A Taxonomy of Network Challenges

Egemen K. Çetinkaya* and James P.G. Sterbenz*†
*Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS, 66045, USA
{ekc, jpgs}@ittc.ku.edu
† School of Computing and Communications (SCC) and InfoLab21
Lancaster LA1 4WA, UK
jpgs@comp.lancs.ac.uk
www.ittc.ku.edu/resilinets

***Abstract*—Communication networks, in particular the Internet, face a wide spectrum of challenges that can disrupt our daily lives. We define challenges as adverse events triggering faults that eventually result in service failures. Understanding these challenges accordingly is essential for the improvement of the current networks and for designing Future Internet architectures. In this paper, we present a taxonomy of network challenges based on past and potential events. Moreover, we describe how the challenges correlate with our taxonomy. We believe that such a taxonomy is valuable for evaluating design choices as well as establishing a common terminology among researchers.**

***Keywords*-Resilience, survivability, disruption tolerance, dependability, performability, security; challenge, fault, error, failure; diversity, redundancy; attack, disaster**

I. Introduction and Motivation

Society relies on communication networks extensively. However, communication networks in general, and the Internet in particular, are susceptible to a variety of challenges. Network service failures disrupt daily lives and cost financial damages. Moreover, network disruptions have the potential to result in human losses. It is therefore essential to build networks that are resilient against a wide spectrum of challenges.

A *challenge* is a characteristic or condition that may manifest as an adverse event or condition that impacts the normal operation [1]. A challenge triggers *faults*, which are the hypothesized cause of *errors*. Eventually, a fault may manifest itself as an error. If the error propagates it may cause network services to *fail* [2]. In the context of communication networks, these challenges include the following: human errors, malicious attacks, large-scale disasters, environmental challenges, unusual but legitimate traffic, failure of dependent infrastructures, and socio-political and economical events.

Establishing a correct threat model is essential for the cost efficient and resilient system design. Therefore, better understanding of the challenges and possible impacts on the networks and services is essential for improving existing networks and designing the Future Internet. Categorising communication network challenges can help us understand the impact of disruptions, improve existing network resilience, as well as aid in designing the Future Internet architectures and protocols. A taxonomy of challenges and their correlation can help assess resilient designs and mechanisms. While the IFIP 10.4 working group *fault taxonomy* has focused on *computer systems* [3], we further expand this taxonomy and systematically develop our taxonomy with an emphasis on *challenges in network systems*. Moreover, establishing a common terminology assists cooperation among researchers.

The rest of the paper is organised as follows: We present the ResiliNets strategy in Section II. Past known challenges and potential challenges are summarised in Section III. Characteristics and taxonomy of network challenges are presented in Section IV. Finally, we conclude our paper in Section V.

II. Resilience Strategy

The ResiliNets architectural framework [1], [4] provides a strategy and set of principles to alleviate the impact of challenges. The challenge tolerance of networks can be increased via the ResiliNets strategy [1], [4], formalised as D^2R^2+DR. Real-time D^2R^2 mechanisms include defence, detection, remediation, and recovery. Long-term DR mechanisms include diagnosis and refinement.

The first step for preserving the resilience of a network involves *defensive* measures. Defence mechanisms can be passive or active. Passive defence primarily involves structural improvement of the network. Two such mechanisms are placing redundant components within the network in order to achieve fault-tolerance and increasing the diversity of the network to mask correlated failures for survivability. An example of an active defence includes firewalls that filter anomalous traffic. Next, *detection* is required to discover if the defensive measures have been penetrated. After detection of abnormal conditions, the effects of the adverse event or condition should be *remediated*, and once the system is remediated the system provides the best possible level of service constrained by available resources. *Recovery* involves bringing the operations to the original and normal state including redeploying destroyed infrastructure. The long-term DR loop involves diagnosis as a first step. Diagnosis involves localisation of faults. Once the faults are identified by root-cause analysis, the system can be *refined* to improve future defence, detection, remediation, and recovery (D^2R^2) in the future for a given challenge.

III. Past and Potential Challenges

In this section we summarise a wide spectrum of challenges and their impacts and group them into major categories for convenient description. We *italicise* the challenge categories that will be covered in Section IV. The list of selected major challenges include:

Large-scale disasters: Communication networks have become dysfunctional due to *large-scale natural disasters*. The 2006 Taiwan earthquake [5], the 2008 Wenchuan earthquake [6], and the 2011 Japan earthquake [7] caused major disruptions to *hardware* and *links* in the earthquake-hit *regions* [7], [8]. Hurricanes caused significant disruptions to communication networks as well [8]–[11]. Natural disasters are not only caused by *terrestrial* and *meteorological* events, but also they can be caused by *cosmological* events such as geomagnetic storms [12], [13].

Human-made disasters can be the result of simply ignoring an early warning in a system's operation or can be the result of a malicious act such as terrorism. *Target*, *objective*, and *intent* of the human actions can also vary. A pandemic is a spread of disease that can impact large populations *globally*. In the case of biological warfare, it originates with a *malicious objective* and *deliberate intent*. The potential impact of a *long-lived* influenza pandemic on telecommunications and information technology could be *catastrophic* [14].

Socio-political and economic challenges: Social, political, and economic challenges caused by deliberate human actions can threaten resilient communication [15]. Canonical examples include collateral damage to communication networks due to *terrorism* [16], nationwide Internet outage due to *political* decisions [17], and peering disputes to gain *economical* advantage in markets [18].

Dependent failures: Critical infrastructures, such as the Internet and the power grid, increasingly rely on each other [19]. During the Northeast US blackout of 2003, the average outage duration for large network service providers ranged from 12 to 33 hours [20]. The impact of the blackouts are *regional*, rather than global in scope [20], [21].

