PRIORITY INTERNATIONAL COMMUNICATIONS

STAYING CONNECTED IN TIMES OF CRISIS

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

ISBN: 978-0-9856824-2-2

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow. For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info

www.ewi.info

PRIORITY INTERNATIONAL COMMUNICATIONS

Staying Connected in Times of Crisis

Karl Frederick Rauscher and **Stuart Goldman**

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

Dedication

To those who stand by, ready to respond to the worst disasters we face.

FOREWORD

During times of crisis, countries need effective communications more than ever. But during recent tragedies like Japan's tsunami and nuclear meltdown in 2011, the July 7, 2005 London bombings, the 2008 Mumbai and September 11, 2001 terrorist attacks, critical communications failed to make it through congested networks. Each year, around the world, lives and property are lost because we do not prioritize the international communications that matter most.

The EastWest Institute (EWI), together with world-class experts and stakeholders, has articulated the straightforward steps needed to deploy a Priority International Communications capability. EWI submits that in this globalized world, we must all prepare for international emergencies. The first step is for countries to be able to communicate reliably during such crises. But despite existing standards addressing how to do so technologically, this ability remains unrealized.

The Priority International Communications report offers immediate solutions to the present impasse. Government officials charged with the protection of their citizens and private sector leaders on whose systems we all depend should take these recommendations to heart. The authors and contributors have consulted world-class technical and business experts from around the world, and present clear, effective recommendations. They have marked a clear path forward and now we must take it.

We trust that this report will prompt the private and public sectors to take action and implement these recommendations.

Sir Peter Bonfield, CBE, FREng
Chairman,NXP Semiconductors
Former CEO and Chairman, BT plc, UK

Michael Chertoff
Co-founder and Managing Principal, Chertoff Group
Former U.S. Secretary of Homeland Security

Alexander Gurko
President, Partnership for Development and
Use of Satellite Navigation Technologies
Member, President's Council for Economic
Modernisation and Innovative Development, Russia
Former CEO, NIS GLONASS

Som Mittal
President, National Association of Software and
Services Companies (NASSCOM), India
Former Senior Vice President, Hewlett Packard

Plamen Vatchkov
Nationl Cybersecurity Coordinator of Bulgaria
Former Chairman of the Council, International
Telecommunication Union (ITU)

Acknowledgements

Rowan Williams,
for converting lessons learned from the 2009 wildfires to
a priority scheme implementation for Australia

David Mowbry,
for critical analysis of the network congestion surrounding
the July 7, 2005 London bombings

Harry D. Raduege, Jr., Brenton Greene, Frank Suraci,
John Graves and the NCS team,
for dedication to ensuring priority communications on public networks in the U.S. during the
September 11, 2001 terrorist attacks and 2005 Hurricane Katrina and New Orleans flood

Eduard Mracka,
for leadership in raising awareness of priority communications
for NATO and Central Europe

Alison Kung, Anneleen Roggeman and Franz-Stefan Gady,
for their assistance in numerous aspects of the Worldwide Cybersecurity Initiative

Greg Austin, Terry Morgan and Vartan Sarkissian,
for their early support of the Worldwide Cybersecurity Initiative

Andrew Nagorski, Abigail Rabinowitz, Thomas Lynch and Dragan Stojanovski,
for their care in assuring the quality of this document's publication

John Edwin Mroz, Ross Perot, Jr., Francis Finlay and Armen Sarkissian,
for their leadership of the EastWest Institute

each of the financial sponsors for EWI's Worldwide Cybersecurity Initiative,
without whose support this report would not have been possible

PREFACE

We are pleased to submit this report, which presents four immediately actionable recommendations that, if implemented, will save lives and property around the world. If we act now, we can assure that the most important communications get through during catastrophes, when networks are often massively congested. At a very low cost, we can do something of very high value for humanity.

All of us have direct experience with priority communications. Both Stephen Malphrus, who has been a unique stakeholder voice for priority communications, and Karl Rauscher, this report's co-author, have used the United States' national-level priority communications capability in the "heat of battle" during historic crises. Stephen relied on the capability from the inner core of the Federal Reserve System in Washington, D.C. to help restore New York City's financial markets after the September 11 attacks. During Hurricane Katrina, Karl used the capability to cast a lifeline to stranded victims whose failed emergency 911 calls were observed by volunteers conducting an innovative search-and-rescue through cyberspace. Co-author Stuart Goldman was one of the pioneering designers and implementers of the first priority algorithms to be used in communications networks more than two decades ago. He has invented numerous enhancements for the capability to prioritize communications, and is now in his fourth decade of contributing to related areas in national and international standards.

Given the underlying mathematics of emerging network technologies and services, congestion-caused outages will become increasingly common. This decade, our devices' thirst for bandwidth has made disruptions due to payload extremes as common as the software glitches of the 1980s. Fortunately, priority schemes are a proven way to increase the probability of completion during congestion. We each testify to the effectiveness of priority schemes. Their extension to international reach is a long overdue step.

Finally, we sincerely recognize each of the experts and stakeholders listed on the next page, whose high-quality contributions to this work provided necessary rigor and breadth of international perspective.

Karl Frederick Rauscher
Distinguished Fellow & CTO, EastWest Institute
President, Wireless Emergency Response Team
Bell Labs Fellow

Stuart Goldman

Stuart Goldman
Chair (fmr), ATIS Network Interoperability Forum
Bell Labs Fellow (fmr AGCS, Lucent, Alcatel-Lucent)
Contributor, IETF, ITU-T & ATIS standards

Stephen Malphrus
Staff Director for Management (fmr), U.S. Federal Reserve System
Chairman (fmr), U.S. President's Council on Y2K Financial Sector Group
Honorary Co-Signer

Contributors

The following individuals served as subject-matter experts during the development of this report. Their contributions from their respective fields of experience as a stakeholder, a corporate manager or technical expert were essential to the analysis, conclusions and guidance presented herein.

Ian Abbott, Nuclear Decommissioning Authority, U.K.

Sanjay Bahl, Consultant, India

James Bodner, The Cohen Group

Sir Peter Bonfield, NXP Semiconductors

Ingrid Caples, U.S. Department of Health and Human Services

Peter Castenfelt, EastWest Institute

Christopher Clegg, Ernst & Young plc

Jack Edwards, Digicom, Inc.

Andrei Korotkov (dec.), Moscow State University of International Relations

Richard Krock, IEEE Technical Committee on Communications Quality & Reliability

Michael Litherland, Huawei

Gerald McQuaid, Vodafone

Scott Morris, U.S. Nuclear Regulatory Commission

Eduard Mracka, Ministry of Transport and Telecommunications, Slovak Republic

Michael Moore, Huawei

Ram Narain, Ministry of Communications & IT,
Department of Telecommunications, India

Wayne Pacine, U.S. Federal Reserve Board

Gulshan Rai, Ministry of Communications & IT, Department of IT, India

Phyllis Schneck, McAfee

Leonid Todorov, The Coordination Center for TLD .RU

Henrik Torgersen, Telenor ASA

Niels Asger Wille-Jorgensen, Ministry of Foreign Affairs, Denmark

CONTENTS

List of Figures

List of Tables

September 2001

In the immediate aftermath of the September 11, 2001 terrorist attacks, then-U.S. Federal Reserve Board Chairman Alan Greenspan was blocked from communicating with the United States from Basel, Switzerland, although this was a financial crisis of the highest order. He and many others were virtually isolated for hours because communications networks were massively congested with far more traffic than they could handle.

March 2011

The earthquake that spawned a tsunami and led to the Fukushima nuclear meltdown also damaged the undersea cables that connect Japan to the rest of the world. This greatly reduced the country's network capacity, which hobbled crisis response in the weeks that followed.

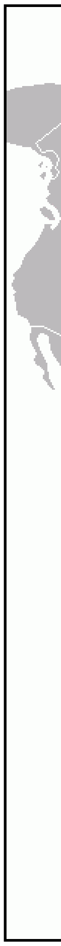
July 2011

Phone networks were jammed for hours after the triple bombing attack in Mumbai. Maharashtra Chief Minister Prithviraj Chavan reported that he was cut off from his police force due to jammed phone networks during the immediate response to the attack. "People started calling near and dear ones to inquire about their well-being. The calls were made not only from within the city, but also from all over the country and even abroad."[1]

Similar paralysis of limited network resources is experienced for hours, days and even weeks when major catastrophes strike. The result is the unnecessary additional loss of life and property.

[1] A telecom source quoted in Call Traffic Surge Jammed Mobile Phone Networks, The Times of India, July 14, 2011.

1. Executive Summary



Surprisingly, only a few countries have a priority communications capability in place. Furthermore, there is no international system for giving important calls priority at crowded gateways.

When catastrophe strikes, lives, property and the environment can depend on a call that absolutely must go through. Recognizing this, some countries give calls from government-authorized users preferential treatment in a crowded network. For instance, in the United States, this service is provided through the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). GETS maintains a database of authorized users who are granted an identification code. When dialing during an emergency, the user's call is recognized by software in public network gear, which gives it special treatment, greatly increasing the likelihood that the call will complete on the first attempt. GETS is just one example of a "priority communications capability." These systems can also give priority to crucial text messages, e-mails and any form of digital information.

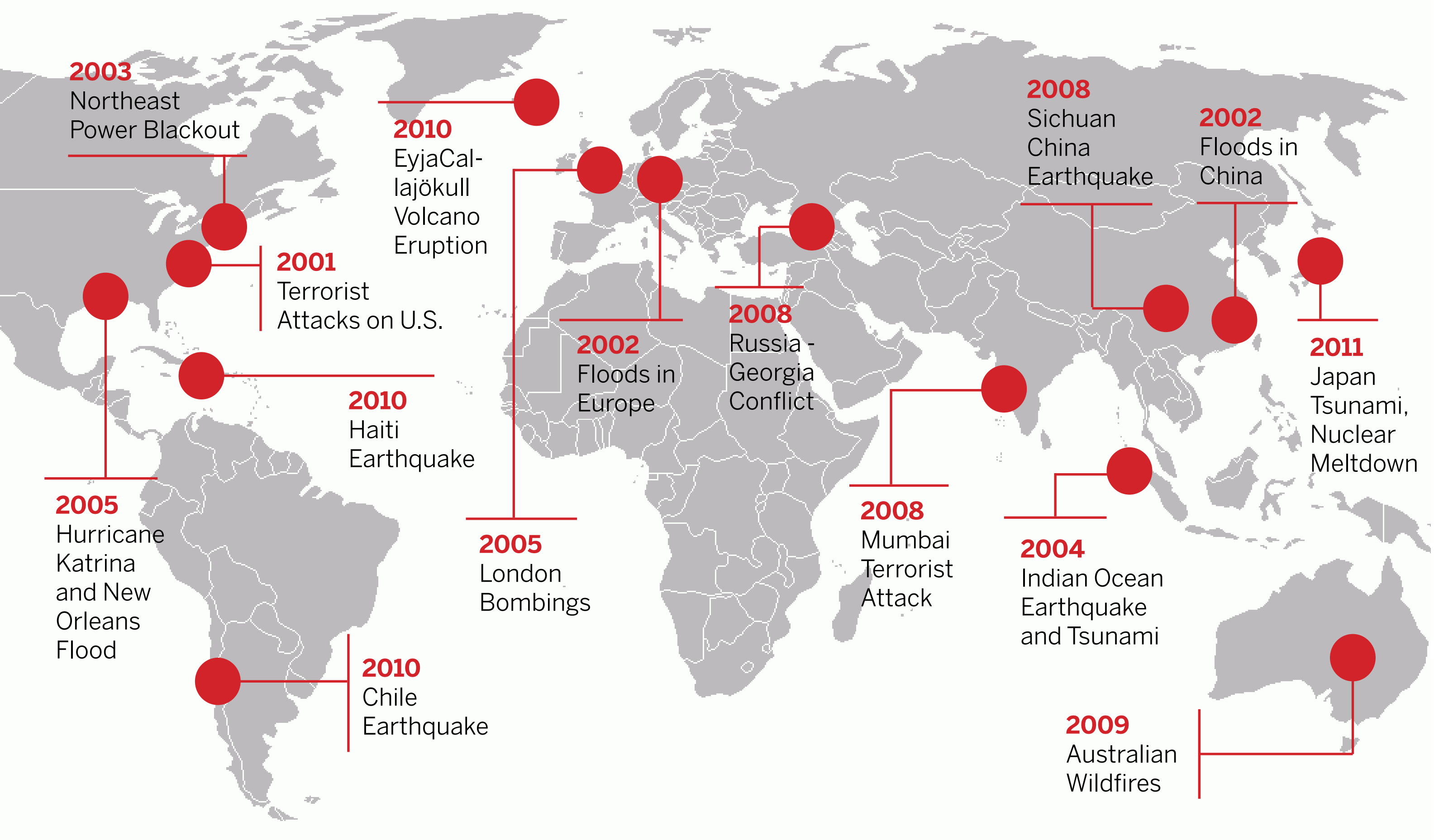
Surprisingly, only a few countries have a priority communications capability in place. Furthermore, there is no international system for giving important calls priority at crowded gateways, where countries' networks connect (with the exception of one connection between the United States and Canada). This is a missed opportunity, particularly as standards-based technical solutions have existed for the past decade. We just need to put these solutions in place.

To that end, this report proposes a Priority International Communications (PIC) capability that would help important communications cross borders more reliably. A PIC capability could make the crucial difference between whether or not life-sustaining functions are supported during a major crisis, when public networks are most congested.[2] In addition, a PIC capability could connect governments' private networks, like those some countries maintain between police and emergency personnel. The problem is urgent, as networks are becoming increasingly overloaded by new communications services, like HD imaging and gaming. To ensure the continuous communications vital to public safety, economic stability and security, we must act now. Developed with the input of technical and business experts and stakeholders around the world, this report lays out the first steps for implementing a low-cost PIC capability that will provide preferential treatment for the most important communications in times of crisis.

The Recommendations

This report presents four immediately actionable recommendations that, if implemented, would allow government-authorized users to communicate even when networks are jammed. These authorized users would include public or private sector individuals with critical roles in times of crisis. Among them: critical infrastructure operators (communi-

[2] This work will often refer to the Government Emergency Services and the Wireless Priority Services in the U.S. as examples. But in the present context, PIC is an extension of priority services beyond traditional telephony (i.e. voice calls) to include all 21st century electronic communications that are increasingly integrated as essential to the operation of important government or civil functions.



cations, energy, financial services and transportation); public safety officials (health care, local government, emergency management) and individuals with national security responsibilities like defense.

Here, we present steps to make our international communications systems more "robust." Robustness is the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions.[3] In a robust international network, important communications will complete even during times of crisis, when traffic loads are extreme and network capacity may well be diminished.

In this report, we call for (a) governments to provide up-to-date emergency preparedness capabilities that include high-assurance international connectivity, (b) for the international communications industry to develop innovative strategies for implementing these successful technologies and (c) for stakeholders to articulate their needs to government, spelling out the real consequences for failed communications in a crisis. Each recommendation is fully presented in Section 4.

RECOMMENDATION 1
Championing Robust International Communications
(Section 4.1)

"Our critical functions cannot operate without connectivity between New York, London and India."
- CIO of a major international financial services firm

Government agencies and other stakeholders must articulate their need for robust international communications. In today's world, multinational enterprises and governments require international communications for their most critical functions. Still, even the most developed and technologically savvy countries accept blocked communications during a crisis.

Governments and other stakeholders should champion the need for Priority International Communications.

[3] *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990.

The alternatives to this approach, and their consequences, include:

- Do nothing and defend the position that failed communication is unavoidable in the face of network congestion during catastrophes… perpetuating unnecessary loss of life and property;
- Wait for industry to develop these capabilities without funding support…which likely won't happen, as there is little economic incentive;
- Do nothing and learn from lessons of the tragedies that occur…accepting responsibility for unnecessary additional loss of life and property.

Governments are responsible for protecting citizens' interests, and citizens expect their leaders to be prepared for emergencies.

RECOMMENDATION 2 Due Diligence for Modern International Crisis Management

(Section 4.2)

"We were winging it."
- Scott Morris, Deputy Director for Incident Response, U.S. Nuclear Regulatory Commission, in reference to the need for better preparedness for coordinating and cooperating in an international incident like the Fukushima crisis.[4]

Governments are responsible for protecting citizens' interests, and citizens expect their leaders to be prepared for emergencies. Experts and stakeholders understand that Priority International Communications are vital to a country's well-being. This report submits that to be considered adequately prepared for emergencies, governments must install available technological solutions that ensure high probability of completion for the most critical international communications.

Governments should maintain a capability for authorized users to communicate internationally with priority over public networks during times of congestion.

Alternatives to this approach, and their consequences, include the following:

- Governments do not implement any priority communications capability … resulting in greatly impeded communications during and after major crises;
- Governments rely on national level emergency communications schemes… placing their country at risk of being significantly isolated during and immediately after a major crisis;
- Governments fail to adequately fund PIC… and the capability is either not implemented or implemented but poorly maintained, limiting its effectiveness in a crisis;
- Governments fail to effectively identify and manage those individuals with critical emergency response functions… rendering PIC to be of little value. If everybody can have priority, then, in reality, no one has priority.

RECOMMENDATION 3 Network Provisioning of Priority International Communications

(Section 4.3)

"Across several continents, governments are suddenly looking for solutions to network congestion."
- Gerald McQuaid, Security Relations Manager, Vodafone

Network operators play a vital role in helping countries implement and maintain a PIC capability. Network operators own, operate and maintain the equipment that makes communications services possible. To make PIC a reality, network operators around the world will need to cooperate in how they implement "gateways," the network nodes that lead to other networks. Gateways currently serve as an interface between countries' communications networks, making them compatible. Using current international standards, these gateways can also be used to map priority communications schemes.

Network operators should provide leadership, cooperating with each other and governments to implement and maintain Priority International Communications capabilities in their networks.

