IDPR, 40 (3) 2018 https://doi.org/10.3828/idpr.2018.18

Jennie Phillips

Risk in a digital age: understanding risk in virtual networks through digital response networks (DRNs)

In a crisis situation, as citizens search online for support, many also move online to respond through digital response networks (DRNs). DRNs are citizen-driven networks that form and/or activate online during crisis to assist those affected, support those mandated to respond, and relay the needs of those affected. Whether humanitarian or advocacy related, they are invaluable to citizens and responders alike. There are associated risks, however, with what DRNs seek to achieve, how they operate and where. Enabling these networks requires risk treatment and resilience development, yet existing research fails to capture a holistic risk profile to base these treatments. Extending Phillips (2015), this study builds risk understanding by exploring inherent risk and resilience in DRNs. Data collected from DRN case studies is combined with elements of the Networked Operational Resilience (NOR) framework (Phillips and Hay, 2017). Discussion describes the DRN context, inherent risk and resilience landscape within the structural and dynamic dimensions of networks. Risk treatment and resilience development strategies, and areas for further research are provided.

Keywords: social media, crisis response, resilience, risk, networks, humanitarian technologies, advocacy, humanitarianism, virtual infrastructure, emergency management

Introduction

When crisis hits, the need for information is just as important as water, food, medicine and shelter; it can save lives, livelihoods and resources; information bestows power (IFRC, 2013). Coupled with access to information, the ability to share and communicate in a disaster is equally fundamental to response and recovery (BBC, 2012). As communities form offline to self-recover, communities form online to facilitate this recovery by responding to information demands in a crisis. Whether the need is to enable communications, respond to requests for information, 'make sense' of information generated, or relay pertinent information to a broader audience, these communities are ad-hoc citizen-driven volunteer networks or Digital Response Networks (DRNs) united under this purpose. DRNs consist of local and global individuals and organisations of varying skillsets from varying cultures and contexts. They have the capability to deliver on a 24/7 timeframe through a worldwide pool of resources, whether parsing big (crisis) data (Meier, 2011), coordinating resource distri-

Jennie Phillips is a PhD student at the University of Toronto, Ontario Institute for Studies in Education (OISE), 252 Bloor St W, Toronto, ON M5S 1V6, Canada; email: jennie.phillips@mail.utoronto.ca

bution, or amplifying human rights violations that would otherwise go unreported. Their vast capability combined with turnaround times and virtual form of operations renders them an indispensable resource to those affected, and those overwhelmed with providing support.

Yet the risk associated with DRN operations combined with a general lack of capability to manage it merits detailed study. Risk – the chance for harm – has been characterised previously in Phillips (2015). Findings showed that DRNs face physical to psychological risk, digital to legal risk, among other external (all-hazards) risks.[1] Yet, DRNs lack in-depth understanding of their risk landscape and are subsequently, underprepared or underequipped to manage risk. In response, this study aims to a) enhance understanding of risk in the context of online, virtual, ad-hoc networks; and b) identify mechanisms to assist the development of risk management capability within DRNs and/or networks of similar nature. This will be accomplished by building on the external risk landscape described in Phillips (2015) to include inherent risk, risk that is commonplace. Risk will be contrasted with inherent resilience, resilience that is naturally occurring. A networked approach will be used from the Networked Operational Resilience (NOR) framework (Phillips and Hay, 2017) to capture this risk, and resilience is assessed using the eight characteristics of resilience identified in complex networks.

Digital Response Networks (DRNs)

Extending local community and volunteer-led initiatives, digital volunteers form DRNs to assist locals affected by the crisis, support those mandated to provide support, and relay the needs of those affected. As depicted in Figure 1, members include affected communities (local and diaspora), and remote volunteers with a desire to help. Their capability is vast, with skillsets spanning disciplines including geographic information systems (GIS), information technology, information management, software development, emergency management, security training, journalism and human rights law. Their purpose can be humanitarian in nature. The Digital Humanitarian Network (DHN), for example, is a network of digital volunteers capable of performing tasks such as map creation, translation, filtering, analysing and visualising data, emergency communications and coding/hacking. They work with the DHNetwork, a broader network of networks that serves a match-making function connecting organisations in need of digital surge capacity with the organisations/networks capable of providing it. The purpose may also be advocacy related, where network activities are more politically focused (Phillips et al., 2016). Activities can include clicktivism (online petitioning for offline action), citizen journalism (citizen-led reporting of events on the ground), information activism (advocacy through information visualisation) or hacktivism

[1] All-hazards risk refers to external threats that can potentially harm an operation, ranging from natural, human-induced and/or digital hazards.

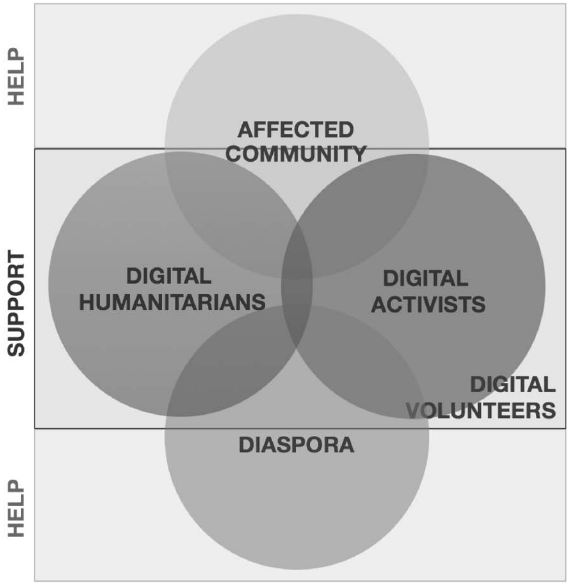


Figure 1 Digital Response Networks (DRNs)
Source: Author, updated from Phillips (2015)

(digital problem solving, ethical to digital attack e.g. the ‘anonymous’ hacker collective). As observed in the transformation of the Occupy movement to Occupy Sandy, or the case of the Russia self-help map (Meier, 2015b), networks can also possess a humanitarian and advocacy-related purpose (Phillips, 2015).

DRNs have the potential to make a profound impact on both communities and responders alike. The case of Kathmandu Living Labs (KLL) during the earthquake in Nepal 2015 is exemplary. The rise of KLL marks the ability of citizen-driven digital response efforts so profound that they shifted from a support to leadership role in a disaster. KLL is a local non-profit organisation specialising in regional mapping through open-source data. During the quake, they emerged to the spotlight for their ability to create maps superior to any official ones, on a turnaround time of hours instead of weeks (Asher, 2015). Through the support of thirty-six local volunteers and 4,300 remote DRN contributors, they collected and geo-located damage reports, and supported requests and photos shared on social media to assess and geo-locate where and what people needed (Wall, 2016). Mapping, combined with their ability to gather situational awareness and coordinate resources on the ground, made them a key focal point in the disaster. KLL became the first organisation to take the lead and become a critical service in a response, supporting several humanitarian organisations a day including the Nepalese Military, the United Nations and the Red Cross (Wall, 2016).

Yet, despite these leaps, KLL faced a series of risks associated with their work and their approach to operations. Financial risk, for example, was inevitable given they were a not-for-profit organisation coordinating a global surge of volunteers to meet a global surge of demand for information. As KLL shifted into recovery, a scale-up of operations was needed to continue operations and prepare for subsequent earthquakes. Yet, they failed to accrue enough funds from the big organisations that used their data. Legal and physical risks arose linked to their reliance on drones or unarmed aerial vehicles (UAVs) for needs and damage assessments. As Meier (2015a) explains, teams assumed full freedom to operate, as there were no formal regulations for UAV usage in Nepal. This disregard for local authority backfired. Dozens of UAVs were confiscated, and some volunteers got arrested. Also, the concern for digital risk was high given Nepal is a heavily censored environment (Gyawali, 2014) with a history of internet shut-downs in 2005 (Besant, 2005), and in 2011 (Rezwan, 2012). Self-censorship and journalist kidnappings and murders are also frequent in Nepal (Article 19, 2012).

Building on the case of KLL, a broader portfolio of external risks DRNs face is characterised in an earlier study (Phillips, 2015). DRNs are vulnerable based on where they work (generally in contexts where the likelihood of natural and human-induced disaster is higher), how they work (critical dependency on connectivity, vulnerability to privacy infringement, surveillance and information controls through online collaboration) and what they seek to achieve (missions that may be perceived as counter-regime). The hazards (accidental events) and threats (malicious events) that may harm a DRN can be described through Bronfenbrenner's ecological systems theory (Bronfenbrenner, 1994; Boon et al., 2011), where the system is understood through the individual in relation to different scales of their surroundings. As depicted in Figure 2,

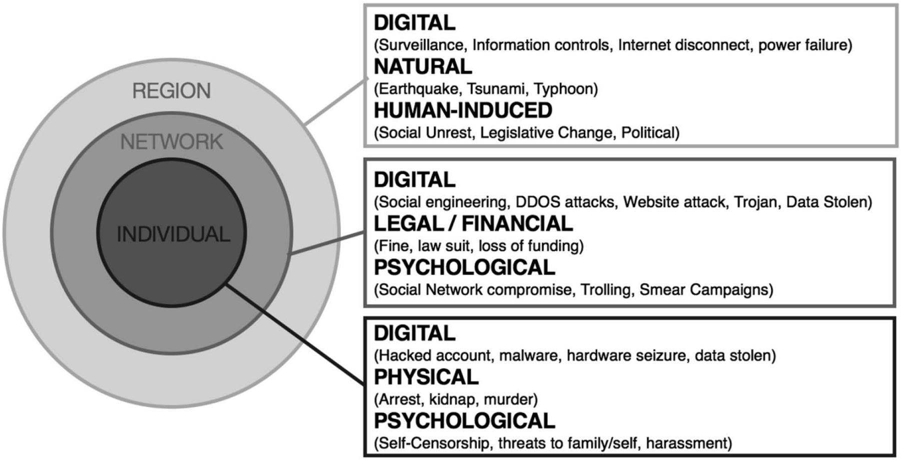

REGION
NETWORK
INDIVIDUAL
DIGITAL
(Surveillance, Information controls, Internet disconnect, power failure)
NATURAL
(Earthquake, Tsunami, Typhoon)
HUMAN-INDUCED
(Social Unrest, Legislative Change, Political)
DIGITAL
(Social engineering, DDOS attacks, Website attack, Trojan, Data Stolen)
LEGAL / FINANCIAL
(Fine, law suit, loss of funding)
PSYCHOLOGICAL
(Social Network compromise, Trolling, Smear Campaigns)
DIGITAL
(Hacked account, malware, hardware seizure, data stolen)
PHYSICAL
(Arrest, kidnap, murder)
PSYCHOLOGICAL
(Self-Censorship, threats to family/self, harassment)

Figure 2 DRN external risk landscape. DDOS refers to Distributed Denial-of-Service attack.
Source: Phillips (2015)

hazards and threats at the regional level include digital, natural and human-induced risk. At the network (organisational) level, risks include digital, legal/financial risk and psychological risks. Finally, at the individual level, risks include digital, physical and psychological risk.

A holistic risk profile is needed to effectively enable, sustain and protect DRN members and initiatives, yet the novel and emerging nature of DRNs limits existing understanding. Additional study is needed to fully comprehend the internal risk DRNs face due to the nature, mission and mechanisms of their operation. This implies capturing their inherent risk balanced with inherent resilience. Risk must be examined from a networked perspective, where structural and dynamic dimensions and attributes are accounted for. Coupled with this research, best practices and recommendations are needed to isolate how to treat these risks and develop broader resilience. The NOR framework (Phillips and Hay, 2017) provides a foundation for creating a more holistic risk profile by addressing each of these elements mentioned above. This paper aims to use concepts from the NOR framework to address these research gaps and better articulate a model for risk in DRNs through a resilience thinking lens.

