INSTITUTE FOR DEFENSE ANALYSES

Resilient National Security and Emergency Preparedness Communications: Service Metrics

Serena Chan, *Project Leader*

Robert S. Sneddon

October 2015

IDA Non-Standard
NS D-5496
Log: H 15-000459
Copy

NSTITUTE FOR DEFENSE
ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2015		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Resilient National Security and Emergency Preparedness Communications: Service Metrics	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311-1882**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

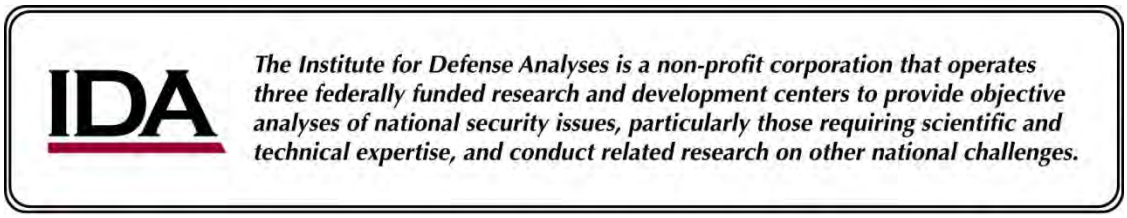
13. SUPPLEMENTARY NOTES

14. ABSTRACT

Resilient communications are critically important in the event of a national security crisis or disaster. In the event of a significant threat to public safety, communications for national security and emergency preparedness must continue to provide an acceptable level of service for senior leader decision makers and first responders. If primary communications are lost, then resiliency is the ability for rapid and effective reconstitution or utilization of alternate means. This paper introduces concepts of communications resilience and suggests appropriate service metrics. The concepts of survivability, tolerance, flexibility, and capacity are used to define system tolerance, system flexibility, and system capacity.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**10**	



About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task ER-5-3697, "National Security Emergency Preparedness Communications," for 1000 Defense Pentagon, Washington DC 20301. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Margaret E. Myers, Robert S. Jack II

Resilient National Security and Emergency Preparedness Communications: Service Metrics

Robert Sneddon
Institute for Defense Analyses
Alexandria, VA, USA
rsneddon@ida.org

Serena Chan
Institute for Defense Analyses
Alexandria, VA, USA
schan@ida.org

***Abstract*—Resilient communications are critically important in the event of a national security crisis or disaster. In the event of a significant threat to public safety, communications for national security and emergency preparedness must continue to provide an acceptable level of service for senior leader decision makers and first responders. If primary communications are lost, then resiliency is the ability for rapid and effective reconstitution or utilization of alternate means. This paper introduces concepts of communications resilience and suggests appropriate service metrics. The concepts of survivability, tolerance, flexibility, and capacity are used to define system tolerance, system flexibility, and system capacity.**

***Index Terms*—Resilience, reliability, communications, service metrics, tolerance, flexibility, capacity, survivability.**

I. Introduction

Resilient national security and emergency preparedness (NS/EP) communications are critically important in the event of a national security crisis or disaster. Moreover, reliable and secure telecommunications are necessary for mission critical communications. This holds true at all levels of government and the private sector for effective management of national security incidents and emergencies. NS/EP communications is a complex and rapidly evolving operational environment because NS/EP communication systems encompass landline, wireless, broadcast and cable television, radio, public safety systems, satellite communications, and the Internet. This paper is part of an effort to accurately characterize the NS/EP communications problem space and address it in a more holistic manner.

Senior leader decision makers and first responders require resilient communications to do their jobs effectively. In a perfect world, NS/EP communication systems would be able to tell users when and whether they are compromised, whether the systems are still operational in full or degraded mode, identify alternatives, and finally, provide the ability to restore the systems to their full operational state. However, currently there is a lack of metrics that directly determine or predict the resilience of a given system. Therefore, the authors will attempt to develop some reasonable metrics that will show the extent to which communication systems are resilient.