Alternatives to this approach, and their consequences, include the following:

[4] Speech to the Government Emergency Telecommunications Service (EGTS) and Wireless Priority Service (WPS) User Council Meeting, Mclean, VA, January 12, 2012.

- Network operators are incapable of reaching an arrangement to support PIC... as a result, their network lacks international robustness when congested and their country is suboptimally prepared for major crises;
- In a competitive market, a single network operator is selected, or attempts to be, the sole provider of PIC...having the effect of less redundancy in network connectivity and possibly less access.

RECOMMENDATION 4
Technology Deployment Leadership
(Section 4.4)

“Disruptions caused by payload extremes in this decade are akin to the software glitches of the 80s.”
- Karl Rauscher and Stu Goldman

Major equipment suppliers do the “heavy lifting” when it comes to technology development. Because PIC will work with existing end-user devices and network systems, the primary deliverable for equipment suppliers is software that will reside on existing network equipment. Several equipment suppliers have already programmed their systems with standards-based software to support countries that have a national-level PIC capability. In fact, one benefit of more coordination on priority communications at the international level is that the overall costs for an individual country can be expected to decrease as the benefits of higher volumes in the marketplace come into play.

Network equipment suppliers should provide international standards-based software within their systems to support Priority International Communications capabilities.

Alternatives to this approach, and their consequences, include the following:

- Network equipment suppliers do not implement PIC capabilities in their equipment . . . resulting in inadequately robust networks;
- Network equipment suppliers implement non-standards-based protocols to support PIC . . . resulting in incompatibility between different networks;
- Network equipment suppliers make an initial deployment of a PIC capability but fail to update with evolving standards . . . resulting in limited capabilities, as new services and applications emerge.

The implementation of these recommendations will dramatically improve the robustness of communications around the world. Given society’s immeasurable dependence on communications-based services, it is imperative that the most critical functions be supported when they are needed most.

The implementation of these recommendations will dramatically improve the robustness of communications around the world.

Key Observations: Why We Should Act Now

Section 3 outlines 40 Key Observations that offer compelling reasons for addressing network congestion right now. They also reveal the rationale behind the report’s recommendations. Here are four of those observations:

Key Observation No. 4. National-level priority schemes are field-tested and effective.

The value of national-level PIC capabilities has been proven. For instance, during September 11, 2001, the United States’ capability kept key communications lines open. According to Brenton Greene, former director of the National Communications System of the Department of Homeland Security, “GETS allowed significant priority access for over 10,000 calls with over 95% completion rate at a time when networks were saturated and nobody else could get through.”

Key Observation No. 12. Essential agreements, standards, policy and regulations (ASPR) that support PIC capabilities are stalled.

Although the concepts and even international protocols for priority communications across borders have existed for over a decade, the implementation of these standards is stalled. Governments clearly value PIC, as they developed these standards, so deploying the policy seems to be the stopping point. Why? The issue (essentially, being prepared for low-probability events) is not sufficiently visible, and the task of getting countries to cooperate is dauntingly complex.

Key Observation No. 20. Network-capacity limitations are a reasonable trade-off for cost management.

Communications networks are engineered and provisioned for normal everyday peaks, and even beyond-normal situations. Networks operators want to carry traffic; that is their business. However, building and maintaining networks to carry 100% of the potential traffic load is not feasible. If networks were designed and built to carry the extreme levels of the traffic theoretically possible given end-users' devices, the monthly price for services would increase by an order of magnitude or more. So, it is simply too expensive for network operators to increase capacity enough to account for major emergencies; instead, we must prioritize communications.

Key Observation No. 32. Priority communications capabilities are very low cost compared to other solutions.

When leveraging public networks, the return on investment for creating PIC capabilities is extremely high, given that the cost is primarily directed toward installing software on existing networks. For comparison's sake, to achieve equivalent high assurance for communications offered ubiquitously across a country via a dedicated network, one would have to pay for hardware and software that make up the network elements, the transport to connect the elements, staff to deploy, operate and maintain, and supporting infrastructure like buildings and vehicles. In addition, the end-users would need to be provided with separate dedicated devices, all of which would need to be continuously upgraded.

Kolchoz

The complete list of Key Observations is presented in Section 3.

Next Steps

The world's government and private sector decision makers have a less-than-acceptable probability of completing critical communications during an international crisis. What may likely be a 90% blocking rate for all communications on public networks during a crisis could readily be addressed with proven low-cost technical solutions, so that stakeholders instead experience a 90% completion rate for essential communications.

With this report, the EastWest Institute is raising awareness of this underappreciated vulnerability. In addition, the institute is convening world-class experts and stakeholders to work out policy solutions, and will champion the mobilization of resources to implement a PIC capability.

Each of the four recommendations is immediately actionable. Further, the report provides suggested next steps to help build on the momentum that has been generated from the consensus around this report (Section 4).

The institute will be joining with key stakeholders, and leaders from industry and government to conduct outreach with the aim of broad implementation of each of these recommendations, and plans to post updates on progress on its website, www.ewi.info.

2. Introduction

Making cyberspace safer, more stable and more secure is a global challenge – one that cannot be solved by a single company or country.

This section provides background information to frame the discussion on Priority International Communications, including the EastWest Institute's objectives and approach to problem solving in cybersecurity. Here, we also explain the scope of this report and analyze existing capabilities.

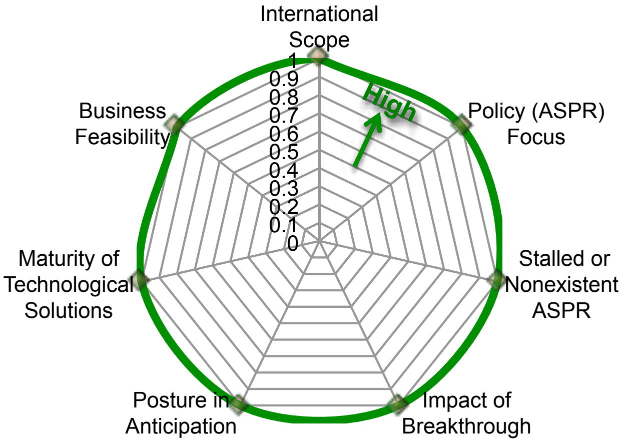
2.1 Why the EastWest Institute is Tackling Priority Communications

Making cyberspace safer, more stable and more secure is a global challenge—one that cannot be solved by a single company or country. That is why the EastWest Institute launched the Worldwide Cybersecurity Initiative (WCI) in 2009, bringing together government and corporate partners to work together in new ways to take on the biggest problems in cyberspace.[5]

Drawing on a 30-year history of building trust and solving seemingly intractable problems, EWI formed the Cyber40, a coalition of representatives from the world's most digitally advanced countries and other countries critical to international security.[6] EWI also collaborates closely with the Institute of Electrical and Electronics Engineers (IEEE).[7] The WCI aims to: build trust among the biggest cyberspace powers (namely China, the EU, India, Russia and the U.S.); secure agreements for norms of behavior in cyberspace, with a particular focus on cyber conflict; champion preparedness for emergencies in cyberspace; and encourage the private sector towards new leadership in implementing innovative solutions.

Why has EWI chosen to focus on the problem of priority communications, given the host of problems in cyberspace? The WCI uses criteria to filter candidate issues, principally whether the subject matter is primarily concerned with Agreements, Standards, Policy and Regulations (ASPR or "Policy" for short) and whether that issue is either stalled or altogether ignored. The criteria ask:

- Is the subject international in scope?
- Is the issue a policy focus?
- Is the policy stalled or nonexistent?
- What would be the impact of a breakthrough?
- Is our posture proactive?
- Are the needed technology solutions mature?
- Is the business proposition feasible?



Score = 1.0

Figure 1. EWI Scoring of the PIC Issue

[5] The WCI commenced in April of 2009 with a meeting at the U.S. Federal Reserve Board in Washington, D.C.

[6] See Appendix B for the EWI Cyber40.

[7] The IEEE Communications Society and EWI established a partnership through a *Memorandum of Understanding for the Promotion of Cyberspace Safety, Stability and Security,* May 2010 in Dallas, Texas.

Figure 2. Interactive PIC Breakthrough Group Session at the 2nd Worldwide Cybersecurity Summit (London) Left to right: Lt. Gen. (ret.) Harry D. Raduege, Jr., Sir Peter Bonfield, Stuart Goldman, James Bodner, Richard Krock, Wayne Pacine.

As shown in Figure 1, the PIC issue obtained an aggregate perfect score of "1.0" across these criteria. This is the only candidate issue that has been graded a perfect score to date.

Other breakthrough group focus areas currently underway are addressing issues related to norms of behavior in cyberspace, the integrity of Information and Communications Technology (ICT) development and supply chains, emergency preparedness of the financial services sector in cyberspace, the reliability of the global undersea communications cable infrastructure (GUCCI), measuring the cybersecurity problem and protecting youth and digital citizenship.

Based on these criteria, PIC is a perfect candidate for attention. In addition, PIC is also tightly aligned with every strategic high-level objective of the WCI. PIC would help countries prepare for emergencies in cyberspace, as it would enable robust international communications in the face of a major crisis. In addition it encourages the private sector to take innovative first steps toward making Priority International Communications a reality, thereby serving as an example of private sector leadership. This breakthrough work also exhorts countries to build mutual trust as they begin to deploy schemes for Priority International Communications interfaces. Finally, the implementation of international standards for handling authorized priority communications across international borders will provide much-needed clarification about what behavior is appropriate in cyberspace during catastrophes.

2.2 Understanding Network Congestion

PIC addresses the problem of congestion in international networks that prevents important communications from taking place. Network congestion is most commonly experienced during and following a large disaster, but can also result from damage that impairs network throughput. Additionally, the nature of emerging network architectures and services makes congestion-related communication failures significantly more likely.

The Eight Ingredient (8i) framework for ICT infrastructure is a useful method for understanding exactly how congestion occurs. It is a systematic and comprehensive framework that (a) takes an ingredient approach, (b) is comprehensive of all of the ingredients, and (c) specifies the eight ingredients as Environ-

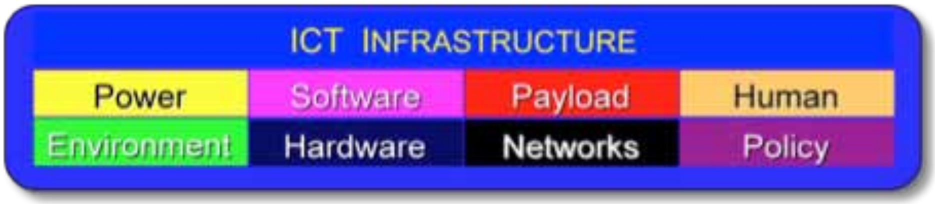


Figure 3. 8i Framework for ICT Infrastructure[8]

Each of these eight ingredients is essential for communications services to work. Failure of any one would prevent or seriously impair services.

ment, Power, Hardware, Software, Network, Payload, Human and ASPR (Agreements, Standards, Policy and Regulations, abbreviated as "Policy") (Figure 3). This framework is used here for understanding the exact role that the intrinsic vulnerabilities have in network congestion.

Each of these eight ingredients is essential for communications services to work. Failure of any one would prevent or seriously impair services. Such failures might appear as network congestion from an end user perspective, but what is actually happening is infrastructure failure (Figure 4). By contrast, network congestion means that the infrastructure is working with the exception that the limited network capacity cannot meet the traffic demands.

Two of the ingredients can cause congestion when their intrinsic vulnerabilities are exercised: Payload, which is subject to statistical variation and extreme loads; and the Network itself, which have capacity limits. Of course, each of these susceptibilities is known. Therefore ASPR, which enables entities to anticipate the behavior of other entities, has intrinsic vulnerabilities, which include lack of ASPR, outdated ASPR, unimplemented ASPR, boundary limitations, ability to stress vulnerabilities and the ability to infuse vulnerabilities.

The intrinsic vulnerabilities themselves are passive. They are exercised by threats, which are active agents. Threats are discussed in the following section.

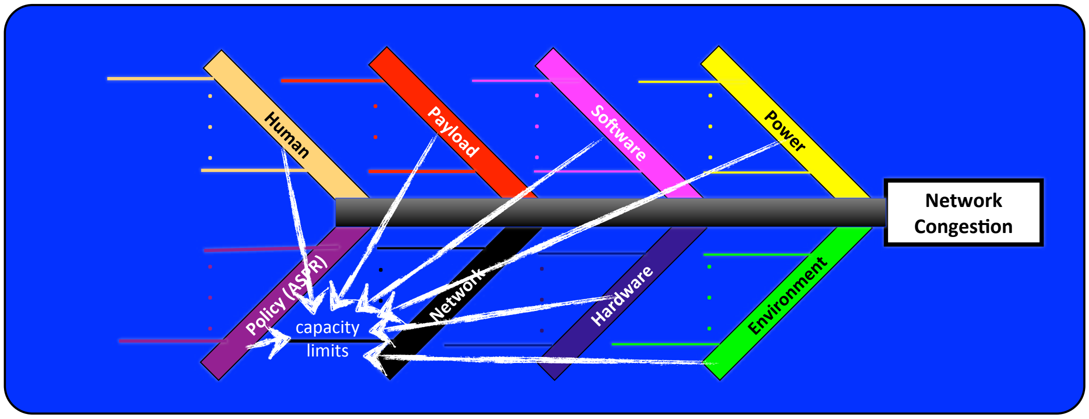


Figure 4. Ishikawa Diagram for Infrastructure Failure

In the discussion of intrinsic vulnerabilities, the types of threats are not relevant. For practical purposes, they are of infinite variety and their appearance is often unpredictable. Rather, the focus here is on effectively living with the intrinsic vulnerabilities, since they cannot be removed from their respective ingredients. Since the intrinsic vulnerabilities are known, they can be anticipated and addressed beforehand. The objective then is to

[8] Rauscher, Karl. F., Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop, www.comsoc.org/~cqr; ATIS Telecom Glossary, www.atis.org ; Rauscher, Karl, F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

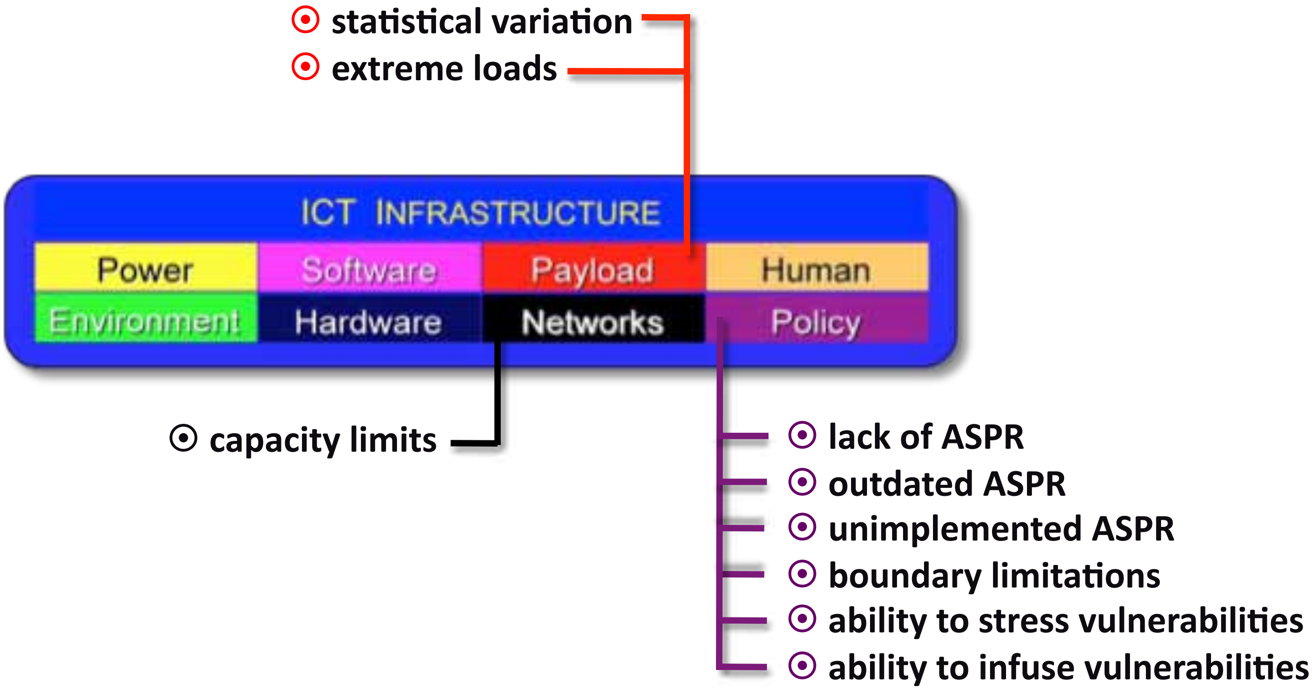


Figure 5. Intrinsic Vulnerabilities Associated with Network Congestion

implement countermeasures to either prevent their being exercised or to ameliorate their impact should they be exercised. Figure 6 shows a cause-effect diagram of the intrinsic vulnerabilities of the Payload, Network and Policy ingredients. The other intrinsic vulnerabilities are not shown. Figure 9 further develops this picture by showing the primary driving force in the relationship between these susceptibilities.

The Payload ingredient inherently carries with it statistical variation, which includes extreme loads, another intrinsic vulnerability.