Dependent failures within an infrastructure can result in cascading failure. Consider the BGP (Border Gateway Protocol) prefix hijacking that occurs when an AS announces an IP address prefix (i.e. destination) that it does not belong to itself. If the upstream provider does not filter the bad routes, incorrect prefixes poison the BGP global routing table, resulting in a *cascading failure*. When a prefix is hijacked, it can cause a blackhole effect in which packets don't reach the destination, resulting in a denial of service attack. Between 1997 and 2009, there were 15 high-profile prefix hijacking events according to a study compiled from NANOG (North American Network Operators' Group) mailing list archives [22].

Human errors: *Non-malicious* human action such as misconfiguration errors is a challenge to networks. Misconfiguration of BGP and DNS result in large-scale network disruptions [23], [24]. According to a 21-day study, BGP misconfiguration errors are *short-lived* (less than a day) and 0.2–1.0% of BGP table entries are affected by the misconfigurations [24]. In addition to the failures in the Global Internet, 50% of the outages in PSTN (public switch telephony network) are due to human errors [25]. Moreover, *incompetence* of operational personnel or designers can result in catastrophic failures. For example, although the Hinsdale central office fire was not human initiated, the fact that the operator initially ignored the alarm resulted in the late arrival of the firefighters, which in turn resulted in severe fire damage [26], [27]. From a security point of view, most threats come from humans [28]; however, designing the systems to tolerate human errors is difficult [29], and requires redundancy, diversity, and heterogeneity [30].

Malicious attacks: *Deliberate* attempts to disrupt service, such as targeted hardware and software attacks, are challenges to networks. Furthermore, damage may be worse if the attack targets *protocols*, since the impact can be global. Malware such as Morris, Code Red, Nimda, Blaster, and Slammer have been the source of the significant Internet disruptions [31].

Unusual but legitimate traffic: Flash crowds are events that are sudden and are due to simultaneous access request of multiple clients to a target. On the day of the 9/11 terrorist attacks on 11 September 2001, major news websites became unresponsive after the second plane crash into the WTC (World Trade Center) [16]. The demand for the CNN.com website increased by an order of magnitude on 9/11 [32].

Environmental challenges: Challenges that are inherent to the communication environment. Examples include mobility of nodes in an ad-hoc network, weakly connected channels, and unpredictably long delays in the *wireless domain* [33].

IV. Challenge Models

In this section, we provide the challenge models. First, we review the challenge → fault → error → failure chain and its relationship with the ResiliNets strategy. Next, we discuss the spatial and temporal impact of challenges. Based on the challenges we identify, we provide a taxonomy of challenges. Finally, we provide a matrix representing how these challenges are correlated with our taxonomy.

A. Challenge → Fault → Error → Failure Chain

A *challenge* is an event that impacts normal operation of the network [4]. A challenge triggers *faults*, which are the hypothesised cause of *errors*. Eventually, a fault may manifest itself as an error. If the error propagates it may cause the delivered services to *fail* [2]. The fault → error → failure chain relationship has been extensively studied by the IFIP 10.4 working group [2], [34]. We note that while the IFIP 10.4 taxonomy focused on *faults* in computer systems, our focus in this paper is taxonomy of *challenges* in communication networks. Challenges to the normal operation of networks include unintentional misconfiguration or operational mistakes, malicious attacks, large-scale disasters, environmental, and deliberate human actions driven by social, political, and economic agendas [4], [33], [35]–[39]. The challenge, fault, error, failure chain relationship and along with the ResiliNets strategy (cf. Section II) is shown in Figure 1.

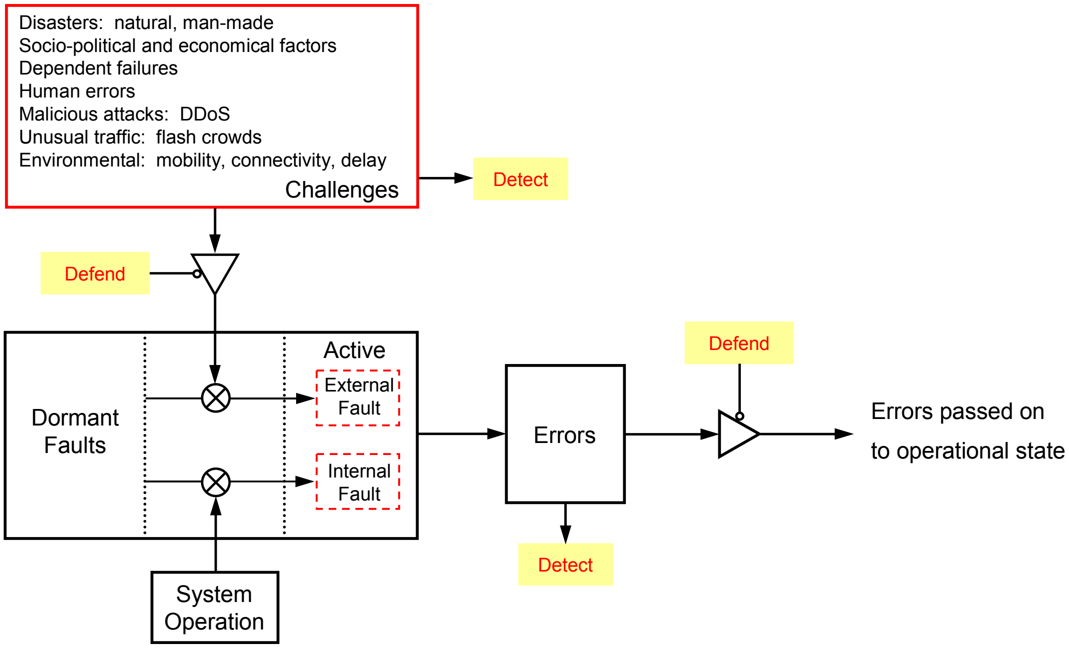
Disasters: natural, man-made
Socio-political and economical factors
Dependent failures
Human errors
Malicious attacks: DDoS
Unusual traffic: flash crowds
Environmental: mobility, connectivity, delay
Challenges
Detect
Defend
Active
Dormant Faults
External Fault
Internal Fault
Defend
Errors
Errors passed on to operational state
Detect
System Operation