In this paper, the authors first review basic concepts of resilience. An architectural framework for resilience and survivability in communication networks is provided in [1], as well as a survey of the disciplines that resilience encompasses. The authors uses concepts derived from [2, 3] to propose NS/EP communications metrics. The newly defined resiliency metrics are then applied to a fictional emergency disaster scenario to illustrate how resilience can be measured.

II. Concepts of Resilient Systems

A. Attributes of Resilience

In general, resilience is often defined as the ability of a communications network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. The terms *resilience* and *reliability* are often used interchangeably, which is inaccurate. Reliability is a necessary attribute of resilience, but only as the initial description.

Reliability of a communications system is often measured as Mean Time Between Failures (MTBF). Highly reliable communications systems have a large MTBF. However, a resilient communications system should also have a high level of survivability, which can be described as the probability that the communications system will survive a realized threat.

Survivability is one of the most fundamental metrics of resilience. The concept of survivability as a function of resilience is extrapolated from [4] and applied to communications systems. Survivability can be defined as the capability of a system to be operated and maintained to fulfill its mission, in a timely manner, and in the presence of threats such as attacks or large- scale natural disasters. There are two aspects to survivability: susceptibility and vulnerability. *Susceptibility* is the inability to avoid being denied, degraded, or destroyed by either manmade attacks or natural occurrences. That is, if there is an attack, what is the probability that the communications network will lose its capability to maintain communications? Susceptibility can be measured as the probability of a "hit" from the attack and is expressed as:

$$\text{Susceptibility} \equiv P(\text{Hit}) \tag{1}$$

The publication of this paper does not indicate endorsement by the Department of Defense (DoD) or the Institute for Defense Analyses (IDA), nor should the contents be construed as reflecting the official position of those organizations.

Vulnerability is the probability of losing a communications capability given that the system has taken a hit. It is written as a conditional probability:

$$\text{Vulnerability} \equiv P\left(\text{Capability Loss} \mid \text{Hit}\right) \quad (2)$$

Thus, the loss of a communications capability is equal to the Susceptibility multiplied by the Vulnerability. It can be called "Risk" and is expressed as:

$$\text{Risk} = P\left(\text{Capability Loss} \mid \text{Hit}\right) P\left(\text{Hit}\right) \quad (3)$$

Therefore, the probability of maintaining a communications capability is 1 minus the Risk. That is, Survivability can be written as:

$$\text{Survivability} = 1 - P\left(\text{Capability Loss} \mid \text{Hit}\right) P\left(\text{Hit}\right) \quad (4)$$

The survivability of a communications system depends on whether it can avoid an attack or overcome one. Survivability can be estimated by a network of conditional probabilities, such as a Bayesian network. Creating this network requires one to work out all plausible threat scenarios and find estimates of the conditional probabilities that make up the chain of events leading to a "risk." These probabilities can be estimated from previous data, the use of subject matter experts using, e.g., the "Delphi Method," or a combination of the two.

Reliability and survivability are attributes that are necessary but not sufficient for a communications system to be resilient. Additional attributes that make a communications system resilient are often described in the systems engineering literature [3, 4] as:

- *Tolerance* - exhibits graceful degradation near the boundary of performance,
- *Flexibility* - ability to use different system elements after a disruption, and
- *Capacity* - ability to operate at a certain level; the capability margin between maximum operating levels and a minimum threshold.

The first and most important of these attributes is tolerance, the ability to decline gracefully instead of in an abrupt manner. For example, a cell phone service that exhibits tolerance during degradation may take a longer time to connect. Voice quality may decline, and the number of dropped calls may increase; however, the service will not end abruptly. Despite interference with performance, voice communications still occur.

A second important aspect of resilience is flexibility, the ability to use different elements of a communications system to deliver a message. For example, most current mobile devices offer 4G LTE. If the device is not in an area with LTE coverage, the device may use 3G technology to support voice, text, and data services. The device may even resort to analog 1G to provide simple telephony service without data. Flexibility means that during a disruption, alternative system elements allow the necessary communication to still be transmitted.