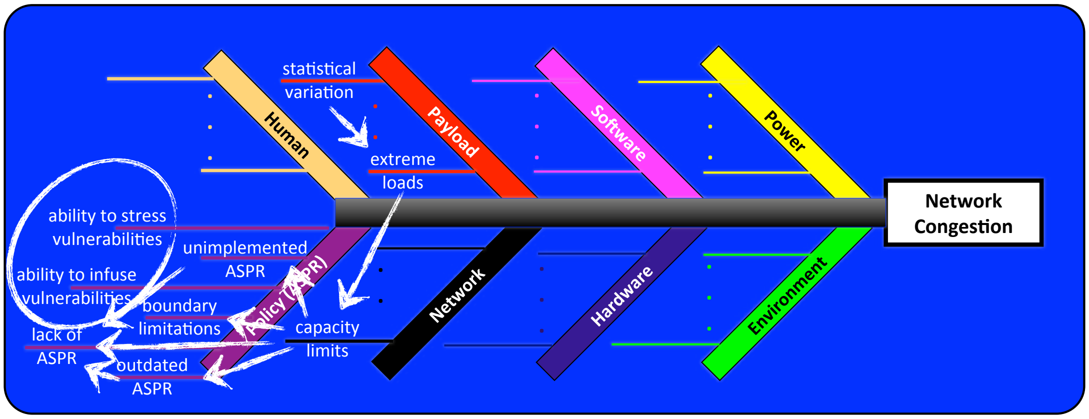


Figure 6. Ishikawa Diagram for Network Congestion with Interrelationship Diagraph

These susceptibilities of Payload are always there and can compete within this ingredient to the detriment of itself. The vulnerabilities intrinsic to the Payload ingredient are problematic because the Network ingredient has similarly intrinsic vulnerabilities, namely capacity limitations. Exercising the capacity limitations are traffic loads that exceed the engineered limitations. Suboptimum responses for addressing the challenges discussed thus far are more homogenous traffic patterns, less traffic or more network capacity—each of which, respectively, limits free use of services, competes with the growth of services or increases the expense of services.[9] More insightful countermeasure concepts for addressing these problems will account for broader interests, including economic, implementation, and the end user experience (Table 1).

[9] Key Observation No. 20, *Network capacity limitations are a reasonable trade-off for cost management.*

Ingredient	Vulnerability	Concept
Network	capacity limitations	utilize limited capacity for most critical functions (i.e. provide robustness)
Payload	statistical variation	anticipate increasing need to handle variability
	extreme loads	prioritize traffic
Policy (ASPR)	unimplemented ASPR	implement existing international standards
	lack of ASPR	create international gateway interfaces for level matching and other policies
	boundary limitations	interface priority schemes at gateways
	outdated ASPR	SDOs integrate PIC with ongoing standards evolution
	ability to stress vulnerabilities	deploy emerging protocols with priority capabilities
	ability to infuse vulnerabilities	implement abnormal usage detection at gateways

Table 1. Concepts for Addressing Intrinsic Vulnerabilities Causing Network Congestion

The PIC capabilities advocated in this report are countermeasures for dealing with the ever-present intrinsic vulnerabilities of the Network and Payload ingredients. In order to be optimally effective, the approach also emphasizes key considerations for the Policy ingredient.

2.3 Extreme Events

The previous section discussed the underlying vulnerabilities intrinsic to communications infrastructure. This section focuses on "the other side of the equation"—the threats. While the vulnerabilities are ever-present and passive, threats are active, but their appearance in space and time is spasmodic.

There are many situations that could stimulate congestion in communications networks. These include natural disasters, such as earthquakes, floods, heat waves, hurricanes, ice and snow storms, insect invasions, sand and wind storms, solar flares, tsunamis, volcanic eruptions and wildfires. Likewise, human actions can cause massive congestion with intentional acts like civil upheaval, political revolutions, military escalations, war, or physical, biological or chemical terrorist attacks. Congestion can also be caused by unintentional "man-made causes," such as technological failures.

Table 2 outlines the relationship between threats and vulnerabilities. A crucial observation here is that we can either primarily focus on threats or vulnerabilities. A focus on the former faces a limitless list of possible scenarios, for which the appearance of each is unpredictable. A focus on the latter is bound to the finite number of intrinsic vulnerabilities that are not oriented around predicting specific future events, but rather on far-reaching benefits that extend to countless threat scenarios. Therefore, the vulnerability approach is far more efficient and effective.

	Ingredient & Intrinsic Vulnerability			
	Network	Payload		Other Ingredient
Threat	capacity limitations	statistical variation	extreme loads	
Earthquake destroys network infrastructure	■			
Earthquake stimulates massive traffic overload		🟥	🟥	
Flood destroys network infrastructure	■			🟩 🟦
Flood stimulates massive traffic overload		🟥	🟥	
Disgruntled network operator employee sabotages network equipment	■			🟦 🟧
Ice storm destroys network infrastructure	■			🟦
Ice storm stimulates massive traffic overload		🟥	🟥	
Wildfires destroy network infrastructure	■			🟩 🟦
Wildfires stimulate massive traffic overload		🟥	🟥	
Terrorist attack destroys network infrastructure as intended target	■			🟩 🟦
Terrorist attack destroys network infrastructure as collateral damage	■			
Terrorist attack stimulates massive traffic overload		🟥	🟥	
Viral computer game causes network overload		🟥	🟥	
Viral computer game causes intermittent network overload		🟥		
Undersea landslide destroys global undersea communications cable infrastructure (GUCCI)	■			🟩 🟦
Thieves lift and remove GUCCI	■			🟦
High winds cause ships to drag anchors at GUCCI chokepoint causing multiple cuts	■			🟦
Outbreak of war motivates strategic cuts in GUCCI	■			🟦
Fishing activity near a GUCCI chokepoint results in multiple cable cuts	■			
Software design error causes widespread network equipment failure	■			🟪
Hardware design error causes widespread network failure	■			🟦
A denial of service attack (DoS) causes massive traffic overload		🟥		
A denial of service attack (DoS) causes intermittent traffic patterns that confuse networks			🟥	
Solar flares (coronal mass ejections) cause widespread network impairments	■			🟦
Civil upheaval targets critical infrastructure, impairing networks	■			🟩 🟨 🟦
Civil upheaval is accompanied by massive traffic overloads		🟥	🟥	
Pandemic depletes communications infrastructure workforce, impairing operations	■			🟩 🟨 🟦 🟪 🟧
Pandemic causes unusual traffic patterns (i.e. higher egress traffic from residential communities during work hours)		🟥		
Pandemic is accompanied by massive traffic overloads			🟥	
Volcanic eruption destroys network infrastructure	■			🟩 🟨 🟦
Volcanic eruption stimulates massive traffic overload		🟥	🟥	
Nuclear meltdown destroys network infrastructure	■			🟩 🟨 🟦
Nuclear meltdown causes workforce absence	■			🟧
Nuclear meltdown stimulates massive traffic overload		🟥	🟥	
Tsunami destroys network infrastructure	■			🟩 🟨 🟦
Tsunami stimulates massive traffic overload		🟥	🟥	
Heat wave stimulates massive traffic overload		🟥	🟥	
Long term commercial power outage impairs network infrastructure				🟨

Table 2. Examples of Threats Resulting in Communications Network Congestion and the Intrinsic Vulnerabilities Exercised by the Threats

A	B	C	D	E
EWI WCI Cyber40	Compatible Equipment (Hardware)		Priority Capability (Software)	
Country	User Devices	Network Elements	National	International
Argentina	Yes	Yes		
Australia [12]	Yes	Yes	Yes	
Austria	Yes	Yes		
Azerbaijan	Yes	Yes		
Bangladesh	Yes	Yes		
Belgium	Yes	Yes		
Brazil	Yes	Yes		
Bulgaria	Yes	Yes		
Cameroon	Yes	Yes		
Canada	Yes	Yes		*
China	Yes	Yes		
Colombia	Yes	Yes		
Cyprus	Yes	Yes		
Czech Republic	Yes	Yes		
Denmark	Yes	Yes		
Egypt	Yes	Yes		
Estonia	Yes	Yes		
Finland	Yes	Yes		
France	Yes	Yes		
Germany	Yes	Yes		
Greece	Yes	Yes		
Hungary	Yes	Yes		
Iceland	Yes	Yes		
India	Yes	Yes		
Indonesia	Yes	Yes		
Ireland	Yes	Yes		
Israel	Yes	Yes		
Italy	Yes	Yes		
Japan	Yes	Yes		
Jordan	Yes	Yes		
Kazakhstan	Yes	Yes		
Kenya	Yes	Yes		

Country key:

🟩 G20
🟨 EU
⬜ Non-G20

Capability:

🟪 Private Network Expected
🟪 Additional Public Network Capability

2.4 Existing Capabilities

In putting forth the recommendations in this report, it is important that a baseline of existing capabilities be described. Table 3 provides an outline of existing capabilities for the 63 countries that make up the Cyber40.[10] In Columns B and C, we see that the user and network equipment deployed in all of these countries is compatible with PIC. Since PIC is accomplished at an international level, it is important to emphasize that the existing technology would support a PIC capability. The actual status of a private emergency network is not known for all countries, in part for security reasons. However it is expected that some type of national security communications capability exists for each country (Column D). In addition to this private network capability, there are several countries with a country-level priority communication capability on their public networks. The glaring observation from a review of Table 3 and Fogure 1 is that priority communications at the international level is a missed opportunity. Here, existing private and public network schemes can be connected at international gateways where differences can be translated.[11]

[10] The inclusion of the EU expands the number beyond 40.

[11] See Key Observation No. 13, *International peering agreements are nonexistent, Key Observation No. 14, PIC accommodates different priority levels, Key Observation No. 29, PIC is Software, and Appendix A, Key Terms: 'Gateways.'*

A	B	C	D	E
Latvia	Yes	Yes		
Lithuania	Yes	Yes		
Luxembourg	Yes	Yes		
Malaysia	Yes	Yes		
Malta	Yes	Yes		
Mexico	Yes	Yes		
Netherlands	Yes	Yes	Yes	
Nigeria	Yes	Yes		
Norway	Yes	Yes		
Pakistan	Yes	Yes		
Philippines	Yes	Yes		
Poland	Yes	Yes		
Portugal	Yes	Yes		
Qatar	Yes	Yes		
Republic of Korea	Yes	Yes		
Romania	Yes	Yes		
Russia	Yes	Yes		
Saudi Arabia	Yes	Yes		
Singapore	Yes	Yes		
Slovakia	Yes	Yes		
Slovenia	Yes	Yes		
South Africa	Yes	Yes		
Spain	Yes	Yes		
Sweden	Yes	Yes		
Switzerland	Yes	Yes		
Thailand	Yes	Yes		
Turkey	Yes	Yes		
Ukraine	Yes	Yes		
United Arab Emirates	Yes	Yes		
United Kingdom	Yes	Yes	Yes	
United States	Yes	Yes	Yes	*

*Canada and the U.S. have a limited degree of priority scheme interoperability as a result of the preparations for the 2010 Vancouver Olympic Games.

Table 3. Existing Capabilities and International Level Gap

2.5 Scope

This section clarifies the scope of PIC as presented within this report. The scope is explored here by reviewing each of the key parameters associated with this important capability. These parameters include considerations related to the types of networks, technologies, services and related factors. In summary, the details below describe a capability that is of immediate value to every country, and for current as well as emerging services and applications. PIC will be international, compatible with both public and private networks, applicable across the broad range of technologies and applications in use today and tomorrow, including voice, data, and video.

The intent is that PIC should be inclusive of the various electronic protocols and networks used around the world. The end user should be able to use any common communication device to reach the desired party, who may be using a different technology. This is no different from placing a call from a cell phone to a landline.

Network Coverage

The scope of network coverage is international. While national-level networks are not the

[12] Of note, neighboring country New Zealand has a national level capability deployed. This is noteworthy given the close proximity of these two countries in this otherwise relatively isolated part of the world.

Priority Networks of Country A (originating)	Priority Networks of Country B (terminating)	Will PIC Increase Probability of Completion?
Only Public	Only Public	Yes
Only Public	Both Public & Private	Yes
Only Public	Only Private	Yes
Only Public	No Capability	Yes
Both Public & Private	Only Public	Yes
Both Public & Private	Both Public & Private	Yes
Both Public & Private	Only Private	Yes
Both Public & Private	No Capability	Yes
Only Private	Only Public	Yes
Only Private	Both Public & Private	Yes
Only Private	Only Private	Yes
Only Private	No Capability	Yes
No Capability	Only Public	Possibly*
No Capability	Both Public & Private	Possibly*
No Capability	Only Private	Possibly*
No Capability	No Capability	No

*An end user from Country B with authorized priority in that country, when originating a communication from a country (A) without any priority capability, could have the priority information passed without priority treatment until the communication enters the gateway for Country B.

Table 4. PIC Gateway Compatibility where Bilateral Agreements Exist

focus of this report, it is anticipated that national-level priority communications will benefit from the high volume application of priority communications services expected as a result of a focus on PIC.[13] [14]

Gateway Interface

The scope of gateway interfaces includes both public and private networks.[15] [16] That is, a country can extend its national-level priority capability from public, private, or both types of networks with the network of other countries when interfacing at an international gateway (Table 4).

The international gateway nodes are tasked with the recognition of a priority indicator in the incoming protocol stream, and the conversion to the international standard for the international leg of the transmission as well as providing preferential treatment. The far end gateway would likewise be tasked with any conversion to a national network for completion of the session. The gateways would of course also do any required protocol conversions to resolve differences between the protocols of the originating nation and the terminating nation.[17]

Network Access

Network access is not an issue, as PIC is about the prioritization in transport. The method of network access is not a factor. The scope of network access can include whatever type of network that country's government chooses, including:

- cable (coaxial cable)
- optical (fiber optic cable)
- wireless (air interface)
- wireline (copper wire)

Network Technologies

PIC can be deployed across all of the major technologies deployed in modern communications networks as well as those technologies emerging in future generation networks. The following abbreviated, alphabetically ordered list demonstrates the broad viability of the PIC capability. These technologies represent communication platforms, protocols and standards.[18]

- Asynchronous Transfer Mode (ATM)
- Broadband Wireless Access (BWA)
- Data Over Cable Service Interface Specification (DOCSIS)
- Code Division Multiple Access (CDMA)
- Fourth Generation Mobile Communications (4G)

[13] Key Observation No. 33, *The cost-sharing benefits lower entry barrier for developing and deploying PIC.*

[14] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*

[15] A public network is one on which service is offered to the general public. A private network is one that is limited to providing services to a restricted set of users (e.g. government).

[16] Note that excluded communications are two-way radio-based systems such as those used in public safety by emergency first responders (fire, police, ambulance).

[17] e.g., there are currently different country flavors or dialects of SS7 that are not "plug and play" compatible and need the services of a gateway to map the communication.

[18] Some of these technologies are inclusive of others.

- Global System for Mobile Communication (GSM)
- Intelligent Network (IN)
- Internet Protocol (IP) v4 and v6
- IP Multimedia Subsystem (IMS)
- Long Term Evolution (LTE)
- Next Generation Networks (NGN)
- Session Initiation Protocol (SIP)
- Signalling System 7 (C7, SS7)
- Synchronized Optical Networking (SONET)
- Synchronized Digital Hierarchy (SDH)
- Third Generation Mobile Communications (3G)
- Time-Division Multiplexing (TDM)
- Wireless Fidelity (WIFI) IEEE 802.11
- Wireless Local Area Network (WLAN)
- Worldwide Interoperability for Microwave Access (WIMAX) IEEE 802.16
- Universal Mobile Telecommunications Service (UMTS)

This service should be "future-proofed" as far as possible by the extension of protocol indicators and corresponding procedures, so the service concept does not need to be reinvented each time a new version of technology is deployed. To achieve this, legacy wireline, wireless, next generation IP, and future, as yet undefined, technologies should be designed to inherently support PIC.[19]

Subscriber Applications

PIC supports the complete spectrum of subscriber services. There are two important observations in this regard. First, PIC includes both old and new services. Second, the nature of these services varies considerably. For example, traditional voice service has a relatively predictable and small use of bandwidth and requires real-time transmission. In contrast, most data services have a highly unpredictable bandwidth requirement and usually do not have real-time transmission support. Still, some video or conferencing applications may require both high-bandwidth and real-time transmission support.

Historically PIC has been focused on voice, but with the understanding that data and video would follow. Applications such as conferencing depend on protocols for voice, data, and video and are envisioned to be included. Remembering that PIC enables the international portion of the transmission, what is taking place in terms of actual types of applications is not a factor. So while from the end user's standpoint a priority communication is being initiated from a device in one country to a user's device in another country, from the PIC transport perspective, the type of application is not relevant. Whether that communication is designated for priority or not is their only point of concern.

Users

The scope of users of PIC includes both members of the private and public sector. A government will typically assign PIC capabilities based on functions that are critical to national security and public safety during the response to a crisis.[20] [21] [22] [23]

2.6 Illustrative Scenario

At the 2nd Worldwide Cybersecurity Summit (London, 2011), the working group tackling PIC called for storyline-based materials that could be used in outreach to convey how PIC would be used, and how it would make a difference. To this end, the scenario on the following pages has been developed. It should be noted that while the aggregation of the elements of the storyline are fictitious, each of the key events is based on true historical events. The type of simultaneous events included here, or similar ones, are real possibilities and we must plan for the worst scenarios imaginable when considering PIC.[24]

The scope of users of PIC includes both members of the private and public sector. A government will typically assign PIC capabilities based on functions that are critical to national security and public safety.

[19] Key Observation No. 16, *Applications and services will continue to evolve.*

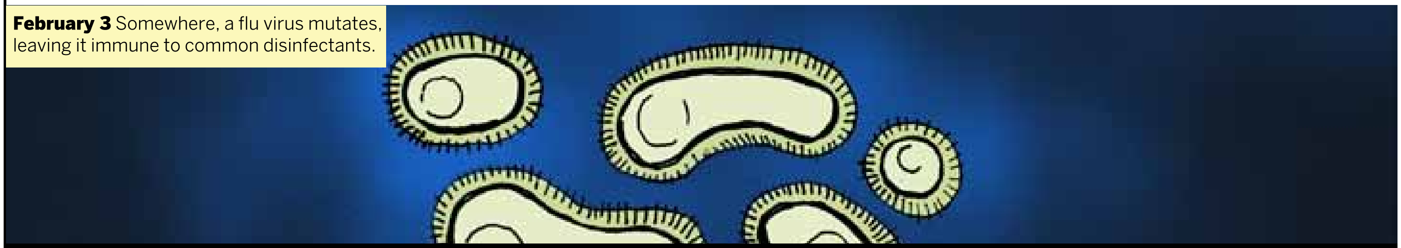
[20] The ability to dynamically assign authorized users is also a viable option. The authors note that school bus drivers became critical assets during the evacuation of New Orleans following the Hurricane Katrina flood.