Methodology

Data collection

Data for this risk profile were collected from multiple research projects and stakeholders across the digital activist and digital humanitarian realm. A qualitative case study approach was used to gain understanding of DRNs and assist with developing theory specific to their context (Yin, 2009). Formal research was conducted with two participant groups:

1) Cyber Stewards Network (CSN) – a global donor-funded network of individuals and organisations that uses evidence-based research for advocacy purposes to promote a secure and open internet (Citizen Lab, 2013);
2) Digital Humanitarian Network (DHNetwork) – a network of networks that bridges humanitarian response organisations in need of support with digital humanitarian networks (DHNs) capable of providing support (DHNetwork, 2015).

All participants were selected through convenience (access) and purposeful (most engaged) sampling. Data collection events included emergency and risk management workshops, in-person and remote face-to-face interviews, focus groups and online surveys. Tools included interview and focus group protocols, outputs from workgroup activities e.g. completed handouts, as well as online surveys. Data was collected along the following themes: the context and operations of DRNs; the risk landscape (perceived versus actual); existing knowledge and practice of risk management; perceptions of resilience in DRNs; current context, opportunities and challenges of building local DRNs; and the capacity and capability for emergency management, risk management and resilience development. Additional supplementary data is used from the 'What motivates citizens to participate' study (Phillips et al., 2016), as well as informal conversations, conferences, workshop and workgroup participation with DRNs to gain deeper understanding on research themes. All data was collected through note-taking techniques and analysed through qualitative coding to identify themes and research findings.

Theoretical framework

Research findings are analysed through elements of the NOR framework to build the DRN risk profile. The NOR framework prescribes a four-stage approach for developing resilience in virtual and/or physical networks by combining the operational resilience framework (Bristow, 2015; Bristow and Hay, 2014; Hay, 2013a; 2016) with systems, network, risk and resilience theory (Phillips and Hay, 2017). NOR distinctly situates an operation within a network and characterises and assesses risk to the network itself. It captures inherent resilience of a network and operation and provides a framework for identifying resilience development needs, referred to as 'adaptive resilience'. It also outlines how resilience can be captured, projected and evolved in a network through a *tableau* concept.[2]

Approach

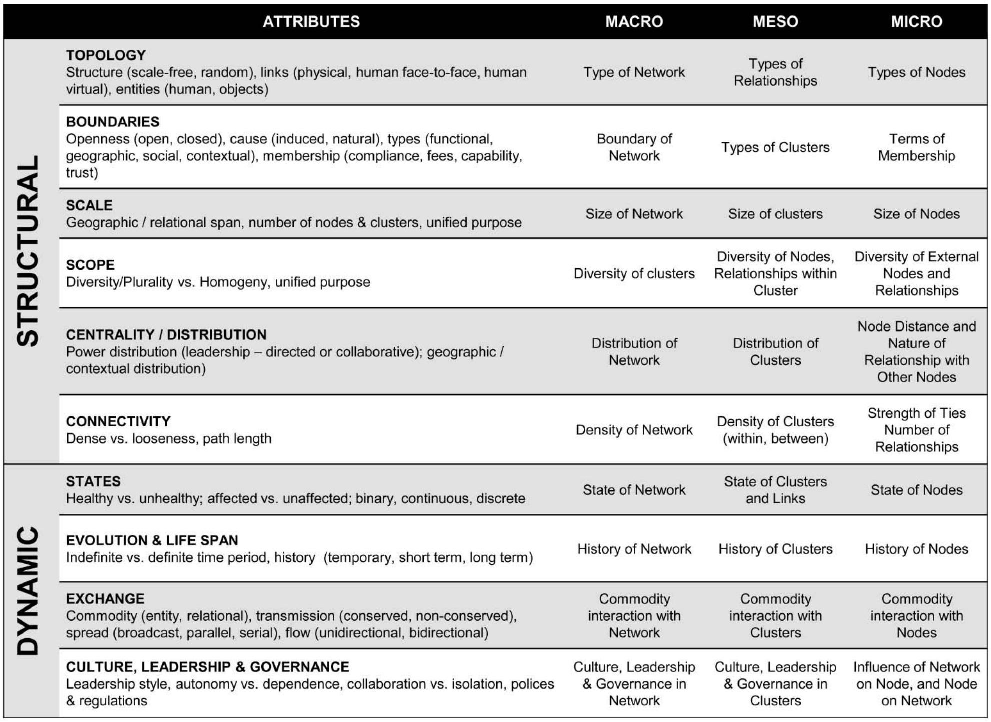
Using the NOR framework, DRN inherent risk is examined in a networked context using the framework for characterising a network (Phillips and Hay, 2017), see Figure 3.

Discussion is broken down along the following dimensions and attributes of networks:

1) Structural dimension: network topology, boundaries, scale and scope, centrality/distribution and connectivity;
2) Dynamic dimension: network state, evolution and lifespan, exchange, and culture, leadership and governance

The profile and inherent risk and resilience is described for each attribute specific to the DRN context. Inherent risk (risk during normal operations) is evaluated as

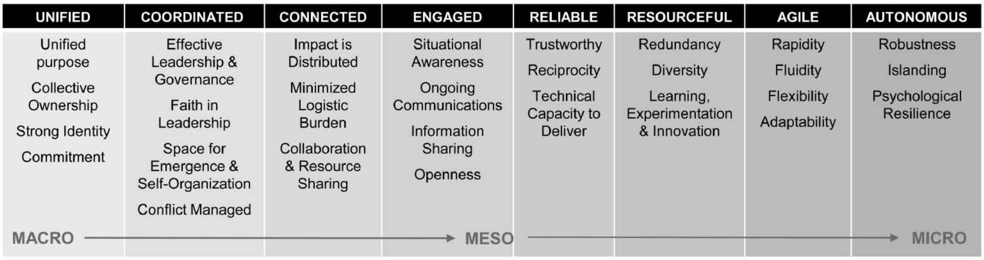
[2] The tableau depicts the operational requirement (what the operation must do and what it depends on) and operational risk independent of context. Risk treatment and resilience development strategies are embedded. The tableau is used to build resilience in a network through projection to other operations. Those with the capability and capacity to enable the operation will import and embed that tableau into their operation, thus assimilating resilience. See Phillips and Hay (2017) for further description.



	ATTRIBUTES	MACRO	MESO	MICRO
STRUCTURAL	**TOPOLOGY** Structure (scale-free, random), links (physical, human face-to-face, human virtual), entities (human, objects)	Type of Network	Types of Relationships	Types of Nodes
	BOUNDARIES Openness (open, closed), cause (induced, natural), types (functional, geographic, social, contextual), membership (compliance, fees, capability, trust)	Boundary of Network	Types of Clusters	Terms of Membership
	SCALE Geographic / relational span, number of nodes & clusters, unified purpose	Size of Network	Size of clusters	Size of Nodes
	SCOPE Diversity/Plurality vs. Homogeny, unified purpose	Diversity of clusters	Diversity of Nodes, Relationships within Cluster	Diversity of External Nodes and Relationships
	CENTRALITY / DISTRIBUTION Power distribution (leadership – directed or collaborative); geographic / contextual distribution)	Distribution of Network	Distribution of Clusters	Node Distance and Nature of Relationship with Other Nodes
	CONNECTIVITY Dense vs. looseness, path length	Density of Network	Density of Clusters (within, between)	Strength of Ties Number of Relationships
DYNAMIC	**STATES** Healthy vs. unhealthy; affected vs. unaffected; binary, continuous, discrete	State of Network	State of Clusters and Links	State of Nodes
	EVOLUTION & LIFE SPAN Indefinite vs. definite time period, history (temporary, short term, long term)	History of Network	History of Clusters	History of Nodes
	EXCHANGE Commodity (entity, relational), transmission (conserved, non-conserved), spread (broadcast, parallel, serial), flow (unidirectional, bidirectional)	Commodity interaction with Network	Commodity interaction with Clusters	Commodity interaction with Nodes
	CULTURE, LEADERSHIP & GOVERNANCE Leadership style, autonomy vs. dependence, collaboration vs. isolation, polices & regulations	Culture, Leadership & Governance in Network	Culture, Leadership & Governance in Clusters	Influence of Network on Node, and Node on Network

Figure 3 Framework for characterising a network
Source: Phillips and Hay (2017)

potential forms of harm internal to the operation. Resilience is evaluated through the 'eight characteristics for network resilience capability' from the NOR framework, see Figure 4.



UNIFIED	COORDINATED	CONNECTED	ENGAGED	RELIABLE	RESOURCEFUL	AGILE	AUTONOMOUS
Unified purpose Collective Ownership Strong Identity Commitment	Effective Leadership & Governance Faith in Leadership Space for Emergence & Self-Organization Conflict Managed	Impact is Distributed Minimized Logistic Burden Collaboration & Resource Sharing	Situational Awareness Ongoing Communications Information Sharing Openness	Trustworthy Reciprocity Technical Capacity to Deliver	Redundancy Diversity Learning, Experimentation & Innovation	Rapidity Fluidity Flexibility Adaptability	Robustness Islanding Psychological Resilience
MACRO →			→ MESO	→			MICRO

Figure 4 Eight characteristics for network resilience capability
Source: Phillips and Hay (2017)

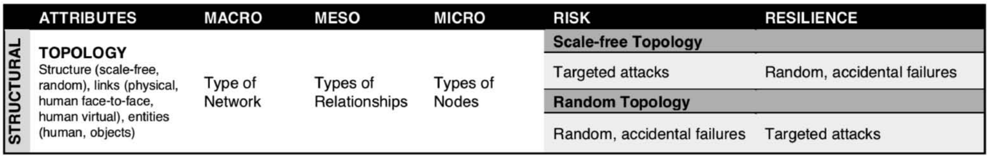
Based on definition by CRCI (2016), resilience is the ability to reduce the chances of shock, absorb stress and reorganise, learn and adapt under change; it is measured as the continued function or timely restoration to achieve its central purpose. A network is deemed capable of resilience if it is unified, coordinated, connected, engaged, reliable, resourceful, agile and autonomous (Phillips and Hay, 2017). Inherent risk and resilience is explained through 'frictions' i.e. elements that may render one network at risk may render another resilient. These frictions are visually depicted in modified segments of Figure 3 to show overlaps with the network profile. Discussion concludes with resilience development strategy and areas for further research.

DRN risk profile – structural dimension

Topology

Profile, risk and resilience

The topology of the network is captured by identifying the types of nodes, relationships and broader structures of the network. Nodes span multiple infrastructure dimensions (build, natural and virtual) where nodes stem from social networks i.e. humans, organisations and sub-networks connected through virtual or hybrid (virtual and face-to-face) relationships, to physical infrastructure networks i.e. the telecommunications and public utilities infrastructure enabling network connectivity. This article focuses primarily on the social network aspect of DRNs and the shared virtual infrastructure between them. DRNs consist of pockets or hubs of densely connected nodes (members) and large areas of the network that are loosely connected forming a scale free network model (Barabási, 2003; Barabási and Bonabeau, 2003). As key individuals (hubs) in these networks are responsible for gathering and leading pockets of the network e.g. organisations or ad-hoc sub-networks, the connections between these individuals and their affiliates are often stronger than the links between them, hence, hubs follow a hub-and-spoke structure. Frictions around risk and resilience are linked to network topology (Figure 5). Relative to random networks (Erdős and Rényi, 1959), the scale-free network topology is inherently at risk of targeted attack but resilient to random attacks or accidental failures (Barabási and Bonabeau, 2003; Medina and Hepner, 2008). More detailed discussion of frictions linked to topology are extrapolated in this risk profile section through discussion of the structural and dynamic dimensions.