Finally, the ability to operate at a certain level despite a disruption is the fundamental attribute of capacity. The attribute is often defined as "the available capability margin between current operating levels and minimum threshold levels" [3]. Thus, a high capacity system has a greater chance of providing communications despite a disruption.

B. State Space Formulation of Resilience

Sterbenz et al. [1] characterize a communication system by emphasizing two things: the operational status of the system and the status of the particular capability or "service" that conducts the communication. These concepts are combined to create a "State Space" description of the communications system. Here, the State Space has two dimensions. The first dimension provides the operational status while the second dimension provides the level of performance of a service parameter.

Sterbenz et al. [1] note "evaluating network resilience in this way effectively quantifies it as a measure of service degradation in the presence of challenges." The operational state describes the readiness of the physical infrastructure and communication protocols, and ideally, the readiness of the operators. The second dimension is about the services being provided (in relation to the system requirements). Thus, communications resilience is evaluated by separating the entire system into these two parts and examining the efficacy of a service in the context of the operational status of the underlying physical infrastructure and protocols. Conceptually, a resilient communications system will continue to provide services despite severe degradation of the operational ability of the underlying infrastructure.

These concepts were further expanded to create an entire framework for formulating resilience, which they call "ResiliNets." The ResiliNets formulation is denoted as: D2R2+DR, meaning Defend, Detect, Remediate, Recover, then Diagnose and Refine. For a system to be resilient, it must first Defend against threats to it, it must be able to Detect when something adverse has happened, it must Remediate the damage that has occurred, and finally, it must Recover to its original state. Additionally, after this recovery from an adverse situation, learning occurs by Diagnosis and Refining the systems ability to Detect and Defend against the threat.

It should be noted that their State Space formulation is an idealization. Clearly, if the operational status of the physical infrastructure and protocols are completely inoperative, then there can be no service. However, a resilient system will still be able to provide necessary services despite a significantly degraded operational capability.

C. State Space Modeling of Resilience

Figure 1 illustrates the concept of changes in state of a communications network. The vertical axis delineates levels of service from Acceptable to Unacceptable. The horizontal axis delineates operational status from Normal to Severely Degraded. "S" values denote the state of the entire system.

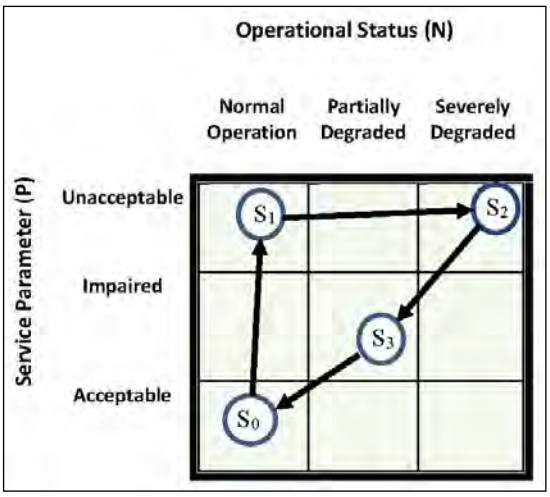


Fig. 1. State Space Model of Resilience.

As an example, we apply the concepts of a State Space to the case of a simple cell phone service during an earthquake scenario. At the beginning, the operational status of the system is Normal (as defined by the operators of the communications system) and the ability to make phone calls is of an Acceptable level. Assume that in the wake of the earthquake, cell phone service is saturated due to a huge upsurge in phone calls. We have moved from state S_0 to state S_1. While the operational status of the cellular network is Normal, the service is saturated, thus rendering it Unacceptable. This is an example of a non-resilient service.

After the original earthquake, several aftershocks knock over the cell phone towers, thus rendering the operational status to be Severely Degraded. It continues to be impossible to place a cell phone call, so the service level remains Unacceptable, but we have now moved to state S_2.