[21] Key Observation No. 7, *The concept of critical functions is widely accepted around the world.*

[22] Key Observation No. 11, *PIC is necessary for the continuity of critical private sector operations.*

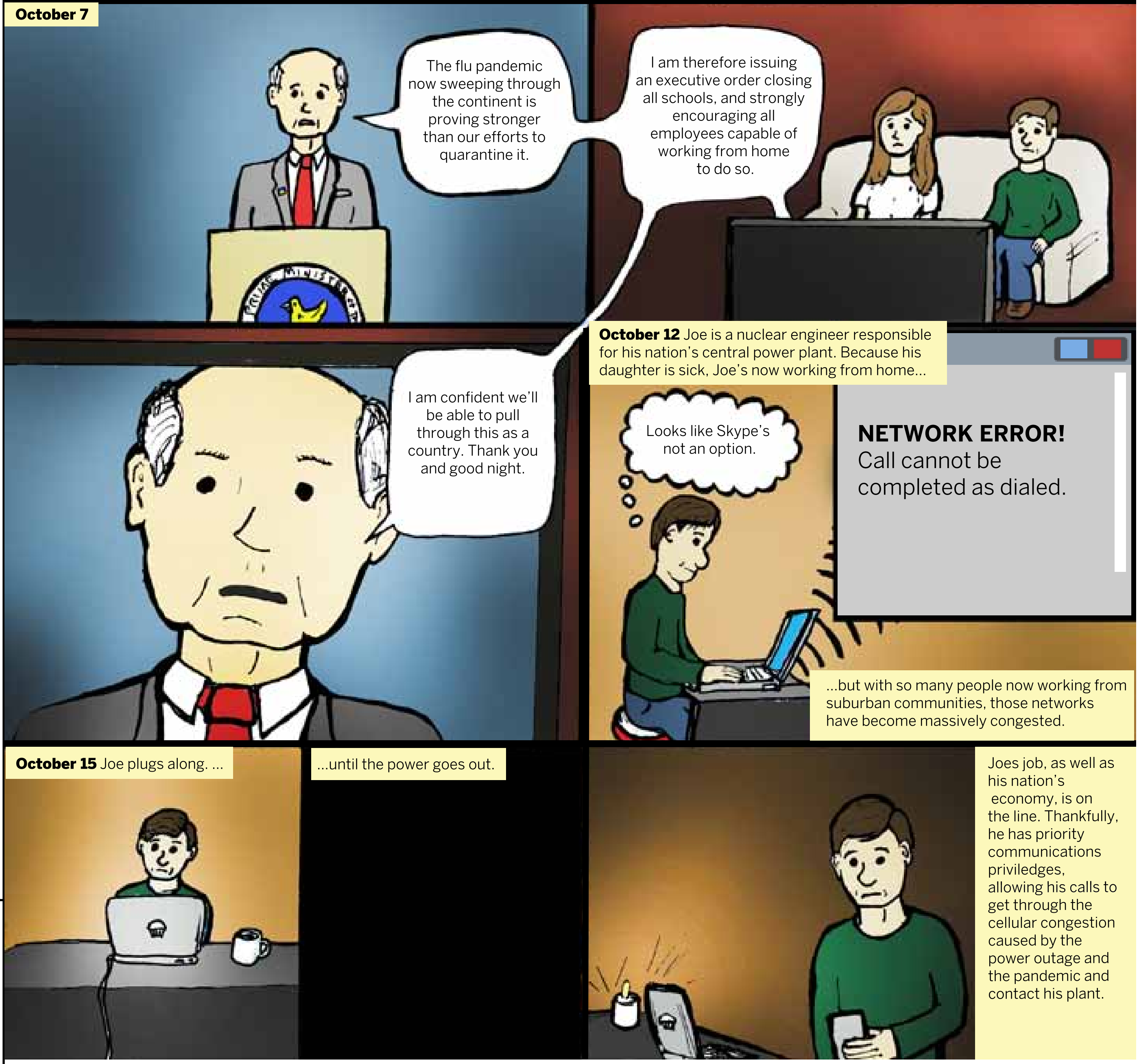
[23] Key Observation No. 28, *There are different methods possible for recognizing authorized users.*

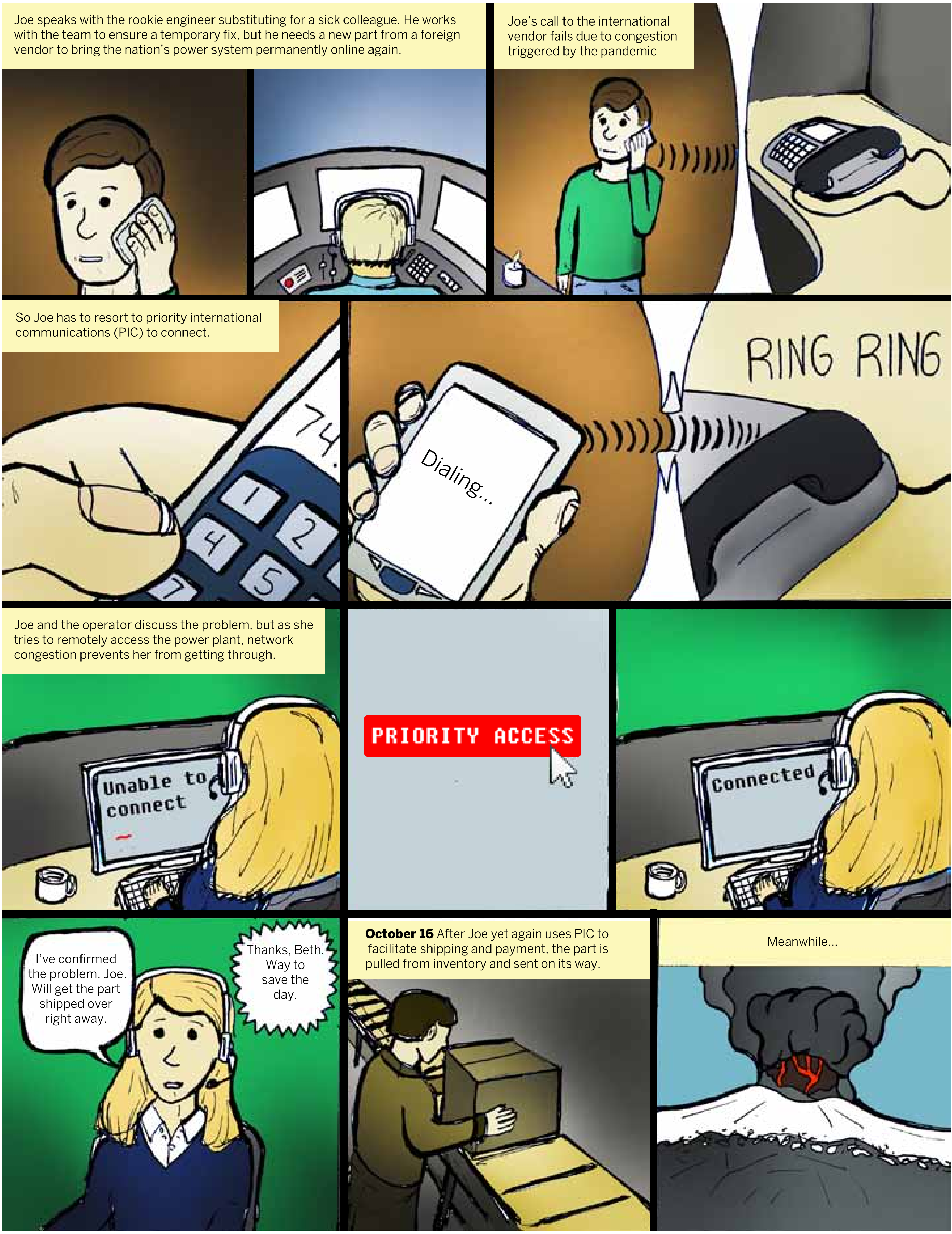
[24] Harry D. Raduege, Jr., Lieutenant General, United States Air Force (ret); Director, Defense Information Systems Agency (2000-2005); Commander, Joint Task Force - Global Network Operations (2004-2005).


February 3 Somewhere, a flu virus mutates, leaving it immune to common disinfectants.

PRIORITY INTERNATIONAL COMMUNICATIONS

By Stu Goldman & Thomas Lynch


October 7
The flu pandemic now sweeping through the continent is proving stronger than our efforts to quarantine it.
I am therefore issuing an executive order closing all schools, and strongly encouraging all employees capable of working from home to do so.
I am confident we'll be able to pull through this as a country. Thank you and good night.
October 12 Joe is a nuclear engineer responsible for his nation's central power plant. Because his daughter is sick, Joe's now working from home...
Looks like Skype's not an option.
NETWORK ERROR! Call cannot be completed as dialed.
...but with so many people now working from suburban communities, those networks have become massively congested.
October 15 Joe plugs along. ...
...until the power goes out.
Joes job, as well as his nation's economy, is on the line. Thankfully, he has priority communications priviledges, allowing his calls to get through the cellular congestion caused by the power outage and the pandemic and contact his plant.



Joe speaks with the rookie engineer substituting for a sick colleague. He works with the team to ensure a temporary fix, but he needs a new part from a foreign vendor to bring the nation's power system permanently online again.

Joe's call to the international vendor fails due to congestion triggered by the pandemic

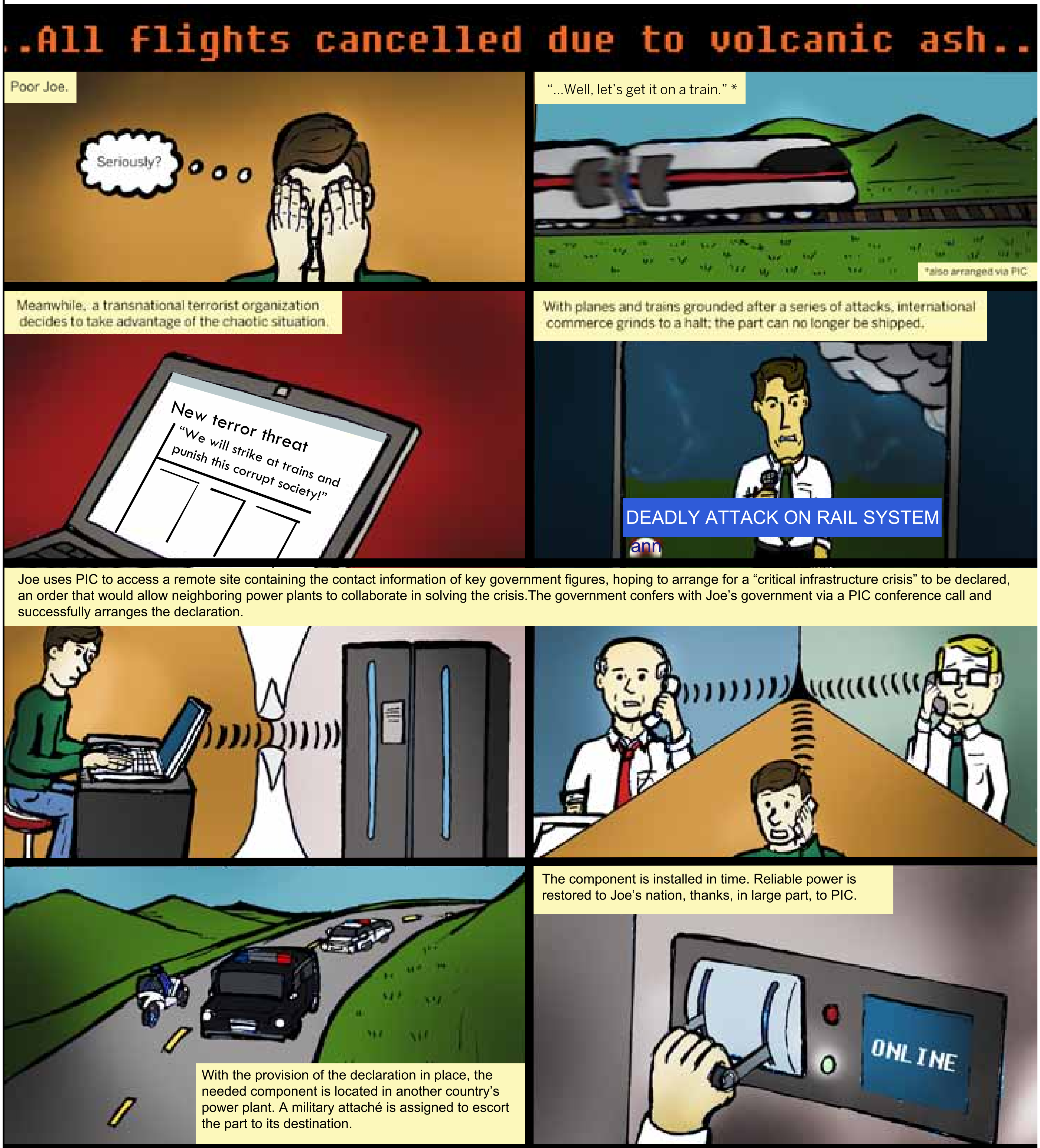
So Joe has to resort to priority international communications (PIC) to connect.

Joe and the operator discuss the problem, but as she tries to remotely access the power plant, network congestion prevents her from getting through.

Unable to connect
PRIORITY ACCESS
Connected
I've confirmed the problem, Joe. Will get the part shipped over right away.
Thanks, Beth. Way to save the day.

October 16 After Joe yet again uses PIC to facilitate shipping and payment, the part is pulled from inventory and sent on its way.

Meanwhile...


..All flights cancelled due to volcanic ash..
Poor Joe.
Seriously?
"...Well, let's get it on a train." *
*also arranged via PIC
Meanwhile, a transnational terrorist organization decides to take advantage of the chaotic situation.
New terror threat
"We will strike at trains and punish this corrupt society!"
With planes and trains grounded after a series of attacks, international commerce grinds to a halt; the part can no longer be shipped.
DEADLY ATTACK ON RAIL SYSTEM
ann
Joe uses PIC to access a remote site containing the contact information of key government figures, hoping to arrange for a "critical infrastructure crisis" to be declared, an order that would allow neighboring power plants to collaborate in solving the crisis.The government confers with Joe's government via a PIC conference call and successfully arranges the declaration.
With the provision of the declaration in place, the needed component is located in another country's power plant. A military attaché is assigned to escort the part to its destination.
The component is installed in time. Reliable power is restored to Joe's nation, thanks, in large part, to PIC.
ONLINE

This is just one of thousands of stories that unfolded during this crisis that was mitigated by the availability of priority communications and a willingness of people to work together to prevent chaos and loss of life and property. While this was going on, others were using PIC to coordinate medical supplies, food, water, critical commerce, and other needed activity to keep civilization afloat.

2.7 Ten Frequently Asked Questions (FAQs)

The following questions are based on interactive workshops and private consultations held in numerous countries around the world that included individuals from a wide range of backgrounds and interests. These questions are often asked when the concept of PIC is introduced.

Q1: Does a priority communications capability violate "net neutrality"?

No, it does not. In its most common usage, the term "net neutrality" is not compromised by PIC. In its most restrictive definition, net neutrality calls for all messages of the same class to be treated with the same protocols, without preferential treatment (enhancement or degradation) for selected originators. But even under these terms, PIC does not violate net neutrality because the industry has a long-held policy wherein different classes of communication are treated differently, including but not limited to separate queues and different treatment for processing messages.[25]

"Priority" treatment was actually in use at the very start of telecommunications, particularly when it came to government messages, as can be seen in The Pacific Telegraph Act of 1860:[26]

> "...That **the government shall at all times be entitled to priority in the use of the line or lines**, and shall have the privilege, when authorized by law, of connecting said line or lines by telegraph with any military posts of the United States, and to use the same for government purposes." (Section 1)
>
> "That messages received from any individual, company, or corporation, or from any telegraph lines connecting with this line at either of its termini, shall be impartially transmitted in the order of their reception, excepting that **the dispatches of the government shall have priority**." (Section 3)

Priority treatment continues to be critical in the United States today, with wireline and wireless national priority services established and utilized by approximately 300,000 and 100,000 users, respectively.[27] The principle that these calls can have a higher level of probability of completion without preemption of normal traffic attempts is the essence of the GETS and WPS capabilities. National policies will vary, and the PIC mechanism put forward here can accommodate the full range of policies and practices.

PIC can be accomplished using the existing Internet architecture. In addition, priority communications capabilities are part of the plans for the Internet's future development.

Q2: Does providing priority communications require re-architecture of the Internet?

No, it does not. PIC can be accomplished using the existing Internet architecture. In addition, priority communications capabilities are part of the plans for the Internet's future development. Protocol elements such as the optional Resource Priority Header (RPH) can be used as a marker, and the necessary enhanced procedures for treatment of the packets can easily be confined to software or firmware within the various nodes. In other words, the data networking protocols have long anticipated the benefits of preferential traffic handling.

It falls upon the gateway nodes to map across any protocol differences between the various networks, thus avoiding incompatibility issues.

Q3: There is so much spare capacity in the Internet that PIC is not needed, right?

There is not enough bandwidth capacity when extreme traffic demands are placed on communications networks. Communica-

[25] "Net Neutrality provides a flat transport network where one service provider's packets are not favored over another's packets in the core network. However, while service providers are treated equally, different applications (e.g., e-mail, voice, video) have different classes of service and thus different priorities. Packets associated with emergency communications also receive priority treatment." Key Findings No. 51, *Net Neutrality May Be Misunderstood*, ARECI Report, p. 74, European Commission, March 2007.