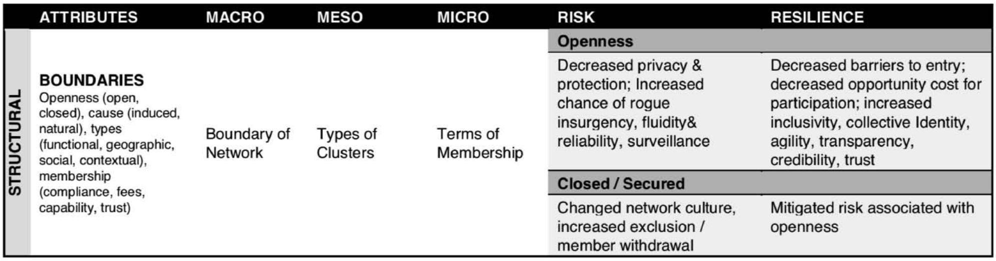
	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
STRUCTURAL	**TOPOLOGY** Structure (scale-free, random), links (physical, human face-to-face, human virtual), entities (human, objects)	Type of Network	Types of Relationships	Types of Nodes	**Scale-free Topology**	
					Targeted attacks	Random, accidental failures
					Random Topology	
					Random, accidental failures	Targeted attacks

Figure 5 Inherent risk and resilience frictions for topology
Source: Author

Boundaries

Profile

Network boundaries delineate where a network ends and begins, and openness is established through criteria for access. DRNs typically span geographic and national boundaries, virtually 'open' to anyone with the willingness and/or capability to engage at the individual, organisational or network level. Some are completely open, like online petitioning networks, with no membership requirements or formal acceptance process; simply an account is required. Operations are completely transparent where all administrative, operational and mobilisation information is shared publicly. More restrictive/focused DRNs grant membership based on reputation, pre-existing relationships, and/or trust. They may stipulate language requirements. Operational requirements may dictate access like the technical capability for online connectivity to compliance with digital security protocols. For networks in receipt of funding, membership will inherently split between those that are funded and those that are not. Risk and resilience varies depending on the openness of a network (Figure 6).



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
STRUCTURAL	**BOUNDARIES** Openness (open, closed), cause (induced, natural), types (functional, geographic, social, contextual), membership (compliance, fees, capability, trust)	Boundary of Network	Types of Clusters	Terms of Membership	**Openness**	
					Decreased privacy & protection; Increased chance of rogue insurgency, fluidity& reliability, surveillance	Decreased barriers to entry; decreased opportunity cost for participation; increased inclusivity, collective Identity, agility, transparency, credibility, trust
					Closed / Secured	
					Changed network culture, increased exclusion / member withdrawal	Mitigated risk associated with openness

Figure 6 Inherent risk and resilience frictions for boundaries
Source: Author

Risk and resilience

Open vs closed networks

The extent a network is 'open' dictates network growth to network vulnerability. Openness builds inherent attributes of resilience into a network. Open membership reduces the barriers to entry and minimises the opportunity cost of participation (Phillips et al., 2016). An open culture encourages information sharing, creates inclusivity, and helps build collective identity and agility into a network. Transparency builds credibility and trust. In political contexts that are heavily divided, for example, one participant explained how openness (publicly sharing all outcomes and activities) helps mitigate perceptions of partisan aid delivery. Conversely, decreasing membership stringency increases the chance of rogue insurgency. When membership is unregulated, participants highlighted challenges of detecting 'harmful' members like those with conflicting incentives to 'rogue volunteers' intending to destroy a network from within (Phillips, 2015). Second, openness enables fluidity and hinders reliability of a network. Participants explained how fluidity (the flow of volunteers in and out of a network) made it challenging to build a stable resource base and provide service. Key contacts within organisations change, often leading to the severance of internal ties with key partnerships. External partnerships depend on the perception of reliability. Third, as transparency increases, privacy and protection decrease. One participant emphasised this risk when digital literacy is low. When individuals do not understand technology and the impacts of use, they may gather and share vulnerable information that should not be shared publicly. Fourth, transparency facilitates surveillance and can empower repressive practices (Deibert, 2013; Boler and Phillips, 2016). Many participants emphasised an increase in digital attacks, from reputational to malicious email attachments, as the transparency and visibility of their operations increased.

Restricting access (closing a network) can address many of the risks above but exposes different risks. Strengthening boundaries can drastically alter network culture. One citizen-media DRN, for example, reported this shift when they transformed from an open to secured network. Initially openness increased contributors, content and visibility, but digital attacks to network members also increased. Closing the network protected members and data, but triggered members to leave the network under the impression that security made the network feel more corporate and closed. Despite threats, members reported feeling network culture no longer aligned with their initial motivations for joining. Second, restrictions may limit the voices being heard. One participant talked about the passive boundaries that emerge in online communication. In discussion of existing free secure video conferencing software, they highlighted how virtual rooms often limit the number of virtual attendees. This indirectly isolates members from the discussion and decision-making process, and, because of low resources, the meeting minutes often are not shared following these meetings.

Scale and scope

Profile

The scale and scope of the network dictates network composition. Scale refers to the size of the network and hubs (geographic and membership span), and scope is the plurality of hubs, nodes and relationships. In tandem with Figure 1, the continuum of online civic engagement (Figure 5) provides an effective snapshot of the scale and scope of DRNs (Phillips et al., 2016). The scale ranges from small hyper-local networks to global. The scope of members includes individuals, organisations, internal networks or sub-networks of individual nodes, with varying skillsets to a simple desire to engage. Homogeneity is frequently observed in smaller networks and clusters and heterogeneity is more common in larger networks. The variation of scale and scope expose frictions with risk and resilience (Figure 8).

Composition is dictated by the unifying purpose of the network i.e. the mission or vision they seek to achieve. The purpose is what defines an operation, a network, a community. It sets the foundation for building the shared identity needed for cohesion and sustained engagement (Phillips et al., 2016), and is one of the factors that differentiates communities that survive versus collapse in a disaster (Hay et al., 2014). The unifying purpose can be political to apolitical in nature (Figure 5). Arguably, any initia-

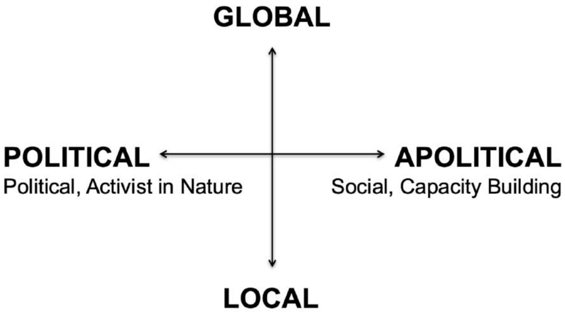
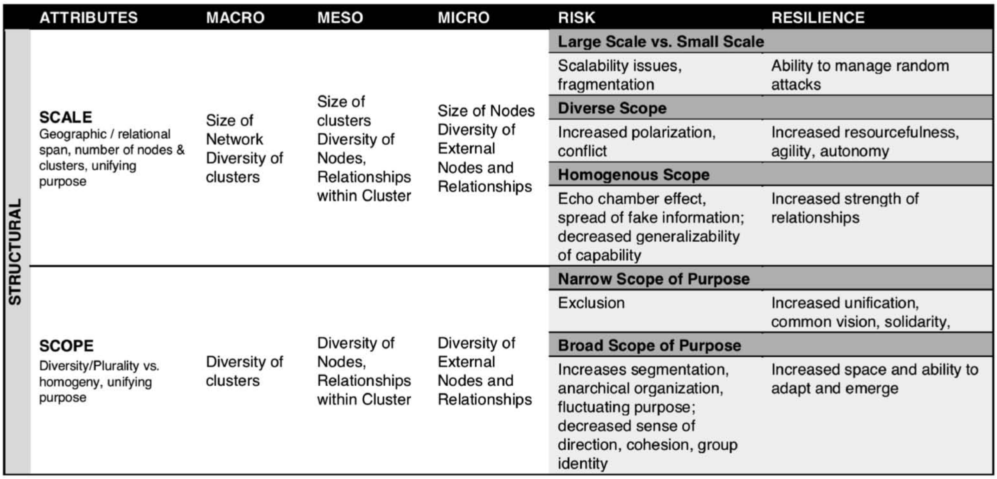


Figure 7 Continuum of online civic engagement
Source: Phillips et al. (2016)



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
STRUCTURAL	**SCALE** Geographic / relational span, number of nodes & clusters, unifying purpose	Size of Network Diversity of clusters	Size of clusters Diversity of Nodes, Relationships within Cluster	Size of Nodes Diversity of External Nodes and Relationships	**Large Scale vs. Small Scale**	
					Scalability issues, fragmentation	Ability to manage random attacks
					Diverse Scope	
					Increased polarization, conflict	Increased resourcefulness, agility, autonomy
					Homogenous Scope	
					Echo chamber effect, spread of fake information; decreased generalizability of capability	Increased strength of relationships
	SCOPE Diversity/Plurality vs. homogeny, unifying purpose	Diversity of clusters	Diversity of Nodes, Relationships within Cluster	Diversity of External Nodes and Relationships	**Narrow Scope of Purpose**	
					Exclusion	Increased unification, common vision, solidarity,
					Broad Scope of Purpose	
					Increases segmentation, anarchical organization, fluctuating purpose; decreased sense of direction, cohesion, group identity	Increased space and ability to adapt and emerge

Figure 8 Inherent risk and resilience frictions for scale and scope
Source: Author

tive is political: the distinction separates networks that are actively or passively political like the Arab Spring versus a disaster relief initiative. Many DRNs share a purpose that is political and apolitical in nature, like a response to a protracted emergency. Others fluctuate between the two. The transformation of the Occupy Movement to Occupy Sandy, for example, demonstrates a shift in purpose from advocacy, 'targeting the 99%', to humanitarian, organising and distributing supplies to disaster victims (Razorfish, 2013). Conversely, during the Russian wildfires in 2010, the humanitarian purpose of 'self-help map' to connect those in need of supplies with those on offer, became innately political as the Kremlin perceived their success as 'exposing the government's incompetence' (Meier, 2015b, 52). Risk and resilience varies with the scope of purpose (Figure 8).

Risk and resilience

Large vs small-scale networks

The scale of the network can increase resilience or increase fragmentation. Some argue that larger networks are inherently more resilient (Berkes et al., 2000; McConney and Phillips, 2011). Yet others claim larger network sizes can induce scalability issues (Jeanson et al., 2007), and increase fragmentation into smaller clusters (Naug, 2009). Dunbar (1998) argues one human node can handle relationships of ratio 1:150: beyond this point, relationships become unsustainable.

Diverse scope vs homogenous scope

Diversity can build capability or opportunities for conflict. It is a widely recognised attribute of resilience (Hay et al., 2017; Hopkins, 2009; Norris et al., 2007; Sage and Biemer, 2007). DRNs are innately diverse. Their open, voluntary, digital membership model creates networks that span cultures and continents, varying in skillsets, capabilities and supports. Resourcefulness, agility and autonomy results from this model and broader inherent resilience. Yet, diversity can also give rise to polarisation and conflict. As reported in Phillips et al. (2016), conflict in DRNs is prevalent. It can emerge from disagreement on core network functions, leadership, governance and an unclear purpose. Combined with the disinhibition affect, the lowered sense of inhibition associated with lack of face-to-face interaction, antagonising relationships result. Behaviours may include micro-aggression, cyber bulling to hate speech between members to the creation of a broader call-out culture. Conflict impacts the desire to engage, and, if mismanaged, triggers members to leave a network.

Homogeneity can unify a network while restricting knowledge and network application. It builds inherent resilience by strengthening relationships. Stevenson

(2014) for example, argues homogeneity in networks, like the internal contacts within a shared industry, can enhance an organisations ability to recover. Yet, homogeneity can inhibit the generalisability of network capability. DRNs are located primarily in the developed world, operating from a developed world infrastructure, high technical literacy rates and, often, greater access to funds. For the DRN model to be translatable to developing world contexts, the resources available to enable operations are incongruent between systems. As crises are often in developing contexts, interview participants cautioned services can be removed from the local context, lack cultural understanding, and/or demand technological resources beyond the capability of the local context. Homogeneity can also enable the echo chamber effect, and the spread of false or harmful information. Participants talked about this phenomenon, and how initiatives often attract likeminded individuals and organisations. Although tools like Facebook offer the ability to reach out and connect with diverse opinions and cultures, people often gather around shared interests and beliefs, shying from those who disagree with their opinions. As reported in the literature, this can subsequently lead to overemphasis or reinforcing false or misinformation; polarisation, compartmentalisation and radicalisation as online communities evolve (El-Bermawy, 2016; Hosangar, 2016; Phillips et al., 2016).

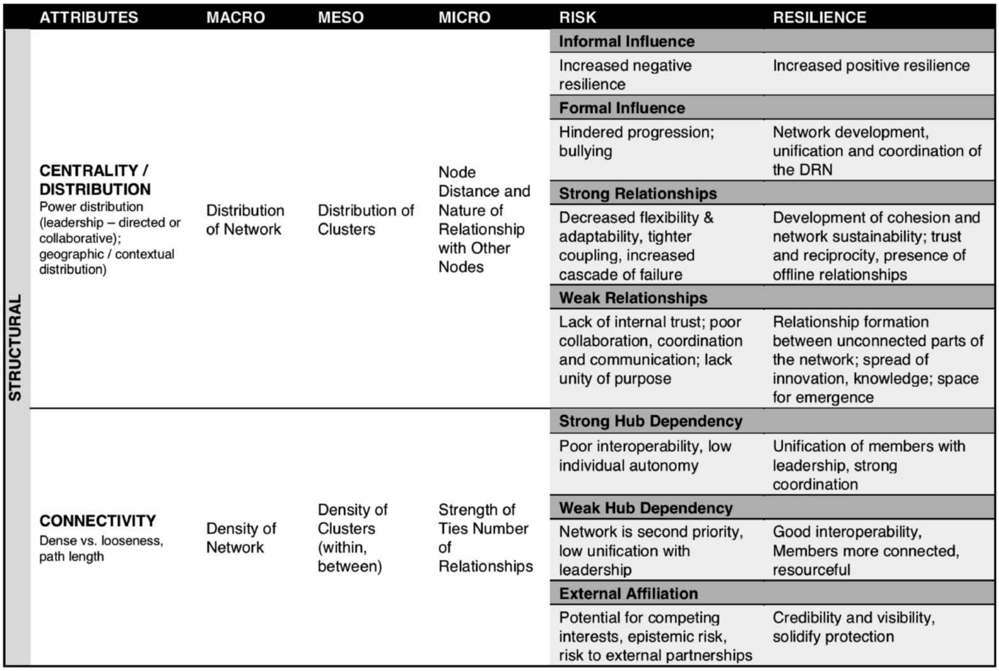
Narrow vs broad scope of purpose

The scope of purpose can lead to the unification of a network or the exclusion from it. A narrow purpose that is clear and concise, creates a common vision and builds resilience in solidarity. Yet, it can also restrict engagement (Phillips et al., 2016). Some interviewees expressed their activity online as a reflection of their offline identity (Boler and Phillips, 2016; Phillips et al., 2016). One person left a network, as she felt attacks on the mission were impacting her personally. In contrast, a broad purpose creates the space to adapt and emerge over time. As DRNs frequently battle both 'Big Data and Big Brother' (Meier, 2015b), space is fundamental for tailoring operations and fluctuate as needed; 'free space' or 'slack' is fundamental to resilience (Zolli and Healy, 2013). Conversely, a broad purpose can make it difficult to isolate a direction, develop cohesion and group identity, and lead to the segmentation. Aligned with Freeman (1972), participants highlighted 'anarchical organisation' may result. The purpose can be more vulnerable to change with conflicting interests. This may occur in line with meeting donor requirements (explained later) or accommodating competing mandates between members' primary organisations or day jobs and the network as second priority.

Centrality and connectivity

Profile

The texture of DRNs can be characterised by looking at *centrality* (the nodes) and *connectivity* (the relationships), and their interaction to form the network. Centrality examines nodes that are more connected than others, and their influence (Borgatti, 2005; Freeman, 1979; Tremayne, 2013). Applied to structureless networks, for example, informal nodes may demonstrate more influence over those that govern the network (Freeman, 1972). This was observed in all networks studied. Connectivity refers to the strength of the relationships between nodes and hubs. With the majority of relationships formed online, DRN relationships are typically weak. Participants explained the lack of face-to-face contact made it hard to build relationships and feel connected with the network. Hub-and-spoke structures (introduced under Topology) are regions of high centrality, with members as 'spokes'. Often, members exhibit stronger ties with the DRN hub and their own networks than with one another. Centrality and connectivity is built through affiliation with external high-profile nodes, like an international organisation. Risk and resilience changes depending on the source of influence (formal vs informal), strength of relationships, strength of hub dependency and the nature of external affiliation.



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
STRUCTURAL	**CENTRALITY / DISTRIBUTION** Power distribution (leadership – directed or collaborative); geographic / contextual distribution)	Distribution of Network	Distribution of Clusters	Node Distance and Nature of Relationship with Other Nodes	**Informal Influence**	
					Increased negative resilience	Increased positive resilience
					Formal Influence	
					Hindered progression; bullying	Network development, unification and coordination of the DRN
					Strong Relationships	
					Decreased flexibility & adaptability, tighter coupling, increased cascade of failure	Development of cohesion and network sustainability; trust and reciprocity, presence of offline relationships
					Weak Relationships	
					Lack of internal trust; poor collaboration, coordination and communication; lack unity of purpose	Relationship formation between unconnected parts of the network; spread of innovation, knowledge; space for emergence
	CONNECTIVITY Dense vs. looseness, path length	Density of Network	Density of Clusters (within, between)	Strength of Ties Number of Relationships	**Strong Hub Dependency**	
					Poor interoperability, low individual autonomy	Unification of members with leadership, strong coordination
					Weak Hub Dependency	
					Network is second priority, low unification with leadership	Good interoperability, Members more connected, resourceful
					External Affiliation	
					Potential for competing interests, epistemic risk, risk to external partnerships	Credibility and visibility, solidify protection

Figure 9 Inherent risk and resilience frictions for centrality and connectivity
Source: Author

Risk and resilience

Informal vs formal influence

In some networks, informal power structures contribute to positive resilience (resilience of optimal conditions) where others render the network ‘negatively’ resilient (resilience of sub-optimal conditions). As Kaufman (2012) describes, if a current state is undesirable, resilience can impede change like the conditions observed in terrorist networks and repressive political contexts. Frequently, the highly connected and influential members (in non-leadership roles) were more effective in building, unifying and coordinating DRNs than those formally appointed. They spearheaded the development of trust and reliability of inter-member relationships. In other cases, members described powerful nodes (also in non-leadership positions) hindering the progression of the network while also bullying some members who later disengaged.

Strong vs weak relationships

The strength of ties may enable network sustainability but hinder growth. Strong ties innately build cohesion and sustainability of a network (Barabási and Bonabeau, 2003; Phillips et al., 2016). Yet, Granovetter (1973) argues weak ties connect parts of a system that would otherwise remain unconnected; they are key for the diffusion of innovation, cultural and scientific ideas (Granovetter, 1983); and they create space for collective individual actions over directed and controlled ones (Hay, 2013b; Johnson, 2012). Likewise, flexibility and adaptability diminish as strength of ties increases. ‘Tightness’ may limit the space for emergence (Johnson, 2012; Meadows, 2008) while increasing the impact of cascading failure (Hay et al., 2017). In discussions, participants linked weak ties to agility, connectivity and resourcefulness. They were particularly useful for advocacy networks focused on empowering free speech and diversity. However, participants felt weak ties represented a lack of internal trust, poor collaboration, coordination or communication and a lack of unity with the purpose – all attributes shown to keep a network together. Some felt that stronger ties represented inherent resilience. It indicated trust and reciprocity, and the presence of offline relationships. Stronger connectedness was reported to make a network more resilient to fluctuations, and more sustainable.

Strong vs weak centrality (hub dependency)

Hub dependency can be depicted in terms of confidence (weak dependency) or lack thereof (strong dependency) (Hay et al., 2017). In reference to the hub-and-spoke structure, participants described member relationships to be stronger with the hub than with one another (between ‘spokes’). This implied poor interoperability and autonomy in members, and strong dependency on the hub. They felt that this dynamic rendered the network highly vulnerable to collapse in the event the hub became unavailable.

Yet, others felt strong ties with the hub reflected a strong hub-to-member relationship, unification of members with leadership, and strength in coordination with the central hub. In networks that felt dependency was weak on the hub, it was observed that members are more connected with one another than with the hub, may have stronger relationships and better interoperability. Yet, they warned if the relationship with the hub is too weak, members may prioritise their own networks and/or bypass the DRN in future endeavours (explained as conflicted members).

External affiliation

The question of 'who is connected to who' can mean resilience or risk. Affiliation with high-profile organisations and individuals can build credibility and visibility of a DRN, and/or solidify protection. It can also place members at risk depending on their context and purpose. One interviewee, constantly bombarded by threats, explained how these high-profile relationships can periodically represent competing interests with a local government and place the individual and/or organisation as a 'foreign agent' in the eyes of the local society. In certain cases, a global support network may not be useful but also dangerous. They explained:

> If the authorities come and pick me up and say I'm working for a foreign agenda, and I try to prove I'm not and I'm dedicated to the country, If a foreign network issues a statement justifying my involvement it can make it worse. (Excerpt from focus group interview with digital activists, 2015)

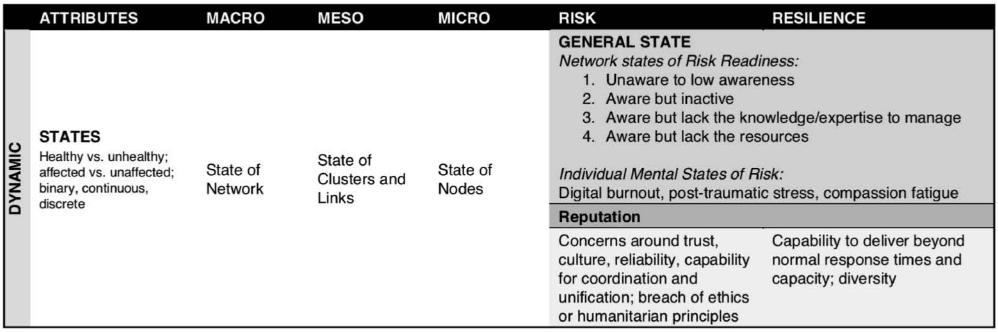
In other cases, a network is only as strong as its weakest link. A network can take all the precautions (e.g. security, training, or risk management) yet epistemic risk will persist and topple a network if realised. Whether simple lack of digital awareness of failure to comply with digital security measures, this negligence exposes vulnerabilities into a network like the risk of hacking and/or broader digital attack. Finally, risk is not to the network itself but what it is connected to. Participants spoke frequently of the vulnerability of external nodes i.e. the nodes outside a network that rely on the network. Frequently they are more vulnerable than nodes within the network itself. In the event of an attack, the network is more likely to manage the consequences than those on the periphery. An internal attack managed improperly may have subtle consequences on a network but dire consequences on the individuals and organisations they are supporting.

DRN risk profile – dynamic dimension

Current state

Profile

The state of the network depicts the 'health' of the network. Perceptions of 'health' varied for different scales of the system. At the network and organisational level, it



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
DYNAMIC	**STATES** Healthy vs. unhealthy; affected vs. unaffected; binary, continuous, discrete	State of Network	State of Clusters and Links	State of Nodes	**GENERAL STATE** *Network states of Risk Readiness:* 1. Unaware to low awareness 2. Aware but inactive 3. Aware but lack the knowledge/expertise to manage 4. Aware but lack the resources *Individual Mental States of Risk:* Digital burnout, post-traumatic stress, compassion fatigue	
					Reputation	
					Concerns around trust, culture, reliability, capability for coordination and unification; breach of ethics or humanitarian principles	Capability to deliver beyond normal response times and capacity; diversity

Figure 10 Inherent risk and resilience frictions for centrality and connectivity for current state
Source: Author

referred to the perceived capability and reputation, as well as the general 'state of readiness'. At the individual level, health referred to 'state of mental health'. Across all levels, state was seen widely as a reflection of vulnerability. Consequently, current state is defined below under risk and resilience, with frictions to follow (Figure 10).

Risk and resilience

Drawing from Phillips (2015), DRNs exhibited low risk awareness, and minimal adoption of risk management and resilience development practices. DRNs fall along four states of readiness described below. Most DRNs interviewed fell into the third or fourth state of readiness.

1) *Unaware to low awareness* – participants were either unaware or lacked a clear understanding of their risk landscape.
2) *Aware but inactive* – participants were aware of potential risks but placed little to no priority on taking measures to manage these risks.
3) *Aware but lack the knowledge/expertise to manage* – participants were aware of their risk landscape but lacked internal knowledge or expertise to manage it. Many were unaware of established practices and confused key concepts.
4) *Aware but lack the resources* – participants were aware of their risk landscape but lacked the human (insufficient members/staff), financial (no funds for risk treatments), and operational resources (plans, more secure and robust online software) to manage it.

States of mental health also varied and digital burnout was common. As described by Lim (2012), DRN-like initiatives are frequently driven by a core group of 'tireless leaders' contributing their time disproportionately to other members. One interviewee reported working seventy hours during some activations above their normal thirty-five-hour work week. Many emphasised the challenges of boundary setting in a context where the contribution of time is unregulated and unmonitored. Post-traumatic stress was raised as frequently experienced and observed in others. One interviewee likened their experience to Ashraf's (2013) recount of his digital involvement in Iran's Green Movement. Ashraf describes 'being connected to something you are disconnected from'. He explains how easy it is to get consumed and how difficult it is to separate, the feelings of isolation, and lack of support. Compassion fatigue, the decline of volunteer interest as a disaster extends, was also mentioned. Participants expressed how this impacts the longevity of volunteer involvement. One DRN explained they only provide support during the first two weeks of a disaster for this reason. Beyond these states of vulnerability, reputation was a point of friction in the context of risk and resilience.

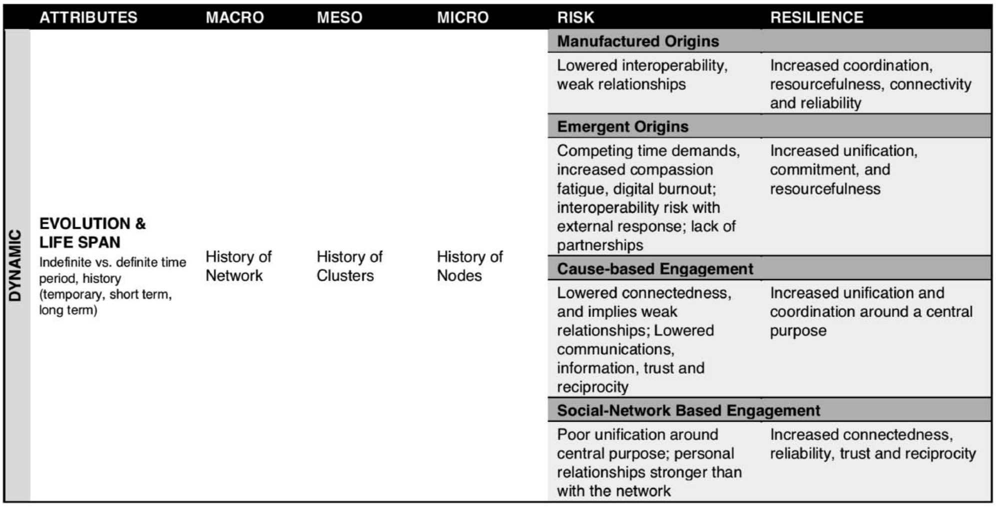
Perceived reputation

Reputation can be the main attractor or deterrent for membership and partnership. Given the scale and scope of membership, diversity of skillsets and unprecedented turnaround times, DRNs are innately resilient in the capability aspect of their reputation. And this ability to deliver and make an impact is fundamental for attracting and sustaining membership and support (Phillips et al., 2016). Yet deep-rooted perceptions of volunteer networks can impose reputational risk. In the literature, formal responders are reported as apprehensive about trust, culture, reliability and capability of volunteer services, and the capacity for coordination and unification between initiatives (Capelo et al., 2012; Orloff, 2011; Whittaker et al., 2015). Recalling KLL, their inability to accrue funding may allude to the depth of apprehension working with citizen-driven initiatives. The DHNetwork formed in efforts to overcome these challenges, to build partnership, but many members emphasised that this disconnect remains and is particularly acute for digital networks where face-to-face contact is not possible. Beyond external perception, participants also highlighted the risk of internal reputational damage i.e. the intentional or accidental breach of ethical code or humanitarian principles can be detrimental to the membership and sustainability of a network.

Evolution and life span

Profile

Evolution and life span depicts how networks emerge, sustain and collapse over time. This can be explained through the nature of origin, reasons for engagement and membership. DRNs have manufactured and emergent origins. Manufactured implies they are intentionally created for a specific purpose, like a digital security network built on receipt of funding. Emergent networks arise naturally around an exigent purpose, such as ad-hoc networks that form in disasters. Reasons for engagement (at the initial stages) include online and offline presence, nature of the task, and capacity for impact (Phillips et al., 2016). The type of organisation, whether identity-based (e.g. LGBTQ rights and issues) or cause-based (e.g. climate change, or human rights) influences leadership dynamics. An identify-based cause tended towards decentralised leadership versus issue based which was more centralised (Phillips et al., 2016). In both types, relationships with the hub were often stronger than between individuals (as described earlier). Coinciding with the literature (Boler and Phillips, 2016; McAdam et al., 2004; Phillips et al., 2016), interviews showed many networks formed as an extension of their existing online or offline personal relationships. In all networks, once membership is granted, participation includes being added to a mailing list, invited to and attending workshops, meetings and conferences, and/or engaging in network activities. Unless imposed through funding requirements, participation and contribution is, most frequently, optional. Frictions around risk and resilience are linked to the nature of origin, and rational for engagement (Figure 11).



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
DYNAMIC	**EVOLUTION & LIFE SPAN** Indefinite vs. definite time period, history (temporary, short term, long term)	History of Network	History of Clusters	History of Nodes	**Manufactured Origins**	
					Lowered interoperability, weak relationships	Increased coordination, resourcefulness, connectivity and reliability
					Emergent Origins	
					Competing time demands, increased compassion fatigue, digital burnout; interoperability risk with external response; lack of partnerships	Increased unification, commitment, and resourcefulness
					Cause-based Engagement	
					Lowered connectedness, and implies weak relationships; Lowered communications, information, trust and reciprocity	Increased unification and coordination around a central purpose
					Social-Network Based Engagement	
					Poor unification around central purpose; personal relationships stronger than with the network	Increased connectedness, reliability, trust and reciprocity

Figure 11 Inherent risk and resilience frictions for centrality and connectivity for evolution and life span
Source: Author

Risk and resilience

Manufactured vs emergent origins

The way a network begins can render it instantly unified or instantly segmented. Manufactured DRNs demonstrate inherent resilience in their coordination, resourcefulness, connectivity and reliability (see discussion under centrality), and risk weak relationships and a lack of interoperability. Emergent networks appeared more unified, committed and resourceful, with risks of competing time demands, digital burnout and compassion fatigue. Discussions revealed that emergent networks also possess interoperability risk with the external response system. Without pre-existing relationships and protocols prior to a crisis, it is often difficult for networks to integrate into a disaster response system.

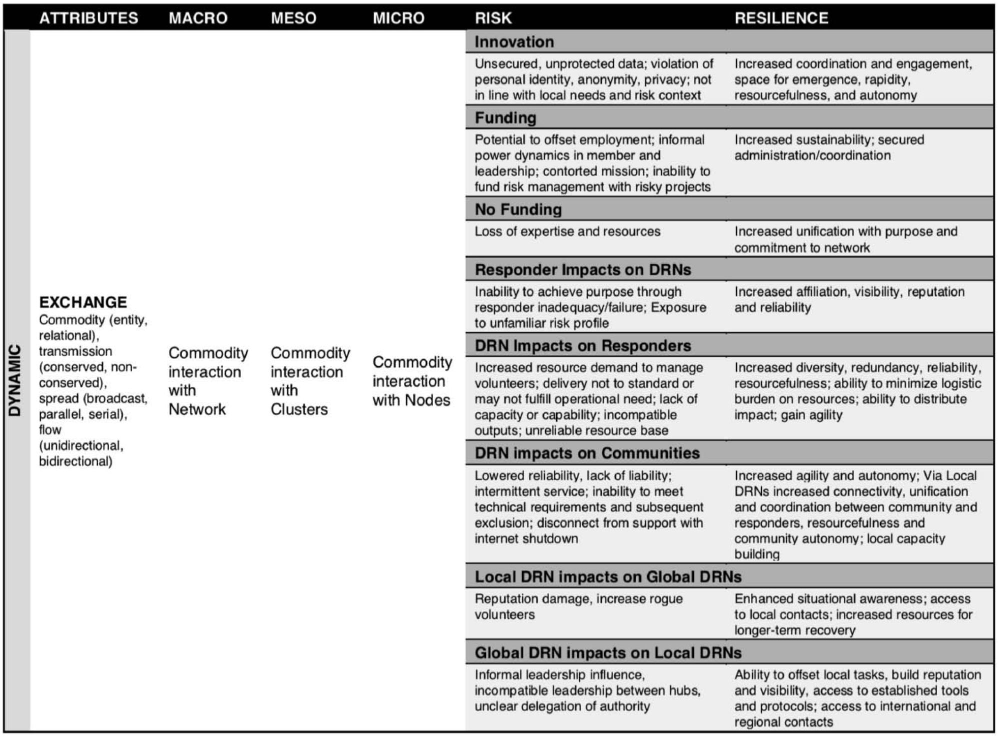
Cause vs social network-based engagement

Cause-based networks appear to be unified and coordinated, but are at risk of low connectedness due to weak relationships between members. Effective communications, information sharing, trust and reciprocity must be developed in these contexts. Poor leadership to facilitate these processes can have devastating impacts on the longevity of the network. Social network-based engagement leads to inherent resilience through connectedness, and reliability through the pre-established trust and reciprocity in these relationships. Yet, the risk is relationships are stronger with one another than with the purpose. Subsequently, there is risk associated with unification of the network.

Exchange

Profile

Exchange refers to transmission of commodities over a network. The primary commodities (network inputs/outputs) identified in DRNs were services and funding. Crisis enables the necessary conditions to trigger just-in-time innovation, one of the DRN services. This ranges from the development and deployment of tools like Ushahidi (a crowdsourcing tool for map generation) during Haiti 2010 (Meier, 2015a) to the usage of drones for image capture and analysis of disaster affected areas (UAViators, 2017). DRNs survive and thrive on the delivery of innovation. Funding is received through donors to seed/crowdfunding, often through a central hub of network administrators. Beyond the hub, members do not receive funding and participation is voluntary. In some cases, one member may be funded to administer the network while the remainder is voluntary, and, in others, the entire network is voluntary. Network transmission occurs between DRNs and responders (e.g. international organisations,



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
DYNAMIC	**EXCHANGE** Commodity (entity, relational), transmission (conserved, non-conserved), spread (broadcast, parallel, serial), flow (unidirectional, bidirectional)	Commodity interaction with Network	Commodity interaction with Clusters	Commodity interaction with Nodes	**Innovation**	
					Unsecured, unprotected data; violation of personal identity, anonymity, privacy; not in line with local needs and risk context	Increased coordination and engagement, space for emergence, rapidity, resourcefulness, and autonomy
					Funding	
					Potential to offset employment; informal power dynamics in member and leadership; contorted mission; inability to fund risk management with risky projects	Increased sustainability; secured administration/coordination
					No Funding	
					Loss of expertise and resources	Increased unification with purpose and commitment to network
					Responder Impacts on DRNs	
					Inability to achieve purpose through responder inadequacy/failure; Exposure to unfamiliar risk profile	Increased affiliation, visibility, reputation and reliability
					DRN Impacts on Responders	
					Increased resource demand to manage volunteers; delivery not to standard or may not fulfill operational need; lack of capacity or capability; incompatible outputs; unreliable resource base	Increased diversity, redundancy, reliability, resourcefulness; ability to minimize logistic burden on resources; ability to distribute impact; gain agility
					DRN impacts on Communities	
					Lowered reliability, lack of liability; intermittent service; inability to meet technical requirements and subsequent exclusion; disconnect from support with internet shutdown	Increased agility and autonomy; Via Local DRNs increased connectivity, unification and coordination between community and responders, resourcefulness and community autonomy; local capacity building
					Local DRN impacts on Global DRNs	
					Reputation damage, increase rogue volunteers	Enhanced situational awareness; access to local contacts; increased resources for longer-term recovery
					Global DRN impacts on Local DRNs	
					Informal leadership influence, incompatible leadership between hubs, unclear delegation of authority	Ability to offset local tasks, build reputation and visibility, access to established tools and protocols; access to international and regional contacts

Figure 12 Inherent risk and resilience frictions for centrality and connectivity for exchange
Source: Author

governments, first responders and non-government/non-profit organisations), DRNs and communities, and, in rare cases, within local to global DRNs. Frictions associated with risk and resilience were linked to innovation, funding and the dynamics of transmission (Figure 12).

Risk and resilience

Innovation for better or for worse

Sage and Cuppan (2001) argue innovation is required for survival in adaptive environments; to be resilient is to be innovative (McManus et al., 2009; Seville et al., 2015). The innovative nature of DRNs demonstrates inherent resilience in their ability to coordinate and engage, space for emergence, rapidity, resourcefulness while also individual autonomy. Yet, innovation exposes certain risks. Participants raised concern over the data collected, stored and shared with these tools. There is controversy, for example, with online people finders and the fine line between situational awareness and surveillance. Sharing information to help locate lost loved ones can be invaluable in some cases (Reidy, 2017), yet publicly sharing the names and identities of people that need protecting may place them at higher risk. Participants, particularly in the digital security realm, emphasised how anonymity and privacy (especially of their location) are imperative to the survival of themselves and those they support, regardless of circumstances. Second, risk innovating from the developed world implies interventions may be developed for contexts with little to no understanding of risk. Combined, most of these tools are developed so quickly that there is no time for testing any risk and security implications. Ultimately, risk transference can become of greater concern.

To fund or not to fund

Funding can solidify key resources to sustain a network whilst also crippling the core mission. As described, networks without funding tend to be unified in their commitment to the purpose and the network. Yet, a lack of funding may imply losing expertise. Interviewees emphasised it is difficult to sustain continuity in networks that do hard work but do not get paid for it. Individuals are competing with their real jobs. Interviewees also discussed the risk of offsetting employment i.e. taking jobs away from those that can get paid. Some felt, if ‘clients’ can get quality support without a cost, why would they pay for it. In contrast, some DRNs felt funding can drastically assist sustainability. Specifically, they equated funding of one key administrative person to enhanced coordination and network operations. When funding is introduced, however, a different subset of risks emerges. First, not all members typically receive funding. The delineation that results between funded and unfunded members was reported to influence power dynamics and equal weighting between member voices and decision making. Second, funding can enforce involuntary power dynamics on leadership. One funded network, for example, explained how attempts to build horizontal leadership failed due to the underlying power dynamics linked to funding requirements. Third, funding is usually temporary/short-term. Interviewees explained the subsequent risk of diverting resources to accommodate funding cycles over their primary purpose. They also explained the risk of contorting their purpose. One participant explained how funding often gets rewarded on ‘keeping things dynamic’ implying funders get tired of funding the same things over time. Networks must identify creative ways to sell their cause over and over. They run the risk of ‘losing their soul’ they explained in trying to meet the requirements. Fourth, funding for high-risk allocates insufficient funds to manage that risk. There is often little to no empathy, understanding or consideration regarding the nature of the work and the risk grantees may experience as part of doing the work. No space for risk management and broader resilience development is allocated in a project, making it difficult to learn about, manage and treat risk. As one participant commented ‘they think we’re superheroes’ (excerpt from digital activist interview, 2015).

Dynamics of transmission

DRNs and their ‘clients’ mutually assume risk and resilient attributes associated with the transmission of service. Directional dynamics between DRNs and responders, from DRNs to communities, and between global and local chapters of DRNs (local DRNs) were mainly discussed and are described below.

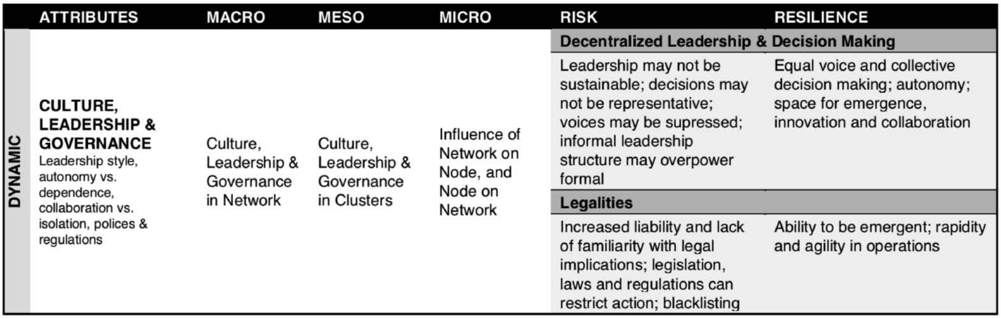
- DRN ← responder – DRNs gain attributes of resilience (e.g. affiliation, visibility and reputation discussed earlier) through this partnership, but also risk their reputation and vulnerability. First, if DRNs fail to deliver they fail to achieve their core purpose, which implies potential reputational damage to loss of partnerships or members. As emphasised earlier, the perception of capability and impact is fundamental to the long-term sustainability of volunteer-led, ad-hoc networks. Participants explained failure may occur through partnership due to incompatible mandates, inaccurate or biased support requests for needs on the ground, an insufficient support period to achieve tangible outcomes, a lack of on-the-ground relationships to enable DRN operations, among others. Second, responders may also expose DRNs to a risk profile that is different from their own, and that they are unprepared for.
- DRN → responder – Responders build resilient attributes like diversity, redundancy and reliability through DRN partnership. As described in (Hay et al., 2017), leveraging remote resources ensures continued support independent of local, competing response priorities and/or connectivity issues during crisis. Remote skillsets supplement those unavailable locally, building resourcefulness, and relieves the overwhelmed, building agility and autonomy. In contrast, accommodating the surge of volunteers can be resource intensive, and uninhibited by geographical and travel cost restrictions, the digital surge can be unmanageable. Responders risk overwhelming their own resources to manage this relationship. Study participants talked about the challenges of meeting capability and capacity requirements and how, if needs are unmet, delivery may not be to standard, or fulfil the operational need. Volunteers may lack the technical knowledge, skills or language needed, or the time required to achieve needed outcomes. Outputs may not be compatible with organisations data standards and file formats. Finally, responders risk losing this capacity over time. Digital burnout to volunteer fluidity implies volunteer numbers may decrease over time and subsequently the reliability and capability to produce outputs needed.

- DRN → community – Communities develop attributes like agility and autonomy, but also face reliability and exclusion risk through DRN partnership. Periodically, communities create local DRNs. Local DRNs connect the local digital volunteer response with the local authorities managing the response (Phillips and Verity, 2016). Engaging authorities in the community-led response builds unification and coordination between groups, resourcefulness through aggregating mandated and emerging responders, and community autonomy. DRN partnership can also assist local capacity building. Participants asserted that DRN initiatives teach new skills and build employability. For example, Humanitarian OpenStreetMap deployed and trained over 300 people on mapping and assessing techniques during the Haiti earthquake in 2010 (Soden and Palen, 2014). In contrast, DRNs typically lack a formalised mandate implying support is intermittent or unreliable. Remote support may be unfamiliar with the local risk context. Outcomes may be skewed or incongruent with the local needs and risk context. A digital response assumes specific connectivity requirements, from technical literacy to communications infrastructure. Communities risk exclusion from their own response without these enabling resources. Participants explained experiences with internet shutdowns. Whether internet loss is accidental or intentional, no connectivity implies the loss of support entirely. One participant also discussed cases where individuals are more engaged in remote digital response than their local physical one. The risk emerges of detracting local resources from their own local response.
- Local DRN ←→ global DRN – The transmission between global and local DRNs was perceived to make local and global DRNs more resilient, with few risks mentioned. Beyond affiliation benefits discussed earlier, the local DRN can offload local demand during crisis by offsetting localised tasks (e.g. long-term planning) onto global resources and tapping into already existing tools and protocols to guide local interoperability. Global DRNs can be used as a conduit to international and regional contacts neighbouring the affected region for assistance. Perceived risk to local DRNs was linked to leadership. Specifically, the risk of informal leadership influence from the global to the local context was raised, combined with incompatible leadership and unclear delegation of responsibility between hubs. In contrast, global DRNs build resilience through local DRN partnership by gaining access to pre-existing established local, trusted contacts and enhanced situational understanding. The local DRNs can play the lead and the global DRN can support, leaving the response, recovery and broader resilience development in the hands of those more invested in the longer-term. Local DRNs, however, can be a risk if not vetted properly. A rogue or questionable purpose in an affiliated DRN, for example, could pose severe risk to the reputation of the network.

Leadership and governance

Profile

The leadership and governance of a network sets the foundation for the culture, purpose and interactions within the network. Most DRNs use an informal, horizontal leadership style. The central hub may include one static leader to multiple dynamic leaders or coordinators rotating annually. Often leaders do not occupy the position because they are elected or qualified. They assume the role as a conduit between a funder and grantees as it is their turn in a rotating schedule, or simply because they started the initiative. Leaders/coordinators work in tandem with hub members to initiate, build and sustain the network. Hub members may be members that are more engaged than others, representatives of the affiliated network organisations to those that are funded over unfunded. Decision making is frequently through an open, distributed collaborative process managed at the central hub or throughout the network as a whole. For example, the Occupy movement (a movement catalysed through online connectivity) used general assemblies (GAs) — face-to-face offline meetings where anyone is free to take part in moving the movement forward (Boler and Phillips, 2016). For networks that were strictly digital, decisions were made using online, open-source decision-making software. In other cases, some decisions were made by central decision makers and others collectively. Frictions on risk and resilience emerge around decentralised leadership and decision making, and the legalities of associated DRN activities (Figure 13).



	ATTRIBUTES	MACRO	MESO	MICRO	RISK	RESILIENCE
DYNAMIC	**CULTURE, LEADERSHIP & GOVERNANCE** Leadership style, autonomy vs. dependence, collaboration vs. isolation, polices & regulations	Culture, Leadership & Governance in Network	Culture, Leadership & Governance in Clusters	Influence of Network on Node, and Node on Network	**Decentralized Leadership & Decision Making**	
					Leadership may not be sustainable; decisions may not be representative; voices may be supressed; informal leadership structure may overpower formal	Equal voice and collective decision making; autonomy; space for emergence, innovation and collaboration
					Legalities	
					Increased liability and lack of familiarity with legal implications; legislation, laws and regulations can restrict action; blacklisting	Ability to be emergent; rapidity and agility in operations

Figure 13 Inherent risk and resilience frictions for centrality and connectivity for leadership and governance
Source: Author

Risk and resilience

Decentralised leadership and decision making

The DRN approach to leadership builds collaborative and emergent qualities into the fabric of the network yet risks sustainability and fair decision making. Equal voice and collective decision making mixed with the freedom to act autonomously, creates the space for emergence, innovation, and collaboration (Evans and Boyte, 1986; Weick and Sutcliffe, 2011). In situations where leadership is assumed from starting an initiative, that leadership may be unsustainable if that individual is overwhelmed or unable to commit the time required to sustain an initiative. Reflecting on their own experience, one participant emphasised leaders must be prepared to commit for one year and play a supportive role for the following two years (at a minimum) for a DRN to be sustainable. Beyond tool constraints highlighted earlier, the voting structure implies decisions may not be representative. Some networks allow one vote per organisation. With this setup, voting power is imbalanced if comparing one vote from a large organisation that is heavily active versus one from a small one with sporadic involvement. Conversely, in verbal decision-making events, whether online or offline, participants remarked on the imbalance of small and big players. Without formal regulation or rigorous voting mechanisms, the voices of the more dominant can easily outweigh the passive ones.

Accommodating legalities

Despite the resilience benefits outlined, participants discussed legal frictions with ad-hoc organisations. Operations ‘outside the system’ grant DRNs the freedom and rapidity to emerge and the agility to transform as needed without the weight of compliance requirements and bureaucratic protocols slowing them down. Yet, members and the broader network face liability risk. Robson (2012) explains the notion of tort (‘civil wrong’) liability for digital volunteers linked to mistaken or neglectful actions like spreading false information or failing to act when there is a ‘duty to rescue’. He highlights the legal responsibility digital volunteer organisations have to their volunteers, and explains risks linked to jurisdictional law in cyberspace. Sometimes, he explains, a digital volunteer can be drawn into court under an unexpected law and unexpected place. And many of the existing laws and protections fail to account for digital volunteer groups. Second, the design and implementation of legislation, laws and policies can directly impact network activities. One participant explained ‘Article 19’ in Pakistan, an effort to prohibit YouTube in Pakistan (Article 19, 2013), drastically constrained the space to tackle freedom of expression online. Similarly, anti-terrorist laws increase risk of digital surveillance. Deibert (2013) reports, for example, that one billion internet users live in countries with regularly censored internet. Third, organisations can be blacklisted. One participant explained they were denied a bank account to receive donor funding as a means to suppress operations. Unable to pay for activities or staff salaries otherwise, they were forced to partner with a local organisation as an executor to accept and distribute their funds. Yet, this partner requested compensation limiting the full dissemination of funds to the organisation, while also adding to network vulnerability. The interviewee remarked 'it's like having two people holding onto one life vest'.

Existing risk treatments and resilience development

The capability to address expected risk but also manage the unexpected can be developed through the development of resilience (Weick and Sutcliffe, 2011). In lieu of identifying treatments for individual risks highlighted in this study, this section outlines strategies for the development of broader DRN resilience. Building on previous discussion, observations and participant examples are provided along five themes: resilient purpose, administration, membership, partnership and funding.

Resilient purpose

Identify if resilience is needed, and if so, to what, of what and for whom

A clear vision is required of what needs to be made resilient. Independent of context, the development of resilience starts with a clear understanding 'of what, to what and for whom' resilience is being developed (Cote and Nightingale, 2012). Not all networks require resilience. Some require resilience but not sustainability. Ad-hoc networks that form during disasters, like Occupy Sandy for example, may rise for a specific purpose and fall once that purpose is achieved. These networks may require resilience temporarily but may also thrive in their ability to be temporary. Networks, like the DHNetwork, that strive to become an embedded resource in disasters, would require indefinite resilience and sustainability.

Administration

Ensure sustainable leadership, a shared purpose and identity, legal capacity and the right tools

The administration of the network must build a foundation that will sustain a network. Leadership must build and spread the purpose (McAdam et al., 2004; Phillips et al., 2016). As reported in Phillips et al., 2016, they should create a shared identity by encouraging individual perspectives, a group identity to perform collaborative tasks, establish clear communications and responsibilities, set cultural norms and develop policy and guidance to do so. They must be committed – at least one to two years and support the network for a third year (Phillips and Verity, 2016). Leadership can be diversified. One network uses three leaders rotating annually from a 'board' of network members that works in tandem to coordinate the network. They should take risk seriously. Participants highlighted the need for legal capacity. Robson (2012) identifies some of the emerging protections for digital volunteer groups including the Volunteer Protection Act enacted in 1997, as well as liability-reducing strategies. Open data protocols are needed to align DRN outputs with client systems. Participants also emphasised the need for tools and resources for learning about and treating risk. Often, what exists is designed for corporate clients on corporate budgets. Little support documentation is digestible for small-scale initiatives with few human resources and little to no funds.

Membership

Use organisational membership, build trust, encourage collaboration, build a code of conduct, micro task

Sustainable and reliable membership is needed for a network to exist. Fluidity can be addressed with organisational instead of individual membership. Individuals can change within an organisation, but an organisational relationship will remain. As noted, these memberships must still be monitored for internal organisational fluidity. Access to a network can be through a double-vetting process, where individuals are accepted if they are known and trusted by two or more members. Member outflow can be deterred through building trust and strengthening relationships. This can be done through mimicking offline interaction online, emulating face-to-face interactions through events like a 'virtual beer', or actually creating opportunities for offline face-to-face encounters and group socialisation (Phillips et al., 2016). Interoperability can be built through collaborative projects. Conflict can be mitigated through 'safe spaces' and support systems or, even, digital counsellors to moderate discussions and intervene when necessary. Systems and procedures can be established like a code of conduct to govern member interactions, create a positive culture while mitigating potential polarisation, conflict and/or cyberbullying. In the digital humanitarian space, engagement can be enhanced through micro-tasking – breaking down network requests into small, tangible pieces – to allow volunteers to step in and out of the response easily, accomplish something and gain a sense of achievement (Phillips et al., 2016).

Partnerships

Build local DRNs, leverage rapid response networks

DRNs may benefit from internal segmentation and drawing on expertise. Local DRNs should be used to develop resilience in global DRNs and communities (Phillips and Verity, 2016). DRNs should also familiarise and leverage existing rapid response DRNs. Whether a humanitarian or advocacy initiative, there are DRNs that exist for the sole purpose of supporting DRN networks and members at risk. Initiatives exist like the Rapid Response Network (RaReNet) who developed a digital first-aid kit to support the adoption of digital security measures or Digital Defenders that deploy and provide digital security training.

Funding

Use alternate compensation or seed funding, fund collaboration, ensure funders acknowledge risk

Discussions about funding revealed approaches to manage the process of getting funded, sustaining funding and operations without funding. Networks with limited funds used alternate forms of compensation to sustain engagement. Measures included sending members to conferences and/or granting a stipend for these types of activities, celebrating their names, and ensuring they get thanked. In many cases, recognition alone facilitates sustainability (Phillips et al., 2016). Others diversify funding sources through seed funding or multiple grants with different donors. Some networks only fund one administrative person to handle any administrative and sustainability aspects of the network organism (mentioned previously). Some grant funding based on collaboration between members, a mechanism that builds internal connectedness while relieving hub dependency. One network described their idea of developing a parallel not-for-profit (NPO) organisation to act as a subsidiary funding body for their network. The NPO would act independently to support and fund network activities without imposing the cultural and political implications of directly injecting funding into the network itself. Some networks preferred not to receive any funding, as they felt it would interfere with network dynamics and members voices, as well as the intrinsic motivations for joining and engaging with the network. Yet many interviewees felt funding was necessary for continuity. They said funding to cover the cost of tools, one admin person and/or coordinators is needed at minimum. Participants also highlighted the need for funders to embed risk management into their thinking. Specifically, they need to mandate adoption of risk management practices in the funding requirements, while creating the space in the funding process to allocate funds to risk treatments and resilience development practices.

Next steps

Further study of risk and resilience in DRNs is needed. DRNs are a novel concept but, as time passes, more data is becoming available. Experiences with humanitarian-focused and advocacy-focused DRNs showed much overlap between both types of operations, but in application they envision themselves as separate and act accordingly. Further study is needed to contextualise the intersection between these networks and develop mechanisms to bring these communities together.

In disaster situations, the demand for social media monitoring and analysis continues to increase yet agencies fail to engage DRN resources. Research is needed to contextualise the impact of DRN partnerships, and policy is needed to build and sustain these relationships, as well as outline interoperability guidelines. Further study is also needed to evaluate the impact of DRNs on communities, specifically in the ability to serve but also support community and develop broader resilience. The idea of local DRNs remains a novel concept and poses potential for contributing to resilience of responders and communities. The notion of local DRNs and/or collaboration with DRNs as a means to empower communities and shift the disaster response culture from a 'saviour to enabler' approach (Phillips, 2016) emerged during this research and merits further study. Funders must begin to account for and fund risk management and resilience development was a recurring theme in this study. Subsequently, research is needed to identify mechanisms for doing so, as well as how to generate resilience across funded networks.

Finally, a concrete process for the development of resilience in DRNs is needed. Combined with Phillips (2015), this study uses the NOR framework to create a holistic understanding of risk (internal and external) and inherent resilience in networks but does not prescribe a methodology for how to develop resilience based on this understanding. Application of all stages of the NOR framework is needed to achieve this. Subsequently, this article sets the foundation for subsequent study of using the NOR framework to demonstrate resilience development in DRNs.

Conclusion

Extending Phillips (2015), this study has developed a holistic risk profile for DRNs. This has been accomplished by first describing DRNs and their importance, the known all-hazards risk landscape (external risk) and the need for better risk understanding. The argument has been made that risk is better understood if inherent risk is assessed and balanced with inherent resilience of these networks; and that a networked approach must be used. Data was collected through case study of two primary DRNs (the DHNetwork and the Cyber Stewards Network), complementary study (Phillips et al. 2016) and informal involvement with other DRNs. The NOR framework was used to provide the approach for characterising these networks (Phillips and Hay, 2017) and assessing embedded resilience. Discussion was divided along two network dimensions and associated attributes: structural (topology, boundaries, scale and scope, centrality and connectivity) and dynamic (state, evolution and lifespan, exchange, leadership). The DRN context was explained for each attribute and frictions around inherent risk and resilience are described through perceptions of research participants. Resilience development strategies and areas for further research have been proposed.

This paper has shown how technology is enabling citizens to collaborate and coordinate on new levels, often beyond the understanding of those that may benefit most. The need is now to shift from 'saviour to enabler' (Phillips, 2016), and leverage these digital opportunities. Doing so begins with shifting more attention to understanding DRNs and identifying ways in which to collaborate. Measures must be identified and applied to minimise and manage risk that members and organisations may face in this process, and broader resilience must be developed within these networks, between the communities they support and the responders they enable. This study sets the foundation for this understanding and provides the context for asking the right questions in moving forward to consider and develop networked resilience across citizen-driven and official response systems.

References

Article 19 (2013) *Pakistan: Telecommunications (Re-organization) Act*, http://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf (accessed 20 May 2017).

Article 19 / IFEX (2012) 'Nepal. Mission finds worsening law reform, impunity and self-censorship', 28 February 2012, https://www.ifex.org/nepal/2012/02/28/media_mission/ (accessed 20 May 2017).

Asher, S. (2015) 'How "crisis mapping" is helping relief efforts in Nepal', *BBC News*, 6 May 2015, http://www.bbc.com/news/world-asia-32603870 (accessed 20 May 2017).

Ashraf, C. (2013) 'The psychological strains of digital activism', *Global Voices Advocacy*, 17 April 2013, https://advox.globalvoices.org/2013/04/17/the-psychological-strains-of-digital-activism/comment-page-2/ (accessed 20 May 2017).

Barabási, A. L. (2003) *Linked*, New York, Basic Books.

Barabási, A. L. and Bonabeau, E. (2003) 'Scale-free networks', *Scientific American*, 288, 50–59.

BBC Media Action (2012) *Still left in the dark?*, Policy Briefing #6, March 2012, http://downloads.bbc.co.uk/mediaaction/policybriefing/bbc_media_action_still_left_in_the_dark_policy_briefing.pdf (accessed 20 May 2017).

Berkes, F., Folke, C. and Colding, J. (2000) *Linking social and ecological systems*, Cambridge, Cambridge University Press.

Besant, A. (2005) 'Nepal suffers brutal return to a feudal past', *The Guardian*, 11 February 2005, 1–2.

Boler, M. and Phillips, J. (2016) 'Entanglements with media and technologies in the occupy movement', *The Fibreculture Journal*, 26, 1–32, http://twentysix.fibreculturejournal.org/fcj-197-entanglements-with-media-and-technologies-in-the-occupy-movement/ (accessed 20 May 2017).

Boon, H. J., Cottrell, A., King, D., Stevenson, R. B. and Millar, J. (2011) 'Bronfenbrenner's bioecological theory for modelling community resilience to natural disasters', *Natural Hazards*, 60(2), 381–408.

Borgatti, S. P. (2005) 'Centrality and network flow', *Social Networks*, 27(1), 55–71.

Bristow, D. (2015) 'Asset system of systems resilience planning: the Toronto case', *Infrastructure Asset Management*, 2(1), 15–22.

Bristow, D. and Hay, A. H. (2014) *Balancing protection and resilience*, Centre for Resilience of Critical Infrastructure, Toronto, University of Toronto.

Bronfenbrenner, U. (1994) 'Ecological models of human development', *International Encyclopedia of Education*, 3(2), 1–7.

Capelo, L., Chang, N. and Verity, A. (2012) *Guidance for collaborating with volunteer and technical communities*, Digital Humanitarian Network, https://www.humanitarianresponse.info/en/applications/tools/toolbox-item/guidance-collaborating-volunteer-and-technical-communities-vtcs (accessed 20 May 2017).

Citizen Lab (2013) 'Cyber stewards join the dialogue', 10 April 2013, http://www.cyberdialogue.ca/2013/03/cyber-stewards-join-the-dialogue/ (accessed 20 May 2017).

Cote, M. and Nightingale, A. J. (2012) 'Resilience thinking meets social theory: situating social change in socio-ecological systems (SES) research', *Progress in Human Geography*, 36(4), 475–89.

Deibert, R. (2013) *Black code. Inside the battle for cyberspace*, Toronto, Signal.

DHNetwork (2015) Digital Humanitarian Network, 11 November, http://digitalhumanitarians.com/about (accessed 3 March 2014).

Dunbar, R. I. M. (1998) 'The social brain hypothesis', *Evolutionary Anthropology: Issues, News, and Reviews*, 6(5), 178–90.

El-Bermawy, M. M. (2016) 'Your filter bubble is destroying democracy', 18 November, *Wired*, https://www.wired.com/2016/11/filter-bubble-destroying-democracy/ (accessed 20 May 2017).

Erdős, P. and Rényi, A. (1959) 'On random graphs 1', *Publicationes Mathematicae*, 6, 290–97.

Evans, S. and H. Boyte (1986) *Free spaces: the sources of democratic change in America*, New York, Harper and Row.

Freeman, J. (1972) 'The tyranny of structurelessness', *Berkeley Journal of Sociology*, 17, 151–64.

Freeman, L. C. (1979) 'Centrality in social networks conceptual clarification', *Social Networks*, 1(3), 215–39.

Granovetter, M. S. (1973) 'The strength of weak ties', *American Journal of Sociology*, 78(6), 1360–80.

Granovetter, M. S. (1983) 'The strength of weak ties: a network theory revisited', *Sociological Theory*, 1(1), 201–33.

Gyawali, S. (2014) 'Censorship in Nepal: forms and evolution', *Fair Observer*, 9 June, https://www.fairobserver.com/region/central_south_asia/censorship-in-nepal-forms-evolution-73208/ (accessed 20 May 2017).

Hay, A. H. (2013a) *Operational survival: 1: putting resilience at the core of infrastructure planning*, London, Explora Research Limited.

Hay, A. H. (2013b) 'Surviving catastrophic events: stimulating community resilience', in *Infrastructure risk and resilience: transportation*, Stevenage, Institution of Engineering and Technology, 41–46.

Hay, A. H. (2016) 'The incident sequence as resilience planning framework', *Infrastructure Asset Management*, 3(2), 55–60.

Hay, A. H., Gómez-Palacio, A. and Martyn, N. (2017) 'Planning resilient communities', in I. Linkov and J. M. Palma-Oliveir (eds) *Resilience and risk: methods and application in environment, cyber and social domains*, Dordrecht, Springer, 313–26.

Hopkins, R. (2009) 'Resilience thinking', *Resurgence*, 257, 12–15.

Hosangar, K. (2016) 'Blame the echo chamber on Facebook. But blame yourself, too', *Wired*, 25 November, https://www.wired.com/2016/11/facebook-echo-chamber/ (accessed 10 May 2017).

IFRC (International Federation of Red Cross) (2013) *World disasters report: focus on technology and the future of humanitarian action*, Geneva, International Federation of Red Cross and Red Crescent Societies.

Jeanson, R., Fewell, J. H., Gorelick, R. and Bertram, S. M. (2007) 'Emergence of increased division of labor as a function of group size', *Behavioral Ecology and Sociobiology*, 62(2), 289–98.

Johnson, S. (2012) *Emergence: the connected lives of ants, brains, cities and software*, New York, Scribner.

Kaufman, S. (2012) 'Complex systems, anticipation, and collaborative planning for resistance', in B. E. Goldstein (ed.) *Collaborative resilience: moving through crisis to opportunity,* Cambridge MA and London, MIT Press, 61–98.

Lim, M. (2012) 'Clicks, cabs, and coffee houses: social media and oppositional movements in Egypt 2004–2011', *Journal of Communication*, 62(2), 231–48.

McAdam, D., Tarrow, S. and Tilly, C. (2004) *Dynamics of contention*, Cambridge, Cambridge University Press.

McConney, P. and Phillips, T. (2011) 'Collaborative planning to create a network of fisherfolk organizations in the Caribbean' in Goldstein (ed.), 207–30.

McManus, S., Seville, E., Vargo, J. and Brunsdon, D. (2009) *Resilience management: a framework for assessing and improving the resilience of organisations* (Research report), Christchurch, NZ, Resilient Organisations.

Meadows, D. (2008) *Thinking in systems: a primer*, White River Junction, Chelsea Green.

Medina, R. and Hepner, G. (2008) 'Geospatial analysis of dynamic terrorist networks', in I. A. Karawan, W. McCormack, and S. E. Reynolds (eds) *Values and violence: intangible aspects of terrorism*, New York, Springer, 151–67.

Meier, P. (2011) 'An open letter to the good people at Benetech', *iRevolutions*, 18 April, https://irevolutions.org/2011/04/18/open-letter-benetech/ (accessed 10 May 2017).

Meier, P. (2015a) 'UAVs and humanitarian response', in *Drones and aerial observation: new technologies for property rights, human rights, and global development. A primer,* online edition, 103, 1–6.

Meier, P. (2015b) *Digital humanitarians: how big data is changing the face of humanitarian response*, Boca Raton, London and New York, CRC Press.

Naug, D. (2009) 'Structure and resilience of the social network in an insect colony as a function of colony size', *Behavioral Ecology and Sociobiology*, 63(7), 1023–28.

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F. and Pfefferbaum, R. L. (2007) 'Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness', *American Journal of Community Psychology*, 41(1–2), 127–50.

Orloff, L. (2011) *Managing spontaneous community volunteers in disasters. A field manual*, Boca Raton, London and New York, CRC Press.

Phillips, J. (2015) 'Exploring the citizen-driven response to crisis in cyberspace, risk and the need for resilience', Paper presented at 2015 IEEE Canada International Humanitarian Technology Conference (IHTC2015), 31 May–4 June.

Phillips, J. (2016) 'Enabling local communities through Digital Response Networks', *Humanitarian Law and Policy*, 19 May, http://blogs.icrc.org/law-and-policy/2016/05/19/enabling-local-communities-digital-response-networks/ (accessed 10 May 2017).

Phillips, J. and Hay, A. H. (2017) 'Building resilience in virtual and physical networked operations', *Infrastructure Asset Management*, 4(2), 50–67.

Phillips, J. and Verity, A. (2016) *Guidance for developing local digital response networks (DRN)*, Digital

Humanitarian Network, http://digitalhumanitarians.com/resource/guidance-creating-local-digital-response-network-drn (accessed 10 May 2017).

Phillips, J., Robinson, L., Bishop, E. B., Daya, S., Gladstone, N., Ko, V., Loewen, P., Sim, A., Wilmot, C. and Wollenberg, S. (2016) 'What motivates citizens to participate?', *The Digital Public Square*, 17, 1–45, https://digitalpublicsquare.com/2016/03/31/what-motivates-citizens-to-participate/ (accessed 23 May 2018).

Razorfish Buzzcut (2013) 'Occupy Sandy's happy hackers', *Razorfish Buzzcut*, http://razorfish-buzzcut.tumblr.com/post/41564190632/occupy-sandys-happy-hackers (accessed 3 March 2014).

Reidy, E. (2017) 'How Facebook helps to reveal the fate of missing Syrian refugees', *Wired*, 9 April, https://www.wired.com/2017/04/locating-missing-refugees-social-media/ (accessed 10 May 2017).

Rezwan. (2012) 'Outrage as Facebook post leads to arrests in India', *Global Voices*, 9 November, http://globalvoicesonline.org/2012/11/19/outrage-in-india-on-arrest-of-girls-for-facebook-post/print/ (accessed 10 April 2013).

Robson, E. S. (2012) *Responding to liability: evaluating and reducing tort liability for digital volunteers*, Washington DC, Woodrow Wilson International Centre for Scholars, https://www.wilsoncenter.org/publication/responding-to-liability-evaluating-and-reducing-tort-liability-for-digital-volunteers (accessed 20 May 2017).

Sage, A. P. and Biemer, S. M. (2007) 'Processes for system family architecting, design, and integration', *IEEE Systems Journal*, 1(1), 5–16.

Sage, A. P. and Cuppan, C. D. (2001) 'On the systems engineering and management of systems of systems and federations of systems', *Information, Knowledge, Systems Management*, 2(4), 325–45.

Seville, E., Van Opstal, D. and Vargo, J. (2015) 'A primer in resiliency: seven principles for managing the unexpected', *Global Business and Organizational Excellence*, 34(3), 6–18.

Soden, R. and Palen, L. (2014) 'From crowdsourced mapping to community mapping. the post-earthquake work of OpenStreetMap Haiti', COOP 2014: Proceedings of the 11th International Conference on the Design of Cooperative Systems, 27–30 May 2014, Nice (France), 311–26.

Stevenson, J. R. (2014) *Organizational resilience after the Canterbury earthquakes: a contextual approach* (Phd thesis), Christchurch, New Zealand, University of Canterbury.

Tremayne, M. (2013) 'Anatomy of protest in the digital era: a network analysis of Twitter and Occupy Wall Street', *Social Movement Studies*, 13(1), 110–26.

UAViators (2017) Humanitarian UAV network, http://uaviators.org/ (accessed 12 April 2017).

Wall, I. (2016) 'Could mapping tech revolutionise disaster response?', *The Guardian*, 25 April, https://www.theguardian.com/global-development-professionals-network/2016/apr/25/could-mapping-tech-revolutionise-disaster-response?CMP=share_btn_tw (accessed 20 May 2017).

Weick, K. E. and Sutcliffe, K. M. (2011) *Managing the unexpected*, San Francisco, John Wiley.

Whittaker, J., McLennan, B. and Handmer, J. (2015) 'A review of informal volunteerism in emergencies and disasters: definition, opportunities and challenges', *International Journal of Disaster Risk Reduction*, 13, 358–68.

Yin, R. K. (2009) *Case study research*, Thousand Oaks, Sage Publications.

Zolli, A. and Healy, A. M. (2013) *Resilience: why things bounce back*, New York, Simon and Schuster.