To partially remedy the situation, the phone company puts up several temporary towers, allowing some cell phone calls to make connections. The operational status of the network is now Partially Degraded and the service is Impaired (state S_3). Finally, when the original cell phone towers are repaired, the operational status is restored to Normal and the service status returns to Acceptable (state S_0).

This earthquake scenario highlights both resilient and non-resilient aspects of a cellular network. Fully understanding "Normal Operations" allows operators to quickly adapt to abnormal operations when the network is saturated, i.e., load balancing which is illustrative of service Flexibility. Erecting temporary cellular towers to keep service up and running is a good tactic to restoring operations, highlighting poor Tolerance in the underlying infrastructure but adequate Flexibility in the addition of new system elements to restore service Capacity.

D. Petri Nets Formulation of Resilience

Valraud and Levis [5] formulate resilient Command and Control (C2) in a rigorous manner by using a Petri Net model. The Petri Net model simulates information flows. A *simple information flow path* is any path in the Petri Net that goes from a source to a sink. In turn, the combination of all simple information flows that lead to the same sink is called a *complete information flow path*. A simple communication function is represented by a simple information flow path. Similarly, a complete function corresponds to the set of simple information flow paths that create a complete information flow. Identifying these complete information flow paths is key to understanding how the network instantiates a particular function. This shows that how the Petri Net model is useful for checking the fulfillment of all requirements of a C2 system and its actual formulation.

A generalization of the Petri Net approach to communications resilience as well as the creation of metrics to measure resilience is given by [2-3]. One can describe the resilience of a capability (in a C2 system) by examining its rate of deviation from a pre-disruption state (or value), as illustrated in Fig. 2. The vertical axis shows the "Measure of Performance" (MoP) of the capability while the horizontal axis describes the phases of capability disruption. The phases of disruption include: Avoidance, Survival, and Recovery. The Avoidance phase is Normal Operations. A disruption occurs decreasing the ability of the capability to perform (Survival phase). Finally, after some time, the capability is in the Recovery phase and is being restored.

Therefore, Tolerance is the rate of decline that a system can handle without losing its ability to perform its function. Let "attributes space" be the space that can describe both the attributes of the C2 system and the attributes of a mission that uses the C2 system. Let L_p be the "locus of performance" in attributes space within which the C2 system can perform. Let L_r be the "locus of requirements," i.e., the set of points in attributes space in which the C2 system is fulfilling its mission requirements [6]. Then, a communications system is exhibiting Tolerance if it exhibits a graceful decline while staying in the part of attributes space that meets both the C2 mission performance attributes and its system requirements attributes. Thus, Tolerance can be expressed as a capability decline:

$$Tol_{RD} = \frac{MoP_{Capability}\left(\frac{L_p \cap L_r}{L_p}, t_d\right) - MoP_{Capability}\left(\frac{L_p \cap L_r}{L_p}, t_{\min}\right)}{t_{\min} - t_d} \quad (5)$$

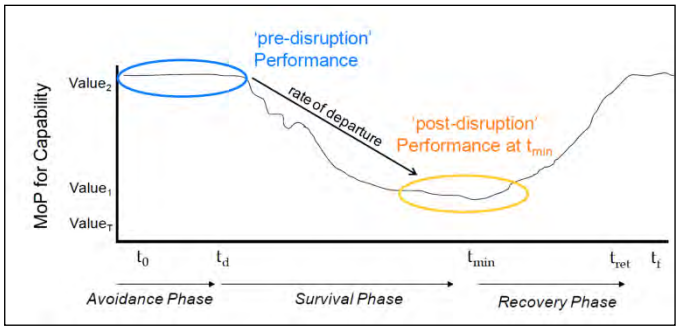


Fig. 2: Petri Net Approach for Measuring Resilience[1].

[1] Used with permission from [2].

where, $MoP_{Capability}$ is the Measure of Performance of a communication capability, which is a metric that shows the level of that communication capability[2]. Tol_{RD} is therefore the measure of the rate of decline of a performance parameter while the system stays within requirements.

Flexibility can be measured in terms of a systems ability to perform a function in different ways to reorganize and re-create the needed functionality, i.e., the number of different ways that a system can perform a function [2]. These different ways are redundant ways to instantiate a capability and that level of redundancy is measured as the "Proportion of Use," the fraction of elements required to deliver a capability and it is expressed as:

$$PoU = \frac{\sum_{i=1}^{r} B_i}{rE} \tag{6}$$

where r = total number of information flow paths,
B_i = number of elements (linkages) in a specific path, l_i, and
E = total number of elements (linkages) used to describe the different ways that information can flow. The smaller the proportion, the greater the level of flexibility. For example, assume there is a single fiber optic connection between a sender and the recipient of an email/VoIP. Then, the number of elements B_i for an email is 1 and for VoIP is 1. The total number of information flow paths, r, is equal to 2 (one for email and one for VoIP).The total number of elements (physical links), E, is 1. Then:

$$PoU = \frac{(1 \text{ email link}) + (1 \text{ VoIP link})}{(2 \text{ information flow paths}) \cdot 1 \text{ connection}} = \frac{2}{2} = 100\%$$

Therefore, the *PoU* is 100%, i.e., there is no actual redundancy. Thus, this measure captures the actual, physical redundancy, not just functional redundancy.

Capacity can be measured as the range of performance that a system has while maintaining a capability, i.e., the difference between the highest level of capacity a system can have and its lowest value where the capability can still be performed. It can be expressed as:

$$\text{Capacity} = \frac{MoP_{\text{Capability max}} - MoP_{\text{Capability T}}}{MoP_{\text{Capability max}}} \tag{7}$$

where $MoP_{\text{Capability}}$ is the Measure of Performance for a Capability (in Fig. 2), with $MoP_{\text{Capability max}}$ being the highest value and $MoP_{\text{Capability T}}$ being the lowest value at which the capability can still be performed. It is a percentage of the total capacity within which the system can still perform its required capability such as Voice communication.

III. Service Metrics for Resilient Systems

The approaches to defining and measuring resilience using State Space and Petri Nets have much to offer. The Petri Nets model leads to proposed measures that capture much of what we call "resilience" [4]. Similarly, the general State Space approach instantiates a fundamental understanding of resilience by separately monitoring operational state and service state [1]. Thus, we propose using a variant of the metrics formulated by [2] in the context of the State Space. Note that the Flexibility metric of [2] will be used unchanged from Eq. (6).

A fundamental attribute of a communications link is its information rate, usually measured in bits/s. Thus, changes in the information rate correspond to increases and decreases in communication service capability. We propose that the information rate be used as a basic Measure of Performance (*MoP*) for a communications capability (service state). This needs to be combined with a measure of operational state.

In the technical literature, this combining of two (quasi-) independent measurements is called *Conjoint Measurement* [8]. The correct measurement function for combining these two independent attributes is created by adding or multiplying the measures of each. Thus, we need an appropriate measure of operational status to multiply it by a Kbps MoP for a communications capability to reach a complete measure of the communications state.

Appropriate metrics for measuring operational status is a serious question that is beyond the scope of this paper. For that reason, we adopt a very fundamental measurement, "percentage of full operational status." For example, a perfectly operating system will have a measure of 100%, a partially degraded system will have a measure of 50%, and a much degraded system will have a measure of 10%.

With these measures in mind, we adopt the metrics developed by [2] and adapt them into general metrics that will quantify resilience by measuring changes of state, such as those given in Fig. 2.

A. Rate of System Change

Combining the measure of Operational Status with Service Status, results in a Measure of Performance (MoP) for the entire system:

$$MoP = (\text{Operational Status Percentage}) \cdot (\text{Service Information Rate}) \tag{8}$$

Therefore, System Tolerance, the rate of decline of the entire system, is expressed as:

$$\text{Rate of System Change} = \frac{MoP(t_{Final}) - MoP(t_{Initial})}{t_{Final} - t_{Initial}} \tag{9}$$

Here, MoP is the Measure of Performance of the entire system. Note that System Failure occurs when the service becomes Unacceptable and System Recovery occurs when the Unacceptable service returns to being at an Impaired state or better. See Table 1.

TABLE I. SYSTEM TOLERANCE, FAILURE, AND RECOVERY

	State of Service Parameter at time *t*:	
Type of System Change	$t_{Initial}$	t_{Final}
System Tolerance	Acceptable	Impaired
System Failure	Acceptable / Impaired	Unacceptable
System Recovery	Unacceptable	Acceptable / Impaired

A basic example of the System Tolerance metric is when a cell phone system gets overwhelmed by a spate of calls over a period of 5 minutes. Assume that the physical aspects of the service remain unchanged, but the rate of information decreases from 200 Kpbs to 20 Kpbs. The rate of decline (rate of bandwidth loss) is:

$$\frac{100\% \cdot 20Kbps - 100\% \cdot 200Kbps}{(5 \cdot 60)s} = -0.6Kbps / s$$

Here, the degradation of the system is measured by calculating the rate of decline of the MoP as the Operational and Service values move to a worse position in the Operational/Service state space.

B. System Capacity

System Capacity measures the percentage between maximum Capacity and minimum Capacity that will allow for the service to still function. The greater the Capacity, the more resilient the communications system. System Capacity can be expressed as:

$$\text{System Capacity} = \frac{MoP_{max} - MoP_{min}}{MoP_{max}} \quad (10)$$

where MoP_{max} is the maximum value of the Measure of Performance of the entire system, and MoP_{min} is that same measure at the value of the lowest level of capacity at which the service can still be performed. Assume the same cell phone system from the previous example, with a minimum performance requirement of 50% for the Operational state and 20 Kbps for the Service parameter. The System Capacity is then calculated to be:.

$$\frac{100\% \cdot 200\ Kbps - 50\% \cdot 20\ Kbps}{100\% \cdot 200\ Kbps} = 95\%$$

Thus, the range at which this cell phone system can perform is high, indicating significant system capacity.

C. Total Capacity Gain / Loss

The Total Capacity Gain / Loss is the percentage increase or decrease of a total communications capability and can be expressed as:

$$\text{Total Capacity} = \frac{\sum MoP_{New} - \sum MoP_{Old}}{\sum MoP_{Old}} \quad (11)$$

For example, if an emergency response team's methods of communications are cell phones and land mobile radios, then the addition of satellite phones will create an increase in overall capacity. Assume that all communications methods occur at 200 Kbps and there are 10 people in the Emergency Response Team (ERT), then the Total Capacity of the new system relative to the old system is:

$$\frac{(10 \cdot 100\% \cdot 3 \cdot 200) - (10 \cdot 100\% \cdot 2 \cdot 200)}{(10 \cdot 100\% \cdot 2 \cdot 200)} = 50\%$$

Thus, with the addition of the satellite phones, the capacity of the communications system has increased by 50%.

IV. APPLICATION OF METRICS: HURRICANE SCENARIO

Assume a natural disaster where a hurricane hits the East Coast of the United States after a tornado. Emergency management services are immediately called into duty to protect, provide, and secure affected residents. This scenario is used to measure the hurricane's effects on the resiliency of communications.

We employ notional State Space values (*MoP*) to illustrate the approach and calculate metrics based on "If, Then" assumptions. For example, assume that a level of partial degradation is 50% of operational effectiveness and severe degradation is 10% of operational effectiveness. Furthermore, assume Normal communication is 10 Kbps, Impaired is 5 Kbps, and Unacceptable is 0 Kbps, as shown in Table II.

TABLE II. NOTIONAL *MoP* VALUES

	Operational Status			
Service Parameter (*P*) Emergency Radios		Normal Operation	Partially Degraded	Severely Degraded
	Unacceptable	0 · 1 = 0	0 · 0.5 = 0	0 · 0.1 = 0
	Impaired	5 · 1 = 5	5 · 0.5 = 2.5	5 · 0.1 = 0.5
	Acceptable	10 · 1 = 10	10 · 0.5 = 5	10 · 0.1 = 1

Assume that the Highway Patrol has old two-way, 2 channel, radios that are vulnerable to congestion during heavy usage. During a tornado emergency prior to the hurricane, in a period of only 10 minutes, their radios decline in throughput from 3.5 Kpbs to 1.0 Kpbs. Although Service is impaired, the Operational Status of their communications systems remains at Normal. If this change in communications capability affects 280 members of the Highway Patrol, then the total System Tolerance of the their radios will decline to an Impaired state at the rate of -2.33 Kbps/s.

$$\frac{2 \cdot 280 \cdot 100\% \cdot 1.0Kbps - 2 \cdot 280 \cdot 100\% \cdot 3.5Kbps}{60s \cdot 10\,\text{min}} = -2.33Kbps / s$$

In terms of Survivability, the probability of a tornado occurring in any given year in this location is *P*(tornado) = 0.05. The probability of communications becoming congested with these old radios given a tornado is: *P*(Congestion | tornado) = 80%. Thus, the risk of radio outage for a tornado is 4%, making survivability 96%.

Not long after the tornado, a hurricane hits the East Coast with devastating fury. The local ERT quickly moves to respond effectively, as well as additional assets from other organizations. Suppose that 280 members of the Highway

Patrol team join the ERT. Each member of the team is given a new 800 MHz trunked radio. If the old radios have a throughput of 3.5 Kbps and 2 channels with a repeater for each channel and the new radios have a throughput of 9.6 Kbps and 5 channels with a repeater for each channel, then the Total Capacity will be increased by 586% =

$$\frac{100\% \cdot 5 \cdot 290 \cdot 9.6\ Kbps - 100\% \cdot 2 \cdot 290 \cdot 3.5\ Kbps}{100\% \cdot 2 \cdot 290 \cdot 3.5\ Kbps}$$

The system's flexibility also shows a significant increase because of the addition of repeaters. There are now 5 elements (5 repeaters) that can be used for a communications path. Assume that each member of the Highway Patrol also has a cell phone, which uses 2 of 5 cell phone towers in the area. Then, a Proportion of Use calculation will illustrate the communications system's flexibility. Assume that one repeater or two cell phone towers are used at any one time. There are 10 elements in the voice communications system and 15 possible pathways. Thus, the Proportion of Use is 2%.

$$\frac{(2\text{ towers})+(1\text{ repeater})}{\big((5\text{ radio paths})+(10\text{ cell paths})\big)\times(10\text{ elements})} = 2\%$$

This is a very small percentage, indicating high flexibility.

During the hurricane, assume there is a power outage that last 3 seconds until backup generators are activated. Of the 100 people in the Emergency Operations Center, 60 people have desktop computers and 40 people have laptops. After 3 hours, the backup generator runs out of fuel and the desktops cease to work. The Service state is Impaired. Over the next 3 hours, the laptop batteries are drained. The Service state moves from Impaired to Unacceptable while the Operational status is Partially Degraded. The decline in System Status over the 3-hour period is -0.37 Kbps/s:

$$\frac{50\% \cdot 40 \cdot 0\ Kbps - 100\% \cdot 40 \cdot 100\ Kbps}{10800s} = -0.37\ Kbs / s$$

Finally, after 4 hours, power is restored. The Service state moves to Acceptable, and the overall Operational status is Normal. This recovery of function occurs at a rate of 1.39 Kbps/s.

$$\frac{100\% \cdot 100 \cdot 200\ Kbps - 50\% \cdot 40 \cdot 0\ Kbps}{14400s} = 1.39\ Kbs / s$$

V. Discussion and Conclusion

In this paper, the authors examined some basic resilience concepts: Survivability, Tolerance, Flexibility, and Capacity. The presented resilience metrics were derived by taking the State Space concept of [1] and applying it to the Petri Net metrics of [2]. The basic properties of the presented metrics correspond to a common sense understanding of resilience. A loss of a communications service is indicated by a negative change in bandwidth. An increase in flexibility is shown by a smaller percentage of system parts being used to instantiate that communications capability. And an increase in communications capacity of a system is shown by a positive change in information rate over time.

Flexibility is largely synonymous with redundancy. The essence of increasing Flexibility is to increase the number of completely different ways to make a communications connection (e.g., path diversity). Equally important is ensuring that the independent channels of communications are actually independent (e.g., physical path diversity in additional to logical path diversity).

System Tolerance is the ability to gracefully decline. A communications system with redundancy is imperative to having high System Tolerance. This needs to be combined with rapid and effective fail-over technologies (e.g., network recovery and reconstitution). System Capacity can be improved by focusing on high throughput sources for critical communications. Service level agreement contracts should include special provisions such as priority.

Furthermore, well-designed plans for extending an hoc communications networks must be exercised. While it is impossible to anticipate all threats, a well-laid out plan and practiced contingency operations will usually make a difference. Well-practiced communications plans will be easier to customize during an actual national security event or emergency disaster.

References

[1] J.P.G. Sterbenz, D. Hutchinson, E.K. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Scholler, et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, pp. 1245-1265, Jun 2010.

[2] M. Pflanz and A. Levis, "An approach to evaluating resilience in command and control Architectures," *Conference on Systems Engineering Research*, vol. 8, pp. 141-146, 2012.

[3] M.A. Pflanz, "On the resilience of command and control architectures," Ph.D. dissertation, Volgenau School of Engineering, George Mason University, 2011.

[4] S. Jackson, *Architecting resilient systems: accident avoidance and survival and recovery from disruptions*, Hoboken, NJ: John Wiley & Sons, 2010.

[5] F.R.H Valraud and A.H. Levis, "On the quantitative evaluation of functionality in distributed intelligence systems," in *Proceedings IEEE International Symposium on Intelligent Control*, pp. 88-93, 1989.

[6] V. Bouthonnier and A.H. Levis, "Effectiveness analysis of C-3 systems," *IEEE Transactions on Systems Man and Cybernetics*, vol. 14, pp. 48-54, 1984.

[7] R.E. Ball, *The fundamentals of aircraft combat survivability analysis and design*, 2nd ed., Reston, VA: American Institute of Aeronautics and Astronautics, 2003.

[8] D.H. Krantz, R.D. Luce, P. Suppes, and A. Tversky, *Foundations of measurement*, New York, NY: Academic Press, 1971.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
09-08-15	Non-Standard Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Resilient National Security and Emergency Preparedness Communications: Service Metrics	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Robert S. Sneddon Serena Chan	ER-5-3697
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-5496 H 15-000459

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Joseph Wassel, DoD C4 Resilience & Mission Assurance 1000 Defense Pentagon, Washington DC 20301 Department of Defense Chief Information Officer	DoD C4 RMA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Serena Chan

14. ABSTRACT

Resilient communications are critically important in the event of a national security crisis or disaster. In the event of a significant threat to public safety, communications for national security and emergency preparedness must continue to provide an acceptable level of service for senior leader decision makers and first responders. If primary communications are lost, then resiliency is the ability for rapid and effective reconstitution or utilization of alternate means. This paper introduces concepts of communications resilience and suggests appropriate service metrics. The concepts of survivability, tolerance, flexibility, and capacity are used to define system tolerance, system flexibility, and system capacity.

15. SUBJECT TERMS:

Resilience, Reliability, Communications, Service Metrics, Tolerance, Flexibility, Capacity, Survivability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Joseph Wassel, DoD C4 Resilience & Mission Assurance
a. REPORT	b. ABSTRACT	c. THIS PAGE	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code)
Unclassified	Unclassified	Unclassified			703-901-7360