[26] *Pacific Telegraph Act - An Act to Facilitate Communication between the Atlantic and Pacific States by Electric Telegraph*, Chapter 137, U.S. Statutes, 36th Congress, 1st Session, 1860.

[27] Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) User Council Meeting Report, January 2012.

tions networks are not designed to be able to support all users simultaneously. If network operators designed, built and operated networks to completely handle all possible traffic, the cost could easily be on the order of ten or one hundred times greater than it is presently, which would certainly result in an increased cost of services for users.[28]

There is usually excess capacity in the backbone networks of most developed countries. Relative to the backbone, or core network, it is the network access (i.e. between end users and their ISPs) capacity that tends to be more limited. This is a function of network architecture design fundamentals. The load requirements and the build-out cost result in high-capacity transport "pipes" in the core, while the same factors produce lower bandwith around the edges.

History has shown that as time passes, communication needs increase dramatically. We have gone from simple e-mail ASCII messages to video applications, and perhaps soon to 3D video. One can reasonably expect that the spare bandwidth of today will eventually become fully occupied.

Some of the types of scenarios that serve as evidence of network congestion include:

- Network Impairment: a natural or man-made disaster destroying communications infrastructure and thus creating chokepoints.
- Payload Attack: a denial-of-service attack or other intentional acts may create points of congestion above the anticipated spare bandwidth allowance.
- Payload Utilization: the traffic during a disaster may very well peak far beyond normal as the population tries to gather information about the disaster and to communicate with family and friends in the area.

Each of these factors alone, and in combination, increases the probability of congestion and thus the need for PIC.

Q4: If we just block texting, videos and gaming, then there would be lots of capacity, right?

Such an approach is overreaching, causing many more problems than necessary. If such applications results in a significant portion of the international traffic, then turning it all off is overkill to provide the necessary bandwidth for the relatively few PIC messages. Throttling the traffic would be more reasonable, but would require a mechanism to determine how much bandwidth is needed for the PIC messages, which may be sporadic and have an unpredictable arrival rate. This would result in wasted bandwidth or blocked PIC attempts, and most likely both over a period of time.

Instead, the use of PIC procedures would allow the bandwidth to be fully used by normal traffic and still allow a higher probability of communication success for PIC, requiring only a bit more algorithm sophistication than a predictive throttling scheme.

Without an unrealistic deep packet inspection, a throttling and blocking node would not know which messages were just "social" and which messages from the population were important for protecting life, limb, and property during a crisis. With PIC, no additional normal attempts are discarded.[29]

Q5: How would everybody else's calls be handled?

The implementation is virtually undetectable for the population at large. When there is congestion in networks, normal users will experience mild-to-severe blocking when they initiate communications. The relatively small number of authorized users means that their impact is negligible on the rest of the population.

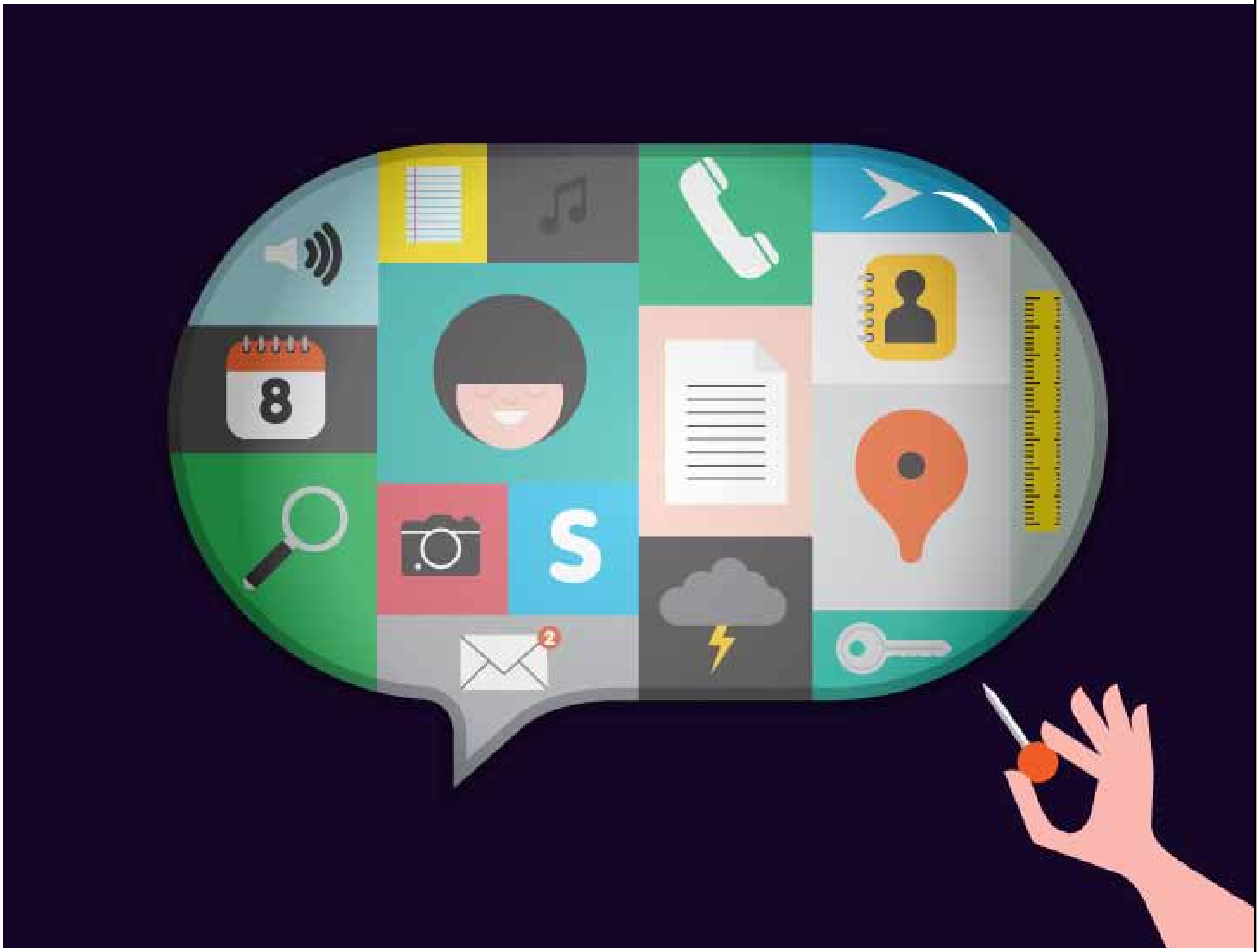
The relatively small number of authorized users means that their impact is negligible on the rest of the population.

Delving further in this discussion, the term "preemption" is introduced to describe the option that existing calls (or sessions, depending on the service) could be terminated in order give capacity to a new priority attempt.[30] This is a matter of local policy for national priority schemes. Some countries

[28] Key Observation No. 31, *There is diminishing value for over-engineering networks.*

[29] Normal attempts are discarded when no bandwidth is available, but are not further impacted by PIC attempts.

[30] Key Observation No. 26, *Non-reserved resources PIC is preferred to avoid wasting capacity.*



Robert Samuel Hanson

(e.g. U.K.) use preemption as the primary scheme during a crisis, while other countries (e.g. U.S.) do not preempt wireline or wireless calls for their national public network priority schemes.[31]

Q6: Why not have a separate, dedicated network for priority communications?

This is a possible solution. However, compared to the PIC approach, its feasibility is problematic. This is because the cost of such a separate international network dedicated solely to PIC traffic would be very high. It is unrealistic to expect that such a network would ever be deployed widely, other than in very narrow point-to-point situations.[32]

The separate dedicated international network approach also introduces a potential single point of failure into priority communications, in that it would depend on a separate, seldom-used network. Priority communications that have access to multiple, competing networks don't face this limitation.

Q7: What about disagreements about who should be given what priority level?

Nation-state governments are responsible for assigning priority levels to their populations. Since PIC communications begin in a national network, the authentication, authorization, and priority level are a matter of local policy.[33] Based on bilateral agreements with peering countries, the gateway node would be responsible for mapping the priority levels between the two national networks. It is expected that peering countries will consider

[31] In the U.K., MTPAS; in the U.S., GETS & WPS.

[32] e.g. point-to-point "red phone" examples.

[33] Some schemes use a single priority indicator while others may use multiple level indicator, such as a five or some other value.

Tsevis

each other's policies in assigning priorities and levels when making agreements to recognize each other's priority designations.[34]

Priority International Communications are likely to be essential for recovery from a disaster, but may typically consist of a relatively small number of messages when compared with the priority communications within the afflicted country or region. Thus, PIC procedures need to be able to support the communications without imposing restrictions upon the national procedures and protocols in use.

Q8: What about someone compromising a network by spoofing authorization and causing a Denial of Service (DoS) attack?

Any scheme that supports making some traffic more "important" has the potential for being misused. The implementation of a PIC policy and capability stresses the existing intrinsic vulnerability of electronic communications that can be emulated. The primary concern would be the misuse of priority credentials to make a DoS attack. There are, however, procedures that can effectively detect and isolate such attacks, reducing the risk while maintaining the advantage offered by priority schemes. There is a range of technical solutions for addressing this concern that involve both prevention of such abuse, as well as detection of an attempt and amelioration of the impact, should such an attempt have initial success.[35]

Q9: Why hasn't PIC already been implemented?

There are several reasons why this idea remains unimplemented:

[34] Key Observation No. 14, *PIC accommodates different priority levels.* (see also , Figure 11, *Example of Mapping of Priority Level*)

[35] The discussion of these methods is too technical for this publication. The authors can be reached for further discussion on this point.

First, few people realize that an elegant, low-cost, immediately deployable solution exists. Others simply don't know that we could have prevented the loss of lives and property due to clogged networks.

Few people realize that an elegant, low-cost, immediately deployable solution exists. Others simply don't know that we could have prevented the loss of lives and property due to clogged networks.

Second, it is hard to adequately plan for low-probability events—even if they are of high consequence.[36]

Third, except for those who are directly affected, such as families who have lost someone, most people largely forget about catastrophes and go on with their lives and focus on more routine events.

Fourth, politicians and increasingly business leaders, are simply much more visible when acting on issues that are visible. This means that when they are reacting to an event, they are more likely to be rewarded than for planning for an event that is not on the "radar screen" of the public, and thus preventing it from becoming worse. For this reason, it is critical for stakeholders to effectively articulate their needs for PIC to decision makers and to further be effective in moving them to action.

The communications media serving the public can play a very important role in promoting the implementation of PIC. The challenge for reporters is a classic one—how to effectively interest their respective audiences in something very important, proactive and that requires some effort to understand. This will require creativity, sincerity and careful articulation. This report is intended to support such efforts. If the public were aware of the current situation and the opportunity to save lives and property, then the result would likely be overwhelming support for the implementation of PIC capabilities.

Q10: Who is going to pay for PIC?

As the protection of human life and property in times of catastrophes is largely a government responsibility, the recommendations presented in this report submit that governments should provide the funding for the implementation and ongoing maintenance of PIC.[37] This is consistent with the practices of the countries currently implementing a national-level priority scheme.

The good news about funding is that the cost is relatively low because the actual expenses for implementation are limited. The proposed approach makes use of existing networks, existing switching and routing hardware, existing end-user devices, and existing protocols. For the most part, the implementation of PIC is simply the addition of some new software in networks.

The question of funding can be a difficult one and that it is why it is the last on the list. From a purely technical point of view, it doesn't matter how the work is funded as long as it happens. But from a practical point of view, the work will not happen until there are international agreements on the need for PIC and the funding model at the national level.[38]

[36] Rauscher, Karl Frederick, *Mutual Aid for Resilient Infrastructure in Europe, (MARIE)* Phase I Report, ENISA, 2011.

[37] Recommendation 2, *Due Diligence for Modern International Crisis Management*, Section 4.

[38] There are different views on whether PIC should be extended to include a business feature as well as a government-controlled disaster recovery feature. For example, it has been proposed to establish multiple levels of levels priority, such as ordinary traffic, a block of business priority levels, and then levels used by the government and critical infrastructure for restoration.   There could be agreements on what types of service would qualify. For example, one type of additional service might be time-sensitive financial services traffic, the processing of which is critical to global economic stability and – since it is data and not bandwidth intensive – makes up a relatively low proportion of all traffic. Others have proposed that PIC be reserved for restoration. Since the levels may be derived from national schemes, this topic may be confined to the bilateral interface agreements directing the gateway mapping procedures for PIC.

3. Key Observations

The reasons for having PIC are clear: Some functions in society are more important than others and therefore require robust communications to effectively operate in response to a major disaster.

This section presents 40 observations that are essential for understanding the current need for priority communications across international borders. The observations provide important insights that span the important areas of technology, business, ASPR (Agreements, Standards, Policies and Regulations) and the nature of human responses to catastrophes. Each key observation is articulated concisely, with supporting material referenced as appropriate. Moreover, the key observations are referenced throughout this report, and particularly in Section 4, Recommendations.

To enable the reader to brush up on the areas of most interest, this section arranges the observations according to the following categories:

- value proposition;
- policy;
- science, engineering and technology;
- business, finance and economics.

3.1 Value Proposition

The following eleven observations are primarily related to the benefits of PIC. Each has been selected from a larger number of observations because of its influence in forging one or more of the recommendations presented in Section 4.

1. Some information is more important than other information.

Based on shared human values for the protection of life, property and our environment, some information is clearly more important than other information.[39] This is evident during a crisis. The specific information characteristics are not rigidly fixed, but vary based of the nature of the unique crisis and may change during the life of the crisis. PIC enables the most important information to be carried across international borders with high probability during times of network congestion.

2. The value proposition for PIC is straightforward.

The reasons for having PIC are clear: Some functions in society are more important than others and therefore require robust communications to effectively operate in response to a major disaster.[40] PIC can promote the robustness and sharing of these functions by ensuring high probably of international communications success for government-authorized individuals in the face of congestion in cyberspace.

3. The value proposition for PIC is compelling.

The difference between critical communications getting through—or not—in a catastrophe is immeasurable because lives are in the balance.[41]

[39] See Section 2.10, *Frequently Asked Questions*, Q1: Do priority communications capabilities violate "net neutrality"?

[40] See "Robustness" in Key Terms.

[41] Key Observation No. 27, *Services and time orientation matters*.

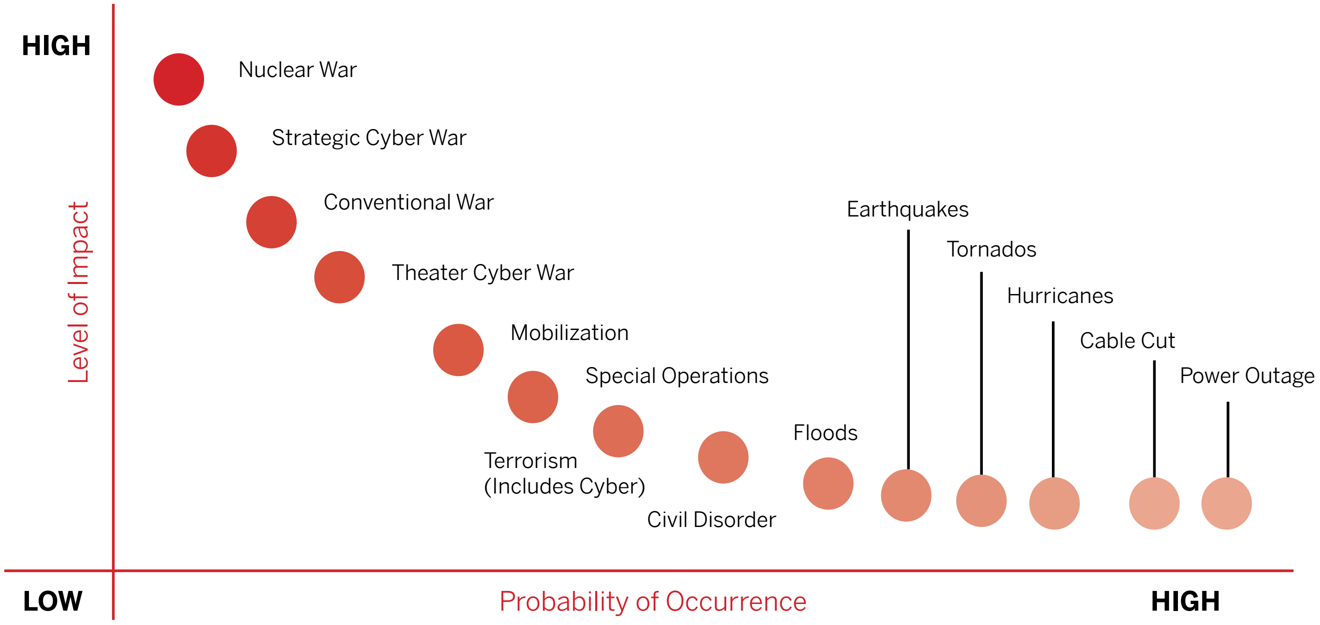


Figure 7. Spectrum of Events with Probability and Impact[43]

4. National-level priority schemes are field-tested and effective.

The value of national-level PIC capabilities has been proven. For instance, during September 11, 2001, the United States' capability kept key communication lines open. According to Brenton Greene, former director of the National Communications System of the Department of Homeland Security, "GETS allowed significant priority access for over 10,000 calls with over 95% completion rate at a time when networks were saturated and nobody else could get through." [42]

5. PIC is for rare-but-high-impact events.

The value to society of the PIC capability increases proportionally with the seriousness of events (Figure 7). This is a conservative assessment that is applicable worldwide. A more relaxed statement –i.e., not rare but regular – may apply to some regions such as in Europe where a high level of cross-border integration of critical infrastructures makes the frequency of utilization much more likely.

6. PIC is a highly leveraged enabler for emergency preparedness.

Communications capabilities are vital for the effective performance of all other critical response functions – energy, financial services, transportation, health care, and government.

7. The concept of critical functions is widely accepted around the world.

Most governments of developed countries have completed some assessment of critical sectors and critical functions to promote emergency preparedness.[44] This suggests that the first step to identifying roles is often already taken, i.e. it will be straightforward to identify who should be government-authorized users. It also suggests that these governments' perceived need to identify critical functions can be more effectively addressed with the provision of PIC to support these functions. PIC increases the probability of

[42] Greene, Brenton, former director, National Communications System, U.S. Department of Homeland Security, NCS Video, April 2008, gets.ncs.gov/docs.html . There are also examples of schemes with considerable lessons learned, i.e. the July 7, 2005 London bombing experience where a preemptive approach was utilized. (David Mowbry presentation to the NRSC, 2005)

[43] Source: U.S. National Communications System (NCS); reformatted.

[44] *An Inventory and Analysis of Protection Policies in Fourteen Countries,* International Critical Information Infrastructure Protection (CIIP) Handbook 2004, Swiss Federal Institute of Technology.

Because PIC can be implemented by utilizing existing networks, network elements, network interfaces, protocols and end-user devices, its implementation can be relatively quick, once agreements are established.

these functions working during a crisis. These critical functions include both public and private sector functions, such as continuity of government at multiple levels, public safety, communications infrastructure, energy infrastructure, certain types of transportation, and medical services.

8. Priority communications capabilities need to be extended internationally.

Assessment of the necessary performance and range of disaster-response communications capabilities suggests that international reach is essential.[45] This need may vary across countries. Some countries with immediate critical infrastructure dependencies on other countries, as is common within Europe, can have more frequent high-impact exposure from network congestion.

9. It only gets better.

For those countries that already have a dedicated emergency network, PIC enhances the value of that network by extending priority beyond that country's borders. Therefore, PIC should not be considered as a competitor to or a replacement for any existing emergency capabilities, but rather as a multiplier of those capabilities.

10. Implementation can be relatively quick.

Because PIC can be implemented by utilizing existing networks, network elements, network interfaces, protocols and end-user devices, its implementation can be relatively quick, once agreements are established.

11. PIC is necessary for the continuity of critical private sector operations.

PIC will increasingly be vital to the continued operation of critical private sector functions during a crisis. Companies that provide essential services to governments, other businesses and the general public require communication to maintain their operations, and these communications often include an international reach. Those companies whose function is deemed vital to public safety, economic stability or national security are candidates to be authorized for priority services by their respective governments.

3.2 Policy

The following six observations are primarily related to existing agreements, standards, policy and regulations (ASPR). Each is presented here because it helped shape the recommendations in Section 4.

12. Essential agreements, standards, policy and regulations (ASPR) that support PIC capabilities are stalled.

Although the concepts and even international protocols for priority communications across borders have existed for over a decade, the implementation of these standards is stalled. This development of PIC standards clearly indicates their value to governments; obstacles must therefore arise at the level of implementation. Why? The issue (essentially, being prepared for low-probability events) is not sufficiently visible, and the task of getting countries to cooperate is dauntingly complex.

13. International peering agreements are nonexistent.

Agreements are needed by equipment suppliers, network operators and governments to establish international interfaces for basic interconnection and interoperability agreements, and to accommodate differences in priority-level schemes.[46]

14. PIC accommodates different priority levels.

The implementation of a priority-scheme interface requires bilateral coordination for the treatment of different levels (Figure 8). Appendix A provides examples of the priority scheme utilized by the U.S. Government for its national-level, voice capabilities.

[45] 88% percent of participants indicated that a proper priority communications scheme should be international; Interactive Participant Polling, *Proceedings of the IEEE CQR Workshop on Priority Communications on Public Networks Workshop*, Bratislava, Slovakia, September 2008.

[46] The lone example is an international agreement for cross-border priority communications that was established between Canada and the U.S. with regard to the limited implementation of WPS.

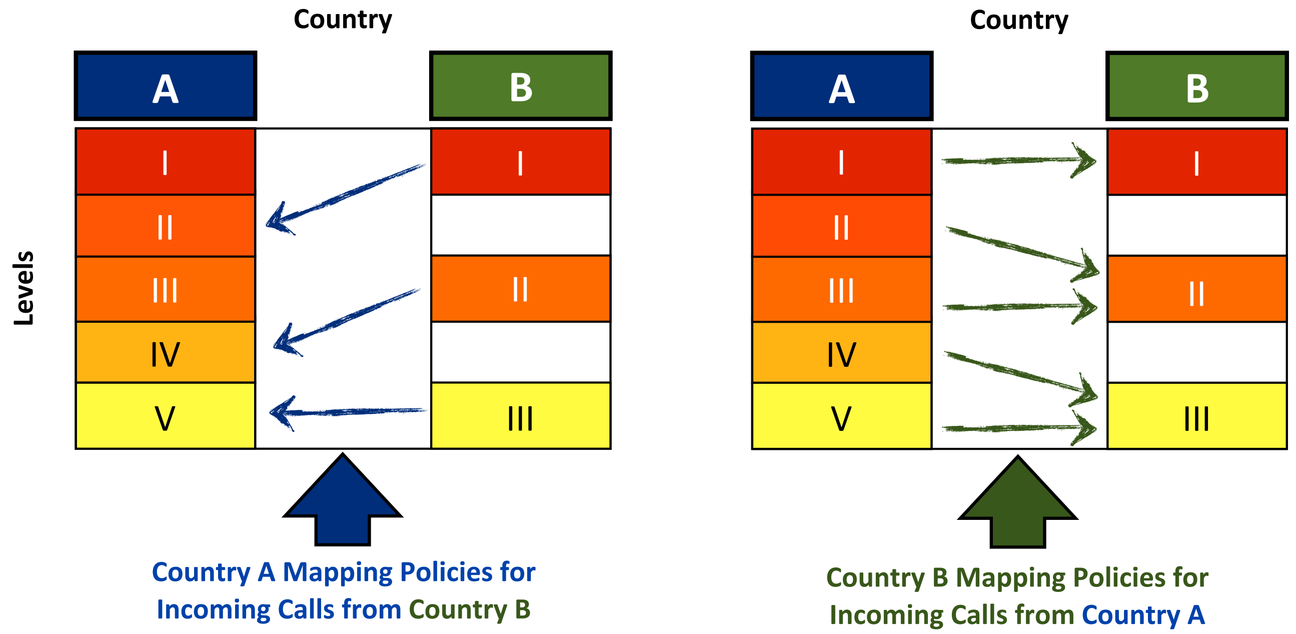

Country
A
B
Levels
I
II
III
IV
V
I
II
III
Country A Mapping Policies for Incoming Calls from Country B
Country
A
B
I
II
III
IV
V
I
II
III
Country B Mapping Policies for Incoming Calls from Country A

Figure 8. Example of Mapping of Priority Levels

15. We need complete ASPR for optimizing PIC.

The supporting policies for getting the most out of PIC will require cooperation on a range of subjects, including the mapping of priority levels between countries, the trust chain for authentication, security practices and handling abuse, and authorization and expectations for reserve capacity for national use.

16. Applications and services will continue to evolve.

New applications and services are expected to continue to be developed in the foreseeable future. Priority capabilities should be integrated into these emerging capabilities.

17. Following standards is wise.

Using an international PIC standard is wise as it greatly increases interoperability and full-feature functionality, enables faster deployment, and reduces the number of times the capability needs to be developed separately, thus reducing cost.[47] If equipment suppliers are required to produce one version of PIC, as opposed to many versions, the total cost will be lower. Therefore, it is important to continue evolving international standards.[48]

3.3 Science, Engineering and Technology

The following 13 observations are primarily related to the physical and logical limitations associated with providing PIC. Each observation has been selected due to the key role that it played in shaping the recommendations presented in Section 4.

18. Communication services are more than voice.

Any viable priority international communication scheme must address the current and likely future technologies for communications via voice, text, data, video and the like. A PIC scheme must also address the potential for conversion from one technology used by an originator to a technology compatible with the terminating party's equipment tech-

[47] 100% of participants agreed with the assessment that the most cost effective priority communications plan would make use of the public networks to some extent. *Proceedings of the IEEE CQR Workshop on Priority Communications on Public Networks Workshop*, Bratislava, Slovakia, September 2008, http://committees.comsoc.org/cqr/Slovakia.html

[48] 82% of participants agreed with the statement *"The ability to evolve priority communications capabilities to future networks is important"* (76% indicated they 'strongly agree"); Interactive Participant Polling, *Proceedings of the IEEE CQR Workshop on Priority Communications on Public Networks Workshop*, Bratislava, Slovakia, September 2008.

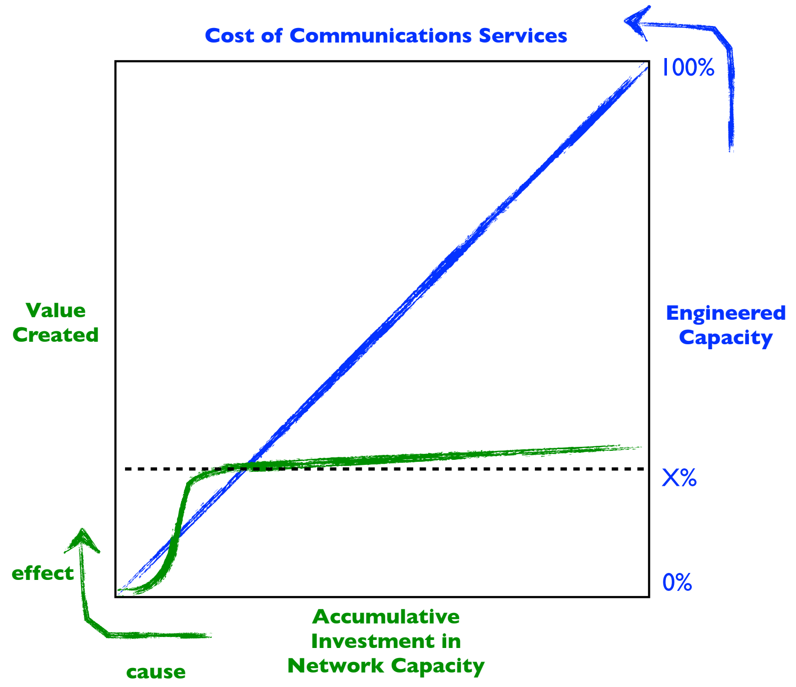

Cost of Communications Services
100%
Engineered Capacity
X%
0%
Value Created
effect
cause
Accumulative Investment in Network Capacity

Figure 9. Value – Engineered Capacity Relationship

nology, so that communications attempts do not fail but complete using the technologies present.[49]

19. Increasing demand for bandwidth.

Emerging services and applications utilize ever-higher amounts of bandwidth, and there is no end in sight for this bandwidth addiction. Thus it is not reasonable to expect the challenge of statistically varying and extreme payloads to lessen.

20. Network capacity limitations are a reasonable trade-off for cost management.

Communications networks are engineered and provisioned for normal everyday peaks, and even beyond-normal situations (Figure 9). Networks operators want to carry traffic: that is their business. However, building and maintaining networks to carry 100% of the potential traffic load is not feasible. If networks were designed and built to carry the extreme levels of the traffic theoretically possible given end-users' devices, the monthly price for services would increase by an order of magnitude or more. So, it is simply too expensive for network operators to increase capacity enough to account for major emergencies. Instead, we must prioritize communications.

21. Capacity limitations are an intrinsic vulnerability of networks.

Networks have engineered capacity limitations as a constraint of fiber optic spectrum saturation, digital signal processing throughput, and other fundamental barriers such as the cost of equipment.[50] When these capacity limits are reached, network congestion occurs and the excess load is blocked.

22. Statistical variation and extremes are intrinsic vulnerabilities of payload.

Communications system traffic has unpredictable variation due to the human-origination of applications and services. Current trends of the new technologies being introduced make it difficult to predict bandwidth demand. The variation in traffic loads includes extreme loads that exceed network capacity.[51]

23. Payload is "the new software."

Just as hardware, software, and human error have been the primary contributors to service outages in the past, ASPR and payload are increasingly being identified as the contributors to loss of service or outages in next-generation networks that provide advanced services.

A historic progression can be seen regarding the major contributors to system failure of modern communications systems since their introduction several decades ago. In their earliest years, through the early 1980s, hardware was the major cause of failures. With the introduction of digital signal processing (DSP), programmed logic and related artificial intelligence (AI) controls, the major contributor soon became software. The next transition occurred in the mid-'90s, as the pace of technology and application advances and the resulting complexity led to human-machine interface challenges, thus making procedural and other human performance factors the

[49] Section 2.5, *Scope*, provides more information on the types of networks, technologies and services included.

[50] See Section 2.2, *Understanding Network Congestion.*

[51] Ibid.

biggest cause of failure.[52] Today, pervasive global connectivity and nondeterministic statistical utilization of bandwidth have ushered in policy and payload as the major contributors to failures in reliability and security in cyberspace.[53] [54]

24. Ingress or egress filtering is inadequate.

Ingress (inbound) or egress (outbound) filtering has been a longstanding method of managing traffic overloads. This approach to traffic management can rebalance the utilization of bandwidth to bias availability in favor of a particular direction (i.e., in or out of a country). However, given the technologies readily available, this approach is too indiscriminate in its traffic management, and will result in highly important calls or other communications being dropped in a crisis.[55] Filtering reduces the load but does so indiscriminately, and therefore does not help priority communications get through. For example, directional filtering would still enable non-critical users to play interactive games, send high definition video and images, and otherwise use up limited bandwidth.

Ingress or egress filtering can be structured in such a way as to exempt priority traffic.

25. Robustness is the word.

Priority communications are about having robust communications.[56] That is, infrastructure must perform its most important functions with a minimum of variation, in the presence of stresses that are beyond its expected operating conditions. The most important functions are the completion of the most important communications and the stresses are the traffic demand beyond engineered capacity.[57]

26. Non-reserved resources PIC is preferred to avoid wasting capacity.

Priority schemes can be introduced with a variety of approaches with respect to non-priority traffic:

- A fixed amount of bandwidth can be reserved in a network just for priority communications. While this approach does provide a block of bandwidth for priority communications, it means that this space is wasted when there are no priority communications needed, and may not be sufficient when there are more priority communications needed than allocated.
- A network management event can block all traffic except priority. While this approach does provide large amounts of bandwidth, it means that there is a delay until the person in charge declares an emergency and invokes the event. When invoked, the non-priority users are frustrated as they cannot communicate even when there is idle bandwidth available.
- A priority communication attempt where insufficient bandwidth is available could preempt an existing non-priority communication. While this approach does provide for immediate completion of priority communication attempts, there is a risk that the communication that was preempted may have also been vital, although not marked.
- A priority communication attempt could "exceed" allocated bandwidth until a communication session is released. This scheme does not work with circuit switched communications, but can be used in a packet network. A second threshold is established which is not exceeded so that the degradation caused by

> It is simply too expensive for network operators to increase capacity enough to account for major emergencies. Instead, we must prioritize communications.

[52] *Procedural Outage Reduction: Addressing the Human Part*, ATIS Network Reliability Steering Committee (NRSC), Washington, D.C., May 1999.

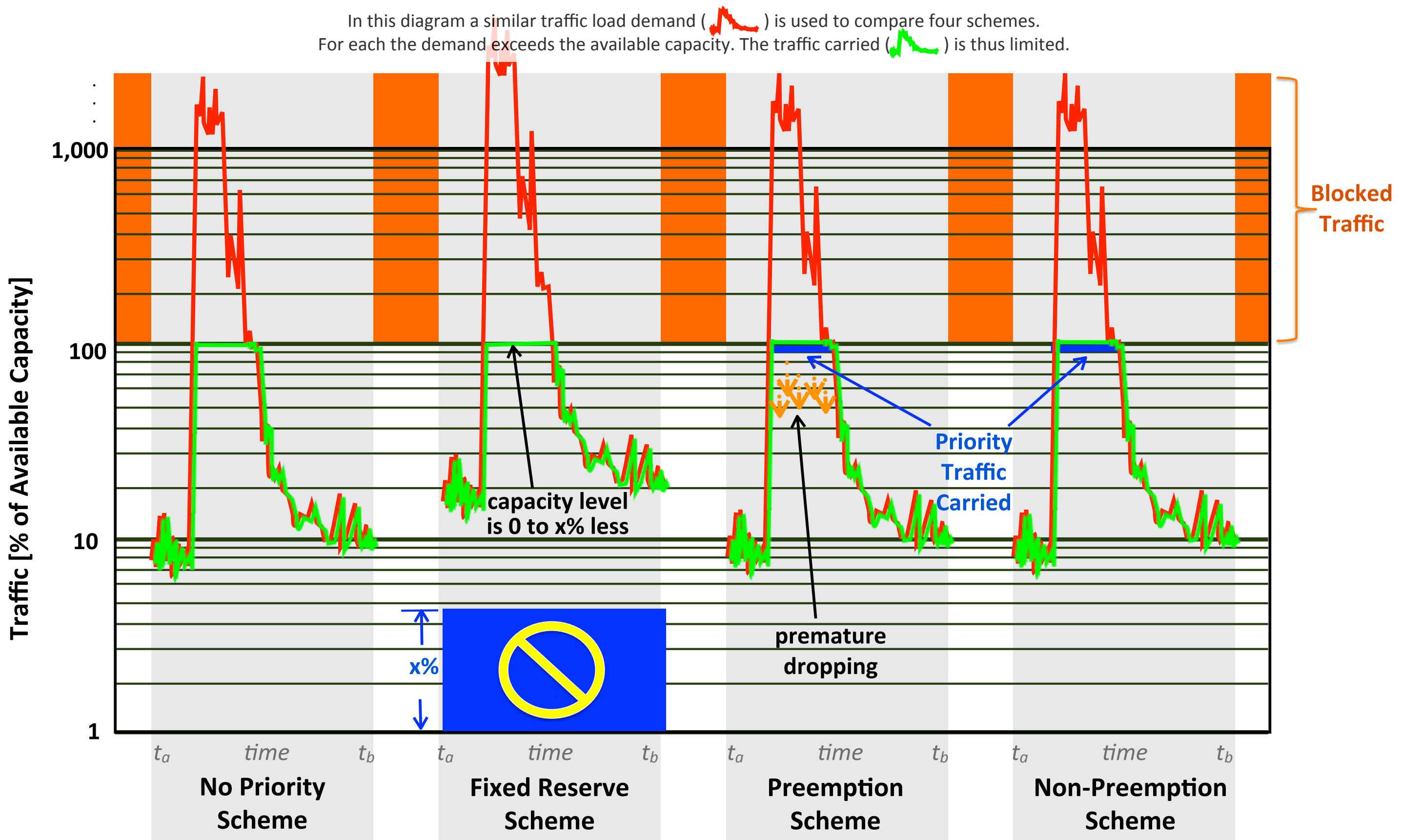
[53] Key Observation No. 22, *Statistical variation and extremes are intrinsic vulnerabilities of Payload.*

[54] Key Observation No. 19, *Increasing demand for bandwidth.*

[55] E.g. for some period after the 2011 Japanese earthquake-tsunami-nuclear meltdown crisis, ingress filtering was applied to provide additional capacity for outbound, Japanese-originated traffic.

[56] Robustness is distinguishable from related terms: the term **resilience** principally means that the infrastructure *will return to performing its function after being overcome*; **reliability** is a statistical term measuring the performance of intended functions, in the context of the environment and during the lifetime it was designed for; and **survivability** meaning principally that the infrastructure will be *preserved in some minimum useful state* after being overcome.

[57] In light of Key Observation No. 18, *Communication services are more than voice,* It includes other communications services beyond voice calls.


In this diagram a similar traffic load demand ( ) is used to compare four schemes. For each the demand exceeds the available capacity. The traffic carried ( ) is thus limited.

With no priority, all traffic greater than 100% capacity is dropped. **The most important (i.e. life saving,) communications are blocked** *indiscriminately.*

A fixed reserve capacity (x%) reduces the available capacity all the time so that when priority attempts are not being made this capacity is unavailable. **In its worst case, x% capacity will be wasted.** If some of the reserved infrastructure is damaged or otherwise unavailable, x % capacity may not be carried.

Priority communications **force premature termination of communications in progress** when there is not enough bandwidth. Capacity is optimized. However those with dropped connections are likely to re-attempt to connect, placing additional loads on resources. Communications not carrying the preference indicator can be interrupted even though it may have been life critical communications from the public.

Priority communications do NOT force premature termination of in-progress communications. Rather, priority communications wait until a resource is released by a previous call, are given greater effort to find a path, and may be exempt from network management control rules. **Capacity is optimized** and those with non-priority calls in progress can complete their sessions, avoiding unwanted load of re-attempts to connect.

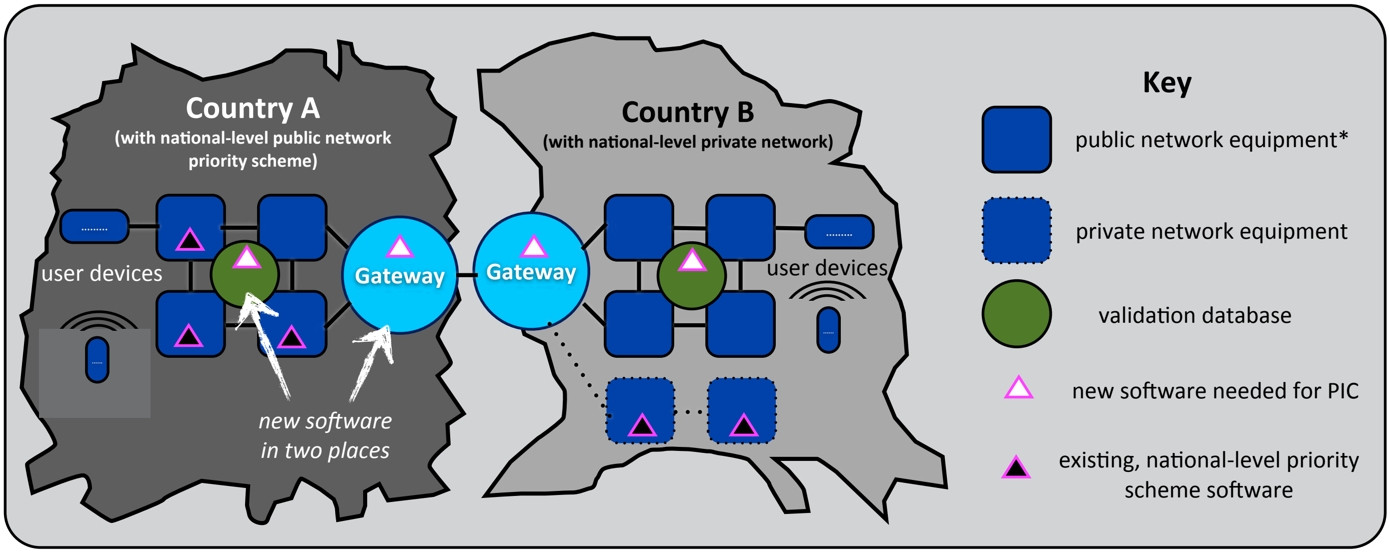
Figure 10. Preemption Effects on Capacity Utilization

random packet loss is an acceptable GoS in an emergency situation.

- A priority communication attempt could queue until bandwidth is available. This approach works well when the priority traffic is a low percentage of the overall traffic and the routes are fairly large, so that the delay time is short.
- A priority communication attempt could grab what bandwidth is currently available and grow to the requested bandwidth as other sessions end. This approach allows a desired communication session such as voice and video to at least start with a degraded performance and rapidly improve as resources are added.
- A network management event that could limit non-priority communications to n seconds. This approach prevents all of the bandwidth being held by indefinite sessions and can be used alone or in conjugation with the other schemes.
- Other approaches or combinations may be used.

27. Services and time orientation matter.

Services have a range of sensitivity to time. For example, some services like traditional voice telephony are highly sensitive to time and are described as being “real time” services. Other services, like e-mail, are near rea time sensitive. Still other services are non-real time sensitive such as large file downloads. During a crisis, for communications that support critical functions, each category can become vital and therefore will benefit from its


Country A
(with national-level public network priority scheme)
user devices
Gateway
new software in two places
Country B
(with national-level private network)
Gateway
user devices
Key
public network equipment*
private network equipment
validation database
new software needed for PIC
existing, national-level priority scheme software

*not all equipment suppliers may implement the capability

Figure 11. Comparison of Bandwidth Utilization During Network Congestion

individual priority relative to other traffic in the same category.

28. There are different methods for recognizing authorized users.

Government-authorized users can be identified in the network by various means. For example by the unique identifier of the device they are using, by a Subscriber Identity Module (SIM) card that can be inter-exchanged with different devices, or by a special account code that is entered when making a communications attempt. These are matters of local policy, as the communication will have to be authorized and marked as priority prior to reaching the international gateway.

29. PIC is software.

The implementation of a PIC capability is primarily software that is included in international gateways. This means that existing networks, network hardware and end user devices can be used as they are. This approach has very favorable cost implications.

Thus, tremendous value is created without additional investment in network capacity (Figure 11).

30. PIC can be accomplished for dedicated private networks.

Those countries with existing or planned dedicated networks can extend their reach by interfacing them at gateways with international network operators and establishing PIC agreements.

3.4 Business, Finance and Economics

The following 10 observations are primarily related to the models for managing the costs for PIC. Each observation has been selected because of its influence in shaping one or more of the recommendations presented in Section 4.

31. There is diminishing value for over-engineered networks.

The relative value, based on a benefit to cost ratio, decreases as networks are engineered to levels greatly exceeding expected traffic loads (Figure 9).

32. Priority communications capabilities have very low costs compared to other solutions.

When leveraging public networks, the return on investment for creating PIC capabilities is extremely high, given that the cost is primarily directed toward installing software on existing networks (Figure 12). For comparison's sake, to achieve equivalent high assurance for communications offered ubiquitously across a country via a dedicated network, one would have to pay for hardware and software that make up the network elements, the transport to connect the elements, staff to deploy, operate and maintain, and supporting infra-

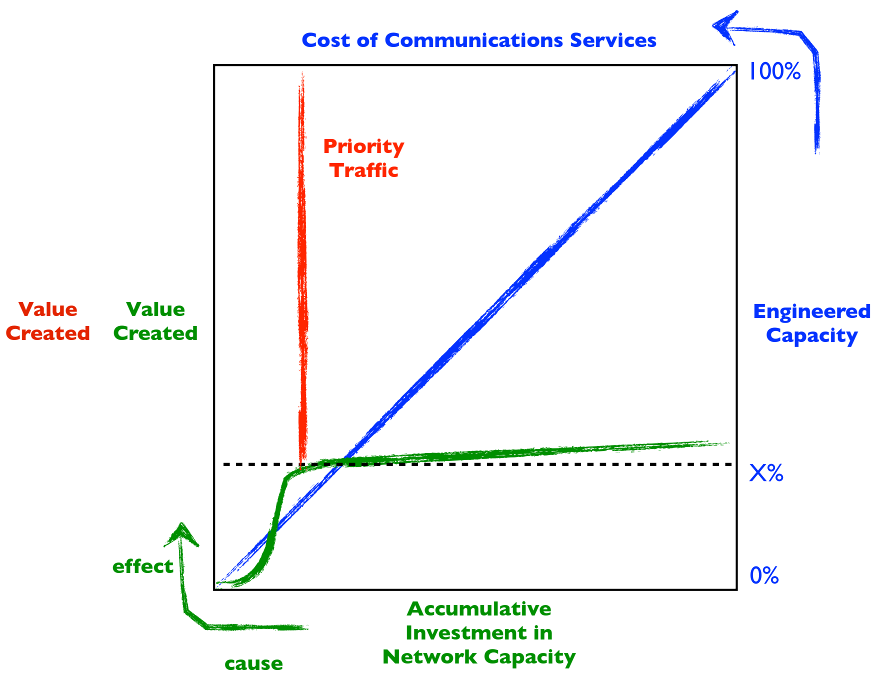


Figure 12. Value – Engineered Capacity Relationship with PIC

structure like buildings and vehicles. In addition, the end-users would need to be provided with separate dedicated devices, all of which would need to be continuously upgraded.

Each country needs to determine the best architecture and approach to meet its needs for a national level priority capability, any of which can be extended to have international reach with PIC.

33. The cost-sharing benefits lower the entry barrier for developing and deploying PIC.

As more countries get involved in deploying national-level and international-level priority communications, the market increases. Since the technology is primarily software deployment, the total software development cost can be shared by many countries and therefore the price per country can be significantly reduced. The envisioned activity of major equipment suppliers and network operators in this arena is expected to reduce the thresholds for entry for many countries.

34. There is a range of funding architecture options.

Governments have a range of funding architectures available to them. One example is an arrangement where all funding is directed to one or more of the major network operators in that country. Another arrangement is for governments to engage both the network operators and equipment suppliers simultaneously. Other aspects include whether the industry's participation is voluntary or mandated. This obviously affects the industry's cost recovery.

35. International gateways integrate public and private networks.

At the international gateway interfaces, it does not matter whether a country has a private or public priority network. Thus, there is a multiplicity of possible interfaces between any two countries (see Table 4, PIC Gateway Compatibility). This enables a country to leverage its existing national-level priority communications capability.

36. There are three basic components for priority communications.

The complete lifecycle costs of PIC can be understood as residing in three basic components. First, there is the technology itself, which is primarily software.[58] Second, the administration and maintenance functions needed to support the operational aspects of a ready-to-use capability. Finally, there are costs associated with the oversight of the program. Table 5 provides additional details for these costs.

Further, each of these functions has both an initial deployment phase and an ongoing cost that needs to be considered.

37. As major network suppliers are few in number, a few players can change the game.

Only a few major network equipment suppliers serve the global market. If even a subset of these suppliers implements the international standards in their equipment, they can make a tremendous step forward towards making PIC capability available worldwide. The economic benefit of leveraging the relatively few equipment suppliers applies to both the gateway network elements and for national level network equipment.

[58] Key observation No. 29, *PIC is software.*

Cost Component	Primary Party	Functions
Technology	Equipment Supplier	Design, development and testing of software that will be enhanced in international gateways[59]
Operations	Network Operator	Includes the provisioning of the software, the operations, administration, maintenance, provisioning (OAM&P)
Oversight	Government[60]	Managing the authorized users, conducting tests, auditing and quality control (failure analysis)

Table 5. Cost Components of PIC

38. Momentum Needed.

Even though the implementation cost of PIC is relatively low and the value high, there is still a need for fresh momentum to be created so a critical mass of interest can be generated within governments and among the public.

39. National-level emergency preparedness interests will also benefit.

One of the expected positive developments from the attention being generated on PIC is that there will be many countries that will now deploy national-level priority schemes. A further derivative of this will be that many additional countries will now begin to better manage the identification of critical functions and correspondingly authorize the same for priority communications.

40. PIC deployment has special market considerations.

The typical business model that drives the communications sector is one where service providers present to their customers a range of features and services. In more competitive markets, there is more attention devoted to developing new features and services to differentiate from industry peers. The service providers are typically not the developers of the underlying technology themselves, but rather depend upon software and equipment suppliers, who are continuously making solutions that can do more – and do it faster, cheaper, and smaller. Thus in the predominant model, it is the equipment supplier who typically leads the service provider, and the service provider in turn leads the end user. End user-led requests for services are not the typical model, however it is what is needed here, as per Recommendations 1 and 2.

Another consideration for understanding the current situation is that, unlike other communications markets, PIC users by definition will be a small percentage of the population and additionally, will only use the service in rare situations. Therefore, it isn't possible to enjoy the competitive advantages of having low margins driven by high-volume-based profit.

[59] A country has an option of enhancing software in the national-level validation database.

[60] A portion of this function may be outsourced to a contractor.

4. Recommendations

These recommendations are for governments and other stakeholders, as well as for network operators and network equipment suppliers of the communications industry.

This report presents four immediately actionable recommendations that, if implemented, will make PIC available across borders during major crises. These recommendations are for governments and other stakeholders, as well as for network operators and network equipment suppliers of the communications industry. In addition, they require the cooperation of international standards development organizations (SDOs). For each recommendation, there is either a leadership or supporting role to be played by those involved (Table 6).

In developing and articulating these recommendations, a number of factors were considered. These considerations included the following:

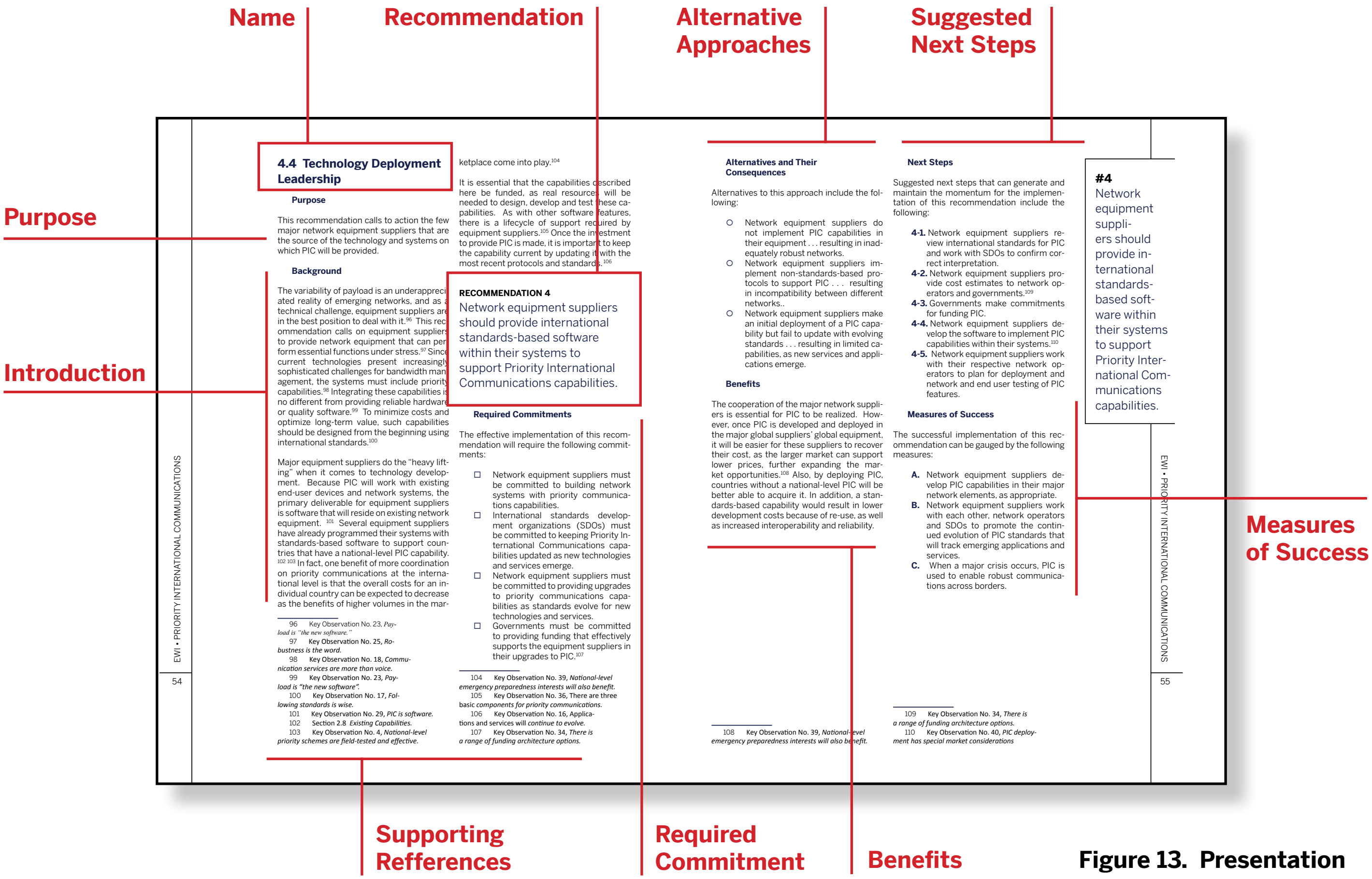
- The Needs
  - » A worldwide increased dependence on ICT for emergency response
  - » The national security interests of governments in implementing PIC
- The Benefits
  - » The international security benefits of PIC
  - » Global economic stability
  - » International mutual aid
  - » Economic benefits of software-based solutions that use existing public network infrastructure or dedicated infrastructure
  - » The business model of previous (i.e. national level) priority communications capabilities
  - » Lowering the hurdles governments face in implementing priority schemes
  - » The methods of priority communications deployment that have proved highly effective
- The Landscape
  - » The frequency of major crises for which PIC could save lives and property
  - » The availability of international standards
  - » The growth of next generation services (e.g. data, video) and next generation technologies
  - » The relative cost of alternative approaches

Each recommendation is presented along with essential decision-supporting information to foster implementation (Figure 13). This includes essential background information, the required commitments, the benefits of implementation, the alternatives and their consequences, next steps and measures of success. For additional discussion of the compelling factors supporting the recommendations, the reader is encouraged to read the other sections of the report, including the frequently asked questions in Section 2.

Recommendation	Government	Other Stakeholders	Network Operators	Equipment Suppliers	Standards Development Organizations
1. Championing Robust International Communications	■	■	▨	▨	▨
2. Due Diligence for Modern International Crisis Management	■	▨	▨	▨	▨
3. Network Provisioning of Priority International Communications	▨	▨	■	▨	▨
4. Technology Deployment Leadership	▨	▨	▨	■	▨

Role key: ■ Leadership ▨ Supporter

Table 6. Leadership for Recommendation Implementation



4.4 Technology Deployment Leadership

Purpose

This recommendation calls to action the few major network equipment suppliers that are the source of the technology and systems on which PIC will be provided.

Background

The variability of payload is an underappreciated reality of emerging networks, and as a technical challenge, equipment suppliers are in the best position to deal with it.[96] This recommendation calls on equipment suppliers to provide network equipment that can perform essential functions under stress.[97] Since current technologies present increasingly sophisticated challenges for bandwidth management, the systems must include priority capabilities.[98] Integrating these capabilities is no different from providing reliable hardware or quality software.[99] To minimize costs and optimize long-term value, such capabilities should be designed from the beginning using international standards.[100]

Major equipment suppliers do the "heavy lifting" when it comes to technology development. Because PIC will work with existing end-user devices and network systems, the primary deliverable for equipment suppliers is software that will reside on existing network equipment. [101] Several equipment suppliers have already programmed their systems with standards-based software to support countries that have a national-level PIC capability. [102] [103] In fact, one benefit of more coordination on priority communications at the international level is that the overall costs for an individual country can be expected to decrease as the benefits of higher volumes in the marketplace come into play.[104]

It is essential that the capabilities described here be funded, as real resources will be needed to design, develop and test these capabilities. As with other software features, there is a lifecycle of support required by equipment suppliers.[105] Once the investment to provide PIC is made, it is important to keep the capability current by updating it with the most recent protocols and standards.[106]

RECOMMENDATION 4
Network equipment suppliers should provide international standards-based software within their systems to support Priority International Communications capabilities.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

□ Network equipment suppliers must be committed to building network systems with priority communications capabilities.

□ International standards development organizations (SDOs) must be committed to keeping Priority International Communications capabilities updated as new technologies and services emerge.

□ Network equipment suppliers must be committed to providing upgrades to priority communications capabilities as standards evolve for new technologies and services.

□ Governments must be committed to providing funding that effectively supports the equipment suppliers in their upgrades to PIC.[107]

[96] Key Observation No. 23, *Payload is "the new software."*
[97] Key Observation No. 25, *Robustness is the word.*
[98] Key Observation No. 18, *Communication services are more than voice.*
[99] Key Observation No. 23, *Payload is "the new software".*
[100] Key Observation No. 17, *Following standards is wise.*
[101] Key Observation No. 29, *PIC is software.*
[102] Section 2.8 *Existing Capabilities.*
[103] Key Observation No. 4, *National-level priority schemes are field-tested and effective.*
[104] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*
[105] Key Observation No. 36, There are three basic *components for priority communications.*
[106] Key Observation No. 16, Applications and services will *continue to evolve.*
[107] Key Observation No. 34, *There is a range of funding architecture options.*

Alternatives and Their Consequences

Alternatives to this approach include the following:

○ Network equipment suppliers do not implement PIC capabilities in their equipment . . . resulting in inadequately robust networks.

○ Network equipment suppliers implement non-standards-based protocols to support PIC . . . resulting in incompatibility between different networks..

○ Network equipment suppliers make an initial deployment of a PIC capability but fail to update with evolving standards . . . resulting in limited capabilities, as new services and applications emerge.

Benefits

The cooperation of the major network suppliers is essential for PIC to be realized. However, once PIC is developed and deployed in the major global suppliers' global equipment, it will be easier for these suppliers to recover their cost, as the larger market can support lower prices, further expanding the market opportunities.[108] Also, by deploying PIC, countries without a national-level PIC will be better able to acquire it. In addition, a standards-based capability would result in lower development costs because of re-use, as well as increased interoperability and reliability.

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

4-1. Network equipment suppliers review international standards for PIC and work with SDOs to confirm correct interpretation.

4-2. Network equipment suppliers provide cost estimates to network operators and governments.[109]

4-3. Governments make commitments for funding PIC.

4-4. Network equipment suppliers develop the software to implement PIC capabilities within their systems.[110]

4-5. Network equipment suppliers work with their respective network operators to plan for deployment and network and end user testing of PIC features.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Network equipment suppliers develop PIC capabilities in their major network elements, as appropriate.

B. Network equipment suppliers work with each other, network operators and SDOs to promote the continued evolution of PIC standards that will track emerging applications and services.

C. When a major crisis occurs, PIC is used to enable robust communications across borders.

#4
Network equipment suppliers should provide international standards-based software within their systems to support Priority International Communications capabilities.

[108] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*
[109] Key Observation No. 34, *There is a range of funding architecture options.*
[110] Key Observation No. 40, *PIC deployment has special market considerations*

Figure 13. Presentation of Recommendations

4.1 Championing Robust International Communications

Purpose

This recommendation effectively calls on government agencies and other stakeholders to articulate their need for robust international communications.

Background

Critical government and private sector functions that support public safety, economic stability and national and international security cannot afford to be impaired—especially during a time of crisis.[61] In today's world, multinational enterprises and governments require international communications for their most critical functions. Still, even the most developed and technologically savvy countries accept blocked communications during a crisis.

Due to economic realities, it is understandable that networks cannot reasonably be designed to handle 100% of all traffic generated during periods of extreme loads.[62] However, having all calls blocked with equal probability reflects neither society's values nor what is possible technologically.[63] Some communications are simply more important than others.[64] Governments and other stakeholders closest to this reality need to articulate the need and make clear the consequences of continuing on the present path into the future, where congestion reigns in cyberspace during catastrophes.[65] [66]

Priority International Communications introduces much-needed robustness into our global cyberspace fabric.[67] This means that we are making sure that the most important communications functions are maintained for those situations where the stresses experienced are beyond design parameters.[68]

The call for PIC is not an overreaction to any one particular historic event, as indeed there have been many to learn from. Neither is the call for PIC an alarming cry for something that will never be used. Is there anyone who would expect the world to stroll through the coming years without further natural and manmade disasters? Rather, the call for PIC is a calm, deliberate one as we plan to be sufficiently ready for the next major emergency.[69]

RECOMMENDATION ONE

Governments and other stakeholders should champion the need for Priority International Communications.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- □ Government agencies must be committed to articulating their need for Priority International Communications to provide continuity of government during crises.
- □ Private sector stakeholders must be committed to articulating their need for Priority International Communications to respond effectively to crises.[70]

[61] Key Observation No. 6, *PIC is a highly leveraged enabler for emergency preparedness.*

[62] Key Observation No. 20, *Network capacity limitations are a reasonable trade-off for cost management.*

[63] Key Observation No. 24, *Ingress or egress filtering is inadequate.*

[64] Key Observation No. 1, *Some information is more important than other information.*

[65] Key Observation No. 2, *The value proposition for PIC is straightforward.*

[66] Key Observation No. 3, *The value proposition for PIC is compelling.*

[67] Key Observation No. 25, *Robustness is the word.*

[68] *Key Terms* and Figures 14 and 15.

[69] Key Observation No. 5, *PIC is for the rare but high impact events.*

[70] Includes wireline, wireless and Internet transport and includes voice, data and video applications.

Alternatives and Their Consequences

The alternatives to this approach, and their consequences, include the following:

- Do nothing and defend the position that failed communication is unavoidable in the face of network congestion during catastrophes… perpetuating unnecessary loss of life and property;
- Wait for industry to develop these capabilities without funding support… which likely won't happen, as there is little economic incentive;
- Do nothing and learn from lessons of the tragedies that occur… accepting responsibility for unnecessary, additional loss of life and property.

Benefits

When government agencies who are stakeholders for such a capability and other key private sector stakeholders champion PIC, PIC will gain the attention it needs in emergency preparedness planning. In addition, the resulting service will be more likely to meet the needs of the critical government-identified end users.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

1-1. Stakeholders from the financial services and other critical sectors articulate their need for PIC through the appropriate channels, both within their respective industries and interactions with governments.
1-2. Stakeholders from the financial services and other critical sectors publicly articulate their need for PIC to garner public support and understanding of the problem.
1-3. Appropriate governments agencies articulate their need for PIC within the appropriate internal channels.
1-4. Governments articulate their needs for PIC in public fora, as appropriate, to establish support for PIC.
1-5. Countries that have an existing national-level capability launch a dialogue to develop restrictions and policies for use of PIC.[71, 72]

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. The affected private and public sector stakeholders understand that network congestion-caused blocking is not something that we must accept during crises.
B. The appropriate decision makers in key governments receive the essential facts about PIC and the disadvantages of continuing on without it.
C. The general public learns about the benefits of having PIC, and the consequences of not having PIC, during times of crisis.
D. PIC becomes a topic in the national news, and funding for such a capability is discussed at international levels.
E. Agreements between governments on the use of PIC are made.

#1
Governments and other stakeholders should champion the need for Priority International Communications.

[71] This can be either bilateral or multilateral. A bilateral approach will be simpler to accomplish one at a time, but requires repetition. A multilateral approach will initially be more complex and likely take longer, but will also engage more countries more quickly.

[72] Key Observation No. 38, *Momentum Needed.*

4.2 Due Diligence for Modern International Crisis Management

Purpose

This recommendation is about governments fulfilling their inherent fiduciary responsibilities to protect the interests of those who are counting on them, particularly in a major crisis.

Background

Citizens expect their government leaders to be prepared for handling emergencies. Experts and stakeholders understand that priority communications is vital to a country's well-being.[73] In today's connected world, communications need to be international.[74]

This report submits that to be considered adequately prepared for emergencies, governments must install available technological solutions that ensure high probably of completion for the most critical international communications.[75] [76] It further submits that the scope of these communications is international.

As a prerequisite to ensuring the most critical communications, governments must identify the most critical government and private sector functions. Encouragingly, governments have already done so.[77] However, the question follows, once those functions have been identified, how do we ensure that they continue to operate during a crisis? In part, these functions must be able to communicate during and after a catastrophe, and this capability must extend to offices, colleagues, suppliers and others across borders.[78]

PIC is not needed every day. But it is most likely to be vital in crises that are of low-probability and high-consequence[79] For this reason, governments must prepare for the full spectrum of threats.[80] PIC is vital in any crisis that requires international communications, which would otherwise fail due to congestion (Table 2 and Table 3).

Both the relative speed with which this capability can be implemented, and its low-cost, make it very attractive. When weighed against the lives and property to be saved, the argument for installing PIC is compelling.[81]

RECOMMENDATION TWO

Governments should maintain a capability for authorized users to communicate internationally with priority over public networks during times of congestion.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- □ Governments must be committed to ensuring effective essential communications during crises.
- □ Governments must be committed to identifying private-and-public-sector functions and individuals who play a vital role during a crisis response, and who are otherwise essential for the continued operation of government and critical infrastructure.
- □ Network operators must be committed to cooperating with governments in operating and maintaining

[73] 87% of respondents agreed with the statements "*A good emergency preparedness plan should include provisions for priority communication*" and "*A priority communications scheme is vital to the well-being of a country's citizen*" (81% indicated they 'strongly agree"); Interactive Participant Polling, *Proceedings of the IEEE CQR Workshop on Priority Communications on Public Networks Workshop*, Bratislava, Slovakia, September 2008.

[74] Key Observation No. 8, *Priority communications capabilities need to be extended internationally.*

[75] Key Observation No. 4, *National-level priority schemes are field-tested and effective.*

[76] Figure 12. Value – Engineered Capacity Relationship with PIC.

[77] Key Observation No. 7*, The concept of critical functions widely accepted around the world.*

[78] Key Observation No. 1, *Some information is more important than other information.*

[79] Key Observation No. 5, *PIC is for the rare but high impact events.*

[80] Key Observation No. 38, *Momentum Needed.*

[81] Key Observation No. 3, *The value proposition for PIC is compelling.*

priority communications capabilities at international gateways.[82, 83]

- □ Governments must be committed to participating in the development of international standards for Priority International Communications capabilities.
- □ Governments must provide funding to the private sector to develop and deploy a Priority International Communications capability, and for its ongoing maintenance and administration.[84]

Alternatives and Their Consequences

Alternatives to this approach include the following.

- ○ Governments do not implement any priority communications capability... resulting in greatly impeded communications during and after major crises;
- ○ Governments rely on national level emergency communications schemes... placing their country at risk of being significantly isolated during and immediately after a major crisis;
- ○ Governments fail to adequately fund PIC... and the capability is not implemented or implemented but poorly maintained, limiting its effectiveness in a crisis;
- ○ Governments fail to effectively identify and manage those individuals with critical emergency-response functions... rendering PIC of little value. If everybody can have priority, then in reality, no one has priority.

Benefits

Government and industry leaders and decision makers will be able to communicate internationally throughout emergency responses to major crises. By identifying a limited set of essential authorized users, priority can be afforded to these users even in a highly congested, damaged network.

Next Steps

Suggested next steps that can generate and maintain the momentum for implementing this recommendation include the following:

2-1. Two or three governments with existing national-level capabilities meet to establish agreements for emergency international communications that allow authorized calls to complete in congested networks.[85]

2-2. Governments that establish effective bilateral PIC agreements create and share their methodology with governments interested in implementing a PIC capability.

2-3. Governments make PIC a budgetary priority and fund its implementation and maintenance.

2-4. Governments create a database of vital functions and corresponding individuals to administer priority communications.

2-5. Network operators, equipment suppliers and governments convene to agree on technical requirements and implementation strategies.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Appropriate funding is provided to establish and maintain PIC for a growing number of countries.

B. When a crisis occurs, individuals with vital functions are authorized to make international calls with priority through congested networks.

#2
Governments should maintain a capability for authorized users to communicate internationally with priority over public networks during times of congestion.

[82] At least two countries are needed to create one agreement.

[83] This can be either bilaterally or through intergovernmental organizations.

[84] Key Observation No. 34, *There is a range of funding architecture options.*

[85] Key Observation No. 14, *PIC accommodates priority levels.*

4.3 Network Provisioning of Priority International Communications

Purpose

This recommendation asks network operators to cooperate in the implementation and ongoing maintenance of a PIC capability.

Background

Network operators own, operate and maintain the equipment that makes communications services possible.[86] The network operators may be working on behalf of the government, private industry, or as the result of collaboration between the sectors. These network operators are responsible for assuring communications during normal times and during catastrophes.[87] Apart from the special dedicated communications systems used by the emergency services (police, fire), military, diplomatic and other special cases, the public networks host the ubiquitous national and international communications for the populous and industry, including the critical infrastructure for the countries.[88]

Therefore, to make PIC a reality, network operators will need to cooperate with international peers at network interface points known as "gateways" in the industry.[89] The gateways can be used to create the interoperability between public networks or private, dedicated networks that a country may have in place. In most cases these networks are already interconnected and interoperable at these gateways with their international network peers.[90] The addition will be that preferential treatment and mapping of priority schemes between countries will now be performed at these gateways.[91]

RECOMMENDATION THREE

Network operators should provide leadership, cooperating with each other and governments to implement and maintain Priority International Communications capabilities in their networks.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- □ Network operators must be committed to cooperating with governments to operate and maintain priority communications capabilities.
- □ Network operators, in order to ensure the viability of PIC, should help develop international standards and participate in the fora related to PIC's implementation.
- □ Governments must provide funding for the capability and for its maintenance and administration.
- □ Governments must create a funding model for network equipment suppliers that provide the software capabilities.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- ○ Network operators are incapable of reaching an arrangement to support PIC . . . as a result, their network lacks international robustness when congested and their country is sub-optimally prepared for major crises;
- ○ In a competitive market, a single network operator is selected, or attempts to be, the sole provider of PIC . . . having the effect of less redundancy in network connectivity and possibly access.

[86] *Key Terms*, Network Operator.

[87] Key Observation No. 7*, The concept of critical functions is widely accepted around the world.*

[88] Key Observation No. 8, *Priority communications capabilities need to be extended internationally.*

[89] *Key Terms*, Gateway.

[90] Key Observation No. 10*, Implementation can be relatively quick.*

[91] Key Observation No. 13, *International peering agreements are nonexistent.*

Benefits

If implemented, this recommendation will enhance a country's ability to respond to a crisis with the expertise of the network operators, the ubiquitous coverage of public networks and the convenience of existing devices.

The more network operators that cooperate, the more coverage will be provided, resulting in greater access. Furthermