in terms of inherent and all-hazards risk and resilience. Virtual online networks are exposed to a broader set of by-laws and legislation linked to the contexts in which members physically inhabit and virtually operate. Hence, compliance risk emerges and must be carefully managed. Similarly, the virtual environments surrounding virtual operations can inhibit or enable operations. Information controls and intrusive surveillance measures may constrain their capability. Tools and techniques may be required to facilitate networks to bypass these restrictions. Variation in the supporting physical infrastructure exposes risk linked to definition of infrastructure requirements for membership ranging from multijurisdictional to multinational distribution, and developed to developing world infrastructure condition. This merits careful design of an operational requirement that is generalisable across infrastructure domains and capabilities. Conversely, these risks are balanced with the capability for autonomous operations. While a local context may impose limitations and future research

The NOR framework is being successfully used to study the ICT connectivity requirements to enable smart city resilience, as part of the United for Smart Sustainable Cities programme. It is also being effectively applied to investigate infrastructure system rehabilitation, blending the complex relationship between virtual, physical and natural infrastructure systems. As speculated earlier, NOR has the potential to apply to multiple forms of networks yet requires further study to test, validate and refine (if needed) the methodology for wider application. Understanding of the virtual environment and the dynamics with the physical environment remains in its infancy. Without more detailed understanding, isolating the detailed requirements to enable virtual operation is difficult. Concurrently, application of NOR to virtual networks is constrained to hypothetical application only. The definition and study of resilience in complex networks remain somewhat novel given the rate the virtual environments are changing; hence the of what, to what, for whom (Cote and Nightingale, 2012) notion of resilience as an end state remains somewhat of a moving target. Partnerships between physical formalised offline networks and virtual online ad hoc networks (the case study in this paper) are also in their infancy. This paper prescribes how these networks can collaborate, the enabling requirements and an approach for co-development of resilience through shared tableau. However, in practice, the organisational cultures between networks often clash. Specifically, formalised networks are frequently hesitant to build

The development of resilience within complex networks is explained through partnership and tableau development between varying levels of the network. Virtual online networks can build resilience into physical operations. This study showed how DRNs build resourcefulness (enhanced capability) and autonomy (lifting the burden from a local resource to remote ones). The more distributed a DRN, the more diversified its enabling infrastructure and the reliability of its continued functioning in the event of communication interruption. As described through the explanation of a global to local DRN tableau, a resilient tableau can be defined at the network level (macro) for projection to the organisational level (meso level) within the same virtual online network – thus developing and transferring resilience between scales of the network. One can be defined between operations at the same scale – for example, from one local DRN to another local DRN in the same region. Otherwise, a tableau can be defined between different network types – for example, physical and virtual and online and offline. This was demonstrated in the construction of the situational awareness tableau shared between the local DRN and the ESN. As tableaux are developed within and between system levels and across network types, resilience development can occur in a complex network.

Limitations and future research

The NOR framework is being successfully used to study the ICT connectivity requirements to enable smart city resilience, as part of the United for Smart Sustainable Cities programme. It is also being effectively applied to investigate infrastructure system rehabilitation, blending the complex relationship between virtual, physical and natural infrastructure systems. As speculated earlier, NOR has the potential to apply to multiple forms of networks yet requires further study to test, validate and refine (if needed) the methodology for wider application. Understanding of the virtual environment and the dynamics with the physical environment remains in its infancy. Without more detailed understanding, isolating the detailed requirements to enable virtual operation is difficult. Concurrently, application of NOR to virtual networks is constrained to hypothetical application only. The definition and study of resilience in complex networks remain somewhat novel given the rate the virtual environments are changing; hence the of what, to what, for whom (Cote and Nightingale, 2012) notion of resilience as an end state remains somewhat of a moving target. Partnerships between physical formalised offline networks and virtual online ad hoc networks (the case study in this paper) are also in their infancy. This paper prescribes how these networks can collaborate, the enabling requirements and an approach for co-development of resilience through shared tableau. However, in practice, the organisational cultures between networks often clash. Specifically, formalised networks are frequently hesitant to build
formal partnerships and depend on informal resources. Detailed research is needed to characterise these challenges and competing attributes of culture and identify mechanisms to build collaboration and the broader integration of these networks.

To further understand the area of resilience development in virtual networks, as well as the viability and usability of the NOR framework, the crisis response context provides a vast range of online networks valuable for the case study. There are three types of applications to explore to evolve this theory. First, virtual online networks of study include advocacy networks and virtual operation support teams (Vosts). Advocacy networks, ranging from citizen journalist to hacker networks, leverage technology to advocate and protect rights and coordinate online to respond to digital crises (cyberattacks, online surveillance), among other activities. Not only do they often face a higher risk profile, but they also have more sophisticated digital security and circumvention techniques lending important insight on risk and resilience development online (Phillips, 2015). Vosts are citizen-driven response networks that formally partner with emergency managers and local jurisdictions to monitor social media during an emergency response. A study will build an understanding of interoperability between informal virtual online networks and formal virtual offline networks. Second, virtual offline networks include the community-led disaster response network Voluntary Organizations Active in Disaster or community emergency response teams. These networks seek to bridge interoperability between organisations operating on the ground during disaster. Research would shed light on formal and informal network collaboration offline during a crisis. Finally, virtual networks with a strong presence online and offline, hybrid virtual networks, include humanitarian aid organisations. A study will reveal complexities associated with internal online and offline virtual organisation and the nature of interaction in offline complex environments.

Conclusions
This study aims to contextualise virtual online networks, identify requirements to enable resilient complex networks and define associated physical infrastructure needs to enable these networks. These objectives are addressed through application of the NOR framework to a simulated case study of a complex network. Specifically, the discussion extends the initial definition and application of NOR from Phillips and Hay (2017) using an ESN – a physical/virtual formalised, offline network – to an ESN partnered with a DRN – a virtual, ad hoc, online network. The discussion begins with an overview of key concepts including networked resilience and the evolution of the NOR framework. The DRN–ESN simulated case study is presented and justified as a useful case study through initial introduction of virtual networks, definition and explanation of DRNs and description of the capabilities for resilience transference associated with partnership between physical offline and virtual online networks. The methodology is outlined by characterising the case study, risk analysis and NOR application process. Next, the four steps of the NOR framework are applied to the case study. First, operational requirements, dependencies and the incident response sequence are identified for a DRN in relation to an ESN. Second, overlaps and distinctions of the operational system and environment are identified for the DRN and ESN, and a network profile is generated for the DRN along structural and dynamic dimensions and attributes. Inherent risk, all-hazards risk and inherent resilience are conceptualised for the DRN as an operation and a network, and the DRN–ESN partnership. Third, the operational requirement is revisited and adjusted based on findings from step 2. Scenarios are used to prioritise and select risks, and risk treatments are identified. Finally, treatment of risk and the development of resilience are explained through the tableau concept using an example of a localised DRN. Following the NOR framework, discussion is provided to highlight study findings and articulate aspects of this research that are useful for broader application.

Understanding virtual operations exposes many challenges and complexities associated with developing resilience. It is apparent that a system is made resilient not only through its respective entities but also in between. Networked resilience is about making the relationship between nodes within and external to a network resilient. Resilience development for complex systems involves moving beyond building resilience for each individual system to building at the intersection of these systems. Through NOR this is possible.

REFERENCES
Canadian Red Cross (2012) Social Media During Emergencies. Canadian Red Cross, Ottawa, ON, Canada.