Fig. 1. Challenge → fault → error → failure chain

Challenges have primary impact on the defence and detection aspects of the ResiliNets D^2R^2+DR strategy. We can defend against challenges passively by building diverse structural components and technologies, as well as using redundant components [30]. Furthermore, we can strengthen networks by installing active defence mechanisms such as firewalls. However, building a 100% resilient system is not practical due to cost constraints. For example, while a full mesh interconnection provides maximum robustness to link failures, it is prohibitively expensive to deploy. As a result, defences may be penetrated and challenges activate dormant faults in the system. We note that system operation can also activate the faults; for example, a particular input pattern can activate faulty software code [2]. Some challenges can be detected by using in-network mechanisms, such as signature-based detection against known attacks or behaviour-based detection against flash crowds. Out-of-network detection includes mechanisms that are outside the boundary of the network system. For example, weather storm tracking or an early warning system against an EMP (electro magnetic pulse) weapon can be used as an input to a predictive algorithm to utilise alternative paths [40]. On the other hand, it is very difficult to detect some challenges, such as operator mistakes, before they result in failure.

Faults are hypothesised causes of errors [2], and once activated, result in errors that can be detected using the network management and monitoring systems. Moreover, we can defend against errors by redundant components and cross-layer techniques. An example is having FEC (forward error correction) at the link layer to protect against wireless challenges. By using a cross-layer mechanism, the transport layer can request retransmission of original data if it cannot recover the corrupted data. Thus, we can defend against errors before they are passed to the operational state.

B. Spatial and Temporal Impact of Challenges

It is important to understand the spatial and temporal characteristics of challenges in order to model them realistically. For survivable operation against threats, a certain geographic distance between data centers is proposed [41]. For example, a minimum of 32 miles and a maximum of 151 miles have been designated in data center topologies for site separation against several threats [41]. We provide order-of-magnitude temporal and spatial characteristics of some challenges in Table I.

TABLE I
SPATIAL AND TEMPORAL CHARACTERISTICS OF NETWORK CHALLENGES

Challenge Examples	Spatial Region		Temporal Duration	
	challenge	impact	challenge	impact
earthquake	100s km^2	100s km^2	seconds	days +
fire	100s m^2	10s km^2	hours	days
hurricane	100s km^2	100s km^2	hours	days +
solar storm	1000s km^2	1000s km^2	minutes	days +
misconfiguration	node	global	seconds	minutes
malicious attack	node	global	hours	hours
terrorism	100s m^2	global	hours	hours +
policy related	N/A	regional +	N/A	years
depeering	N/A	global	seconds	days
pandemic	global	global	days	months
power blackout	100s km^2	regional	minutes	hours

For example, the geographic scope of a devastating earthquake can be on the order of 100 km^2 and its impact region on networks might be the same. On the other hand, a fire's geographic scope in a key network node might be on the order of 100s m^2; however, the impact to the communication networks can be larger. The duration of an earthquake can be on the order of seconds whereas recovery of the communication networks can take days. Another example is a policy decision taken by a governing body in which the spatial region and temporal duration of the challenge might not be accurately known. While the impact of a challenge may be only on a nation or a service that impacts users globally, it might take years to revise a policy.

C. Challenge Taxonomy

Network challenges can be categorised based on the phenomenological cause, system boundary, target, objective, intent, capability, dimension, domain, scope, significance, persistence, and repetition they impose on the communication networks as shown in Figure 2. Our *challenge* taxonomy is based on the IFIP 10.4 working group studies on *fault* taxonomy [2]. We note that, while the taxonomy developed by the IFIP 10.4 working group has focused on *computer systems*, we expand and cover the challenge taxonomy with an emphasis on *network systems*. In accordance, we keep the system boundaries, objective, intent, and capability classes the same as the IFIP 10.4 fault taxonomy [2], [3], [34]. We remove the phase of occurrence class since it is applicable to faults only (as opposed to a challenge to the existing network). We add target, domain, scope, significance, and repetition classes to our challenge taxonomy. We modify the phenomenological cause class to include a dependency subclass, add a protocols subclass to dimension, and modify persistence to cover challenges that might be long-lived and short-lived. The permanent subclass is eliminated for challenge scenarios. Next, we elaborate on each of these classes.

Phenomenological cause: The cause of a challenge can be further classified based on ***natural*** causes, ***human-made*** causes, and ***interdependencies*** between the infrastructures. Natural phenomena can occur ***terrestrially*** (e.g. earthquake, fire), ***meteorologically*** (e.g. hurricane, ice storms), or be caused by ***cosmological*** events (e.g. solar storm, space debris). Human-made challenges can be due to decisions driven by ***social***, ***political***, and ***economic*** causes, as well as causes related to ***terrorism***. Examples of such events include recreational crackers, government decisions to block Internet access to nations, and depeering for some financial gain or to increase market share. Finally, phenomenological causes can be due to dependencies within or between the different infrastructures. A failure within the system, at a ***lower level*** can impact the services provided at the higher levels since the services at the higher levels are dependent on the services of lower levels. For example, end-to-end transport is dependent on the lower level hop-by-hop links. Propagation of incorrect BGP announcements is an example of a ***cascading*** failure across the same level within a system. Finally, a power blackout can impact the communication network due to ***interdependencies*** between the power grid and the Internet infrastructures.

System boundary: The system of interest in which it interacts with its environment can be a single system or a system of systems. For example, while a single AS (autonomous system) can be considered as a single system, the Global Internet, which is a collection of ASes, can be considered as system of systems. The challenges can be ***internal*** as in the case of BGP cascading failures, and ***external*** to the system in the case of natural disasters. Moreover, defensive mechanisms developed for external threats falls short for threats coming from inside a system.

Target: The challenges can be ***directly*** targetted to communication infrastructure (e.g. malicious worm) or the network can suffer ***collateral*** damage as a result of a challenge, such as a terrorist activity not directly targetting the network as in the US 9/11 and UK 7/7 attacks.

Objective: The objective of a challenge can be ***non-malicious*** such as misconfigurations or ***malicious*** such as attacks. Furthermore, a ***selfish*** node or AS can limit network resources in its own interest without a malicious objective.

Intent: The intent of the actions taken by humans can be ***non-deliberate*** such as misconfiguration errors or ***deliberate*** such as attacks.

Capability: The challenges caused by humans can be ***accidental*** or due to ***incompetence***. We note that while incompetence refers to lack of professional competence, accidents generally occur as a result of an inadvertent action by humans. For example, BGP prefix hijackings have occurred due to misconfigurations and incompetence of the operator. In the case of the 2003 blackout in the US, one of the causes of the blackout was contact of the power lines with overgrown trees. If the power lines had been laid underground, the catastrophic event could have been prevented.

Dimension: Challenges can affect the ***hardware***, ***software***, ***protocols***, or the ***traffic*** within a network. For example, random hardware failures fall under the hardware sub-class of the dimension class, software bugs fall under the software sub-class of the dimension class, and attacks exploiting a vulnerability in a protocol fall under the protocol sub-class of the dimension class. Furthermore, legitimate traffic can impact the services being offered by the network such as the case of flash crowds. We note that DDoS attacks also impact the legitimate user traffic.

Domain: Challenges vary depending on the domain in which communication network operates. ***Medium***, ***mobility***, ***delay***, and ***energy constraints*** impose different mechanisms to be considered when dealing with challenges. The medium in which nodes communicate can be using ***wired*** or ***wireless*** links. The nodes can be at ***fixed*** locations or ***mobile*** in which topology control mechanisms are fundamentally different. Delay characteristics in which the networks operate also vary: in a terrestrial network a ***low*** delay, in interplanetary communication a ***predictable high*** delay, and in the case of sensor networks for habitat monitoring ***unpredictably high*** delay occurs. Moreover, energy resources are different for networks operating in different domains: while a desktop computer that is connected to ***power grid*** has unlimited energy, a laptop with a ***rechargeable battery*** face different challenges than an ***energy-constraint*** sensor node in a hostile area in which it might not be feasible to replace its battery.

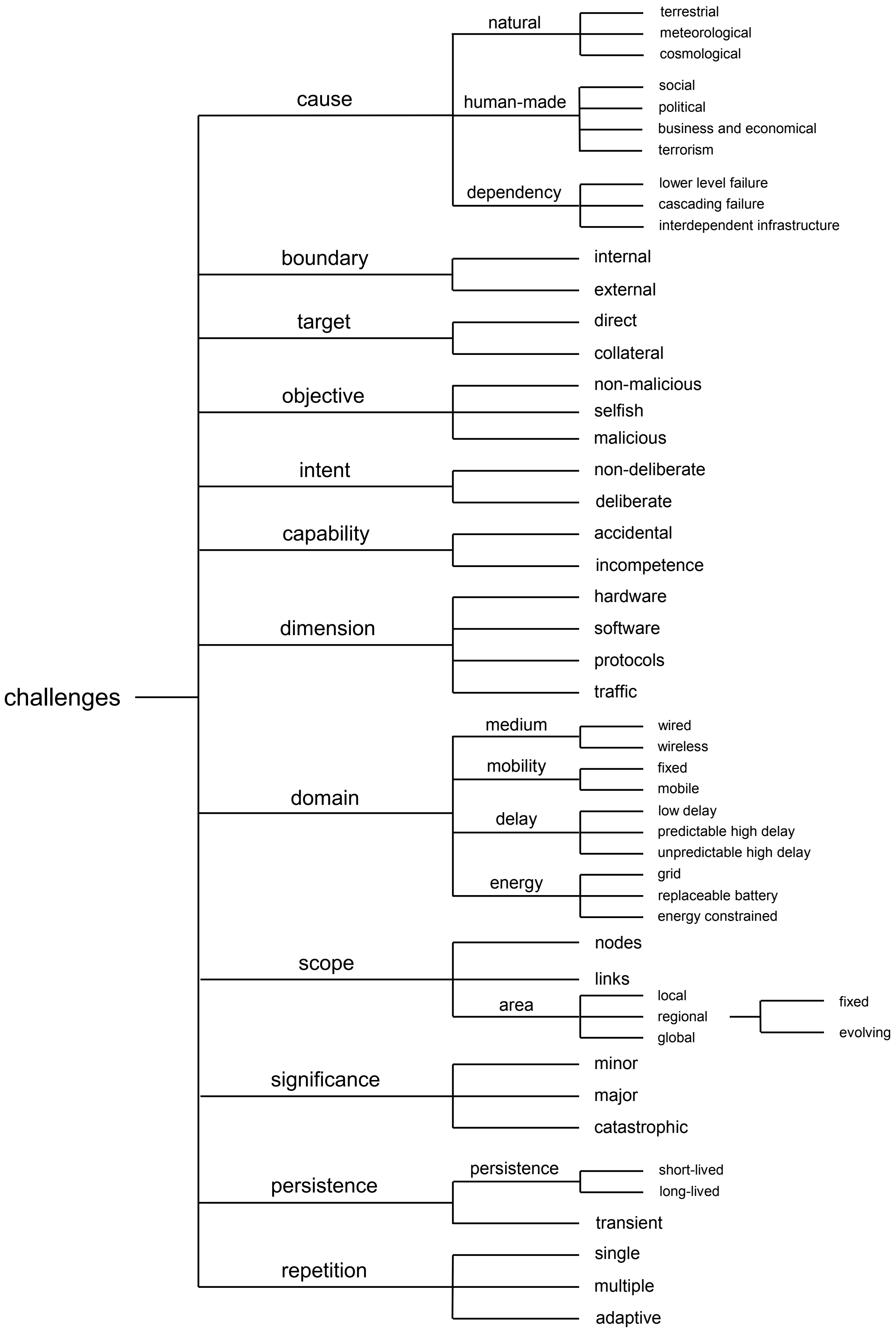

Fig. 2. Taxonomy of network challenges

Scope: The scope of a challenge can impact the ***nodes*** within a network, the ***links*** within a network, and some parts or the entire ***geographic area*** of the network. Geographic scope in which a challenge might impact the network can be ***local***, ***regional***, or ***global***. Moreover, the geographic scope of regional challenges can be ***fixed*** (e.g. earthquake) or ***evolving*** (e.g. Hurricane Irene).

Significance: A challenge's significance can be ***minor***, ***major***, or ***catastrophic***. In the case of the PSTN, the number of lost customer minutes provides a good measure of the significance of an event. Large-scale disasters such as Hurricane Katrina and the Fukushima Earthquake that caused human and financial losses was catastrophic in significance. Depeering of ISPs in which some customers cannot reach each other is a challenge with major significance, whereas a jammer preventing communication between two individuals may be a challenge with minor significance.

Persistence: Persistence captures the continuation property of a challenge. The ***persistent*** challenges such as BGP misconfigurations can be ***short-lived*** or ***long-lived***. The majority of BGP misconfigurations are considered short-lived, meaning that minutes after discovery of the mistake, remediation takes place. An example of a long-lived challenge would be a pandemic that affects communication services for months. A challenge can be ***transient*** such as a lightning strike taking down power equipment.

Repetition: Challenges can occur in ***single*** instances or ***multiple*** instances. While natural disasters are single instance events, malicious attacks might be repetitious. Furthermore, a repeated instance of a challenge that ***adapts*** to failures can cause worse harm.

D. Challenge Matrix

In the previous section, we categorise challenges to the network. In this section, we return to the major challenge groupings introduced in Section III and demonstrate the validity of our taxonomy. The challenges can be broadly listed as follows: large-scale disasters, socio-political and economical challenges, dependent failures, human errors, malicious attacks, unusual traffic, and environmental challenges

We note that, these coarse groupings of challenges overlap with each other partially. For example, a DDoS attack can be categorised under malicious attack as well as under the unusual traffic category. Next, we correlate the challenge taxonomy with the challenge grouping as shown in Table II. In this case, we list the challenge categories from our taxonomy in Figure 2 in the first three columns and the major challenge groupings in the last seven columns. We mark a given (category, grouping) cell with an × if that particular challenge group may occur within that challenge category. Furthermore, not all the binary combinations are possible. For example, a malicious attack is caused by humans, but not by natural phenomena. Such a cross-correlation matrix can be beneficial for correct threat modelling. Next, for each major challenge listed above, we describe its relation to our challenge taxonomy. Note that a summary of challenges are presented in Section III; however, only a select few examples are presented for clarification in this section.

Large-scale disasters can be caused by natural phenomena, human actions, and dependencies among infrastructures. Target, objective, intent, capability, dimension, domain, and persistence aspects of the challenge categories can take any value. On the other hand, the scope of large-scale disasters are not *local* and large-scale disasters are non-repetitive catastrophic events that cause human and financial losses.

Socio-political and economical events are caused by humans challenging communication networks. In the case of nationwide Internet outages these occurred within the nation, thus the system boundary was internal (e.g. Iran blocking its own traffic [42]), whereas DDoS attacks against Estonia due to a political decision was launched from outside of Estonia [43]. While the target and objective category of these challenges can take any value, the socio-political and economical events fall into deliberate intent and incompetence capability of our challenge category. Such social, political, and economic events impact the protocol and traffic dimensions across the wired and wireless domains of challenge categories. In the case of a nationwide Internet outage, the impact of the challenge scope is regional, whereas a policy decision can have global impact on networks with a major or catastrophic significance. During the Arab spring, Syria's network prefixes were withdrawn from the global routing table *multiple* times (3 June 2011 [44], [45], 19 July 2012 [46], 18 August 2012 [47], 29 November 2012 [48]–[51]). Furthermore, in the case of political unrest in Egypt, social networks were initially blocked on 25 January 2011 [52] along with suspension of the mobile telephony service in certain areas [53]. This was followed by the withdrawal of most network prefixes from the global routing table on 27 January 2011, except the prefixes that belong to financial institutions [54], [55]. Eventually, all network prefixes in Egypt were withdrawn on 31 January 2011 [55]–[57], showing an *adaptive* challenge. After more than a week, network services in Egypt returned to normal on 2 February 2011 [58].

Dependent failures occur as a result of the failure of one system that provides service to another one. For example, critical infrastructures such as the power grid and the Internet are becoming more dependent on each other. If the power fails, communication networks can halt as a *collateral* result. The power grid increasingly requires the Internet to transport its SCADA (Supervisory Control and Data Acquisition) [59]. On the other hand, a service failure at a lower level is a *direct* challenge against higher layers. BGP cascading failures are also a direct target against communication networks. The capability of dependent failures are due to accident or incompetence. They impact the hardware, software, and protocol dimensions of the network system across the wired and wireless domains. While the dependent failure's scope can impact nodes, links, and areas, the significance of this challenge can be major or catastrophic. Dependent failures are persistent and repetitious, but not adaptive.

TABLE II
CORRELATION OF NETWORK CHALLENGES

Challenge categories			Large-scale disasters	Socio-political & econo. challenges	Dependent failures	Human errors	Malicious attacks	Unusual traffic	Environ. challenges
cause	natural	terrestrial	×						
		cosmological	×						×
		meteorological	×						×
	human-made	social	×	×		×	×	×	×
		political	×	×			×	×	×
		business & economical	×	×			×	×	×
		terrorism	×	×			×	×	×
	dependency	interdependent infrastructure	×		×				
		lower-level failure	×		×				
		cascading failure	×		×				
boundary	internal			×	×	×	×	×	×
	external		×	×	×		×		×
target	direct		×	×	×	×	×	×	×
	collateral		×	×	×	×			
objective	non-malicious		×	×	×	×		×	×
	selfish		×	×				×	
	malicious		×	×			×		
intent	non-deliberate		×		×	×		×	×
	deliberate		×	×		×	×		
capability	accidental		×		×	×	×		×
	incompetence		×	×	×	×	×	×	×
dimension	hardware		×		×	×	×		
	software		×		×	×	×		
	protocols		×	×	×	×	×		×
	traffic		×	×			×	×	×
domain	medium	wired	×	×	×	×	×	×	
		wireless	×	×	×	×	×	×	×
	mobility	fixed	×	×	×	×	×	×	×
		mobile	×	×	×	×	×	×	×
	delay	low	×	×	×	×	×	×	×
		high	×	×	×	×	×		×
		unpredictable	×			×	×		×
	energy	grid	×	×	×	×	×	×	×
		replaceable	×	×	×	×	×	×	×
		constrained	×				×		×
scope	nodes		×		×	×	×	×	
	links		×		×	×	×	×	×
	area	local			×	×	×		×
		regional	×	×	×	×	×		×
		global	×	×		×	×		
significance	minor					×	×	×	×
	major			×	×	×	×	×	×
	catastrophic		×	×	×	×	×		
persistence	persistence	short-lived	×	×	×	×	×	×	
		long-lived	×	×	×		×		×
	transient		×			×			
repetition	single		×		×	×	×	×	×
	multiple			×	×	×	×		
	adaptive			×			×		

Human errors can directly impact the networks or can cause collateral damage. These are non-malicious activities and occur as a result of non-deliberate or deliberate intent. Operational mistakes occur accidentally or due to incompetence. The dimension, domain, scope, and significance of these challenges vary. Operational mistakes are generally short-lived or transient. There can be a single occurrence or multiple repetitive occurrences.

Malicious attacks are caused by humans directly targetting networks with a malicious objective and deliberate intent. For example, a bot can exploit the vulnerabilities if the host is not properly secured, and this lack of secure perimeter can be accidental or due to incompetence. Dimension, domain, scope, and significance properties can take any value. Malicious attacks can be short-lived or long-lived. Moreover, they can be single, multiple, and adaptive. We note that the system boundary for attacks can be internal and external in which most attacks come from insiders [60]. On the other hand, a non-malicious user writing her password on a sticky note and attaching it next to her computer monitor is a human error with incompetence capability in which an insider or outsider can exploit this to attack the network [61].

Unusual traffic, such as flash crowds, is caused by humans. These events target networks directly with a non-malicious or selfish objective. The intention of users who want to access information is deliberate; however, their intent is not to consume all of the network resources. Therefore, this is a non-deliberate event. In the case of a flash crowd event, network is overwhelmed with requests by users who does not cease trying to access the network resources. If the users understand the situation in a flash crowd and back off, then the resources may be available over a time period; however, the network resources may still not be available at the instant users request. Therefore, we designate this case as incompetence, since users do not know how the network operates and continue trying to access network resources. The impact is on the traffic dimension of the challenge categories. Unusual traffic impacts network resources on nodes and links. This kind of challenge has minor and major significance, since the network might be operational; however, network services can be limited.

Environmental challenges are inherent in the wireless communication medium, such as rain storms and CMEs (coronal mass ejections), therefore the cause can be natural with a non-malicious objective and non-deliberate intent. Moreover, connectivity on a wireless link can be disrupted by a malicious jammer driven by socio-political and economical reasons. As explained in malicious attacks, capability can be due to accidental or incompetence. Their impact is on the traffic and protocol dimension of the challenges. They only impact the wireless medium, impacting links, and have a local and regional area scope; however, in the case of interplanetary communication, the scope of disruption is larger. Environmental challenges have minor or major significance with long-lived and non-repetitious characteristics.

E. Correlation of Challenges

We describe with examples of how the challenges correlate with our taxonomy in Table II. By considering the dimension, scope, significance, and persistence challenge categories, large-scale disasters and malicious attacks can cause the worst harm to networks. Their impact can be global in scope, and they can be long-lived, resulting in catastrophic service failures. Moreover, an attack that adapts to defensive measures can be even more harmful. Environmental challenges, such as delay, mobility, and connectivity are only applicable to the wireless domain, and these challenges should be considered during the design phase. In other words, wired networks can be strengthened using redundancy and diversity; however, the same is more difficult for wireless networks. The capability category is primarily applicable to human errors and not applicable for most of the challenge examples. Incompetence and accidental challenges can be avoided by proper training of the operations personnel. Among the social, political, and economical challenges, nationwide Internet outages are the worst, since a country can be disconnected from the Global Internet. As presented, there exists a wide spectrum of challenges, and we cannot avoid them; however, with careful planning, the consequences can be alleviated.

V. Conclusions and Future Work

Networks face a variety of challenges that disrupt normal operation and understanding these challenges is necessary for developing correct threat models to design resilient networks that are cost-efficient. Based on past and potential challenges that are summarised, we present a taxonomy of challenges that can be beneficial to evaluate network design choices. Furthermore, we describe how these challenges correlate with our taxonomy.

We strive to have a complete and comprehensive taxonomy; however, it will require refinement as new challenges arise. We expect that such a taxonomy will be beneficial for network designers and foster cooperation among researchers.

Acknowledgments

We would like to acknowledge Michael Watson, David Hutchison, and other members of the ResiliNets group for discussions on this work. This research was supported in part by NSF FIND (Future Internet Design) Program under grant CNS-0626918 (Postmodern Internet Architecture), by NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI), by NSF grant CNS-1219028 (Resilient Network Design for Massive Failures and Attacks), and by the EU FP7 FIRE Programme ResumeNet project (grant agreement no. 224619).

References

[1] J. P. G. Sterbenz and D. Hutchison, “ResiliNets: Multilevel Resilient and Survivable Networking Initiative Wiki.” http://wiki.ittc.ku.edu/resilinets, April 2006.

[2] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[3] A. Avižienis, J.-C. Laprie, and B. Randell, “Dependability and Its Threats: A Taxonomy,” in *Building the Information Society* (R. Jacquart, ed.), vol. 156 of *IFIP International Federation for Information Processing*, pp. 91–120, Springer Boston, 2004.

[4] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, “Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines,” *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[5] A. Popescu, T. Underwood, and E. Zmijewski, “Quaking Tables: The Taiwan Earthquakes and the Internet Routing Table,” in *APRICOT*, (Bali), Renesys Corp, 2007.

[6] Y. Ran, “Considerations and Suggestions on Improvement of Communication Network Disaster Countermeasures after the Wenchuan Earthquake,” *IEEE Communications Magazine*, vol. 49, no. 1, pp. 44–47, 2011.

[7] J. Cowie, “Japan Quake.” http://www.renesys.com/blog/2011/03/japan-quake.shtml, March 2011.

[8] A. Kwasinski, “Effects of Notable Natural Disasters from 2005 to 2011 on Telecommunications Infrastructure: Lessons from on-site Damage Assessments,” in *Proceedings of the 33rd IEEE International Telecommunications Energy Conference (INTELEC)*, (Amsterdam), pp. 1–9, October 2011.

[9] J. Cowie, A. Popescu, and T. Underwood, “Impact of Hurricane Katrina on Internet Infrastructure,” technical report, Renesys, September 2005.

[10] D. Madory, “Hurricane Sandy: Initial Impact.” http://www.renesys.com/blog/2012/10/hurricane-sandy-initial-impact.shtml, October 2012.

[11] J. Cowie, “Irene Wallops US Internet.” http://www.renesys.com/blog/2011/08/irene-wallops-us-internet.shtml, August 2011.

[12] D. H. Boteler, R. J. Pirjola, and H. Nevanlinna, "The effects of geomagnetic disturbances on electrical systems at the earth's surface," *Advances in Space Research*, vol. 22, no. 1, pp. 17–27, 1998.

[13] J. Kappenman, "A Perfect Storm of Planetary Proportions," *IEEE Spectrum Magazine*, vol. 49, no. 2, pp. 26–31, 2012.

[14] "Pandemic Influenza Impact on Communications Networks Study," unclassified, Department of Homeland Security (DHS), December 2007.

[15] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, 2011.

[16] C. Partridge, P. Barford, D. D. Clark, S. Donelan, V. Paxson, J. Rexford, and M. K. Vernon, *The Internet Under Crisis Conditions: Learning from September 11*. Washington, D.C.: The National Academy Press, 2003.

[17] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of Country-wide Internet Outages Caused by Censorship," in *Proceedings of the ACM Internet Measurement Conference (IMC)*, (Berlin), pp. 1–18, November 2011.

[18] T. Underwood, "Peering—The Fundamental Architecture of the Internet." http://www.renesys.com/blog/2005/12/peering-the-fundamental-archit.shtml, December 2005.

[19] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[20] J. H. Cowie, A. T. Ogielski, B. J. Premore, E. A. Smith, and T. Underwood, "Impact of the 2003 Blackouts on Internet Communications," technical report, Renesys Corporation, 2003.

[21] J. Li, Z. Wu, and E. Purpus, "Toward Understanding the Behavior of BGP During Large-Scale Power Outages," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, (San Francisco, CA), pp. 1–5, November 2006.

[22] K. T. Latt, Y. Ohara, S. Uda, and Y. Shinoda, "Analysis of IP Prefix Hijacking and Traffic Interception," *International Journal of Computer Science and Network Security*, vol. 10, no. 7, pp. 22–31, 2010.

[23] V. Pappas, D. Wessels, D. Massey, S. Lu, A. Terzis, and L. Zhang, "Impact of Configuration Errors on DNS Robustness," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 3, pp. 275–290, 2009.

[24] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP Misconfiguration," in *Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, (Pittsburgh, PA), pp. 3–16, August 2002.

[25] D. R. Kuhn, "Sources of Failure in the Public Switched Telephone Network," *IEEE Computer*, vol. 30, no. 4, pp. 31–36, 1997.

[26] J. C. McDonald, "Public Network Integrity–Avoiding a Crisis in Trust," *IEEE Journal on Selected Areas in Communications*, vol. 12, no. 1, pp. 5–12, 1994.

[27] G. Zorpette, "Keeping the phone lines open," *IEEE Spectrum Magazine*, vol. 26, no. 6, pp. 32–36, 1989.

[28] G. P. Im and R. L. Baskerville, "A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error," *ACM SIGMIS Database*, vol. 36, no. 4, pp. 68–79, 2005.

[29] A. B. Brown, "Oops! Coping with Human Error in IT Systems," *ACM Queue*, vol. 2, no. 8, pp. 34–41, 2004.

[30] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Redundancy, Diversity, and Connectivity to Achieve Multilevel Network Resilience, Survivability, and Disruption Tolerance (invited paper)," *Springer Telecommunication Systems*, 2012. (accepted April 2012).

[31] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms," in *Proceedings of the ACM Workshop on Rapid Malcode (WORM)*, (Washington, D.C.), pp. 11–18, October 2003.

[32] W. LeFebvre, "CNN.com: Facing a World Crisis," in *Proceedings of the 15th USENIX Conference on Systems Administration (LISA)*, (San Diego, CA), December 2001. Invited Talk.

[33] J. P. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," in *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*, (Atlanta, GA), pp. 31–40, September 2002.

[34] J.-C. Laprie, A. Avižienis, and H. Kopetz, eds., *Dependability: Basic Concepts and Terminology*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1992.

[35] M. Fry, M. Fischer, M. Karaliopoulos, P. Smith, and D. Hutchison, "Challenge Identification for Network Resilience," in *Proceedings of the 6th IEEE/EURO-NF Conference on Next Generation Internet (NGI)*, (Paris), pp. 1–8, June 2010.

[36] ENISA Virtual Working Group on Network Providers Resilience Measures, "Network resilience and security: Challenges and measures," Tech. Rep. WP 2009 – WPK 1.2 VWG 1, ENISA – European Network and Information Security Agency, December 2009.

[37] J. P. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, and J. P. Rohrer, "Modelling and Analysis of Network Resilience (invited paper)," in *Proceedings of the 3rd IEEE/ACM International Conference on Communication Systems and Networks (COMSNETS)*, (Bangalore), pp. 1–10, January 2011.

[38] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. Sterbenz, "A Comprehensive Framework to Simulate Network Attacks and Challenges," in *Proceedings of the 2nd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (Moscow), pp. 538–544, October 2010.

[39] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. Sterbenz, "Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach," *Telecommunication Systems*, pp. 1–16, 2011. doi: 10.1007/s11235-011-9575-4.

[40] A. Jabbar, J. P. Rohrer, A. Oberthaler, E. K. Çetinkaya, V. S. Frost, and J. P. Sterbenz, "Performance Comparison of Weather Disruption-Tolerant Cross-Layer Routing Algorithms," in *Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM)*, (Rio de Janeiro), pp. 1143–1151, April 2009.

[41] R. Cocchiara, H. Davis, and D. Kinnaird, "Data center topologies for mission-critical business systems," *IBM Systems Journal*, vol. 47, no. 4, pp. 695–706, 2008.

[42] C. Labovitz, "A Deeper Look at The Iranian Firewall." http://asert.arbornetworks.com/2009/06/a-deeper-look-at-the-iranian-firewall/, June 2009.

[43] M. Lesk, "The New Front Line: Estonia under Cyberassault," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 76–79, 2007.

[44] J. Cowie, "Syrian Internet Shutdown." http://www.renesys.com/blog/2011/06/syrian-internet-shutdown.shtml, June 2011.

[45] J. Cowie, "Tracing the Syrian Blackout." http://www.renesys.com/blog/2011/06/tracing-the-syrian-blackout.shtml, June 2011.

[46] D. Madory, "Syria Briefly Disconnects." http://www.renesys.com/blog/2012/07/syria-leaves-the-internet.shtml, July 2012.

[47] D. Madory, "PCCW Keeps Syria Connected." http://www.renesys.com/blog/2012/08/china-keeps-syria-connected.shtml, August 2012.

[48] J. Cowie, "Syrian Internet Is Off The Air." http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml, November 2012.

[49] The Internet Society, "The Internet Society on Syria's Internet Shutdown." http://www.internetsociety.org/news/internet-society-syria's-internet-shutdown, November 2012.

[50] M. Prince, "How Syria Turned Off the Internet." http://blog.cloudflare.com/how-syria-turned-off-the-internet, November 2012.

[51] J. Cowie, "Restoration in Syria." http://www.renesys.com/blog/2012/12/restoration-in-syria-1.shtml, December 2012.

[52] https://twitter.com/twittercomms/status/30377205695647744, January 2011.

[53] T. M. Chen, "Governments and the Executive 'Internet Kill Switch'," *IEEE Network*, vol. 25, no. 2, pp. 2–3, 2011.

[54] J. Cowie, "Egypt Leaves the Internet." http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml, January 2011.

[55] E. Zmijewski, "Egypt's Net on Life Support." http://www.renesys.com/blog/2011/01/egypts-net-on-life-support.shtml, January 2011.

[56] A. Toonk, "Internet in Egypt offline." http://bgpmon.net/blog/?p=450, January 2011.

[57] C. Labovitz, "Egypt Loses the Internet." http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet/, January 2011.

[58] J. Cowie, "Egypt Returns To The Internet." http://www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml, February 2011.

[59] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.

[60] E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security*, vol. 21, no. 6, pp. 526–531, 2002.

[61] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, 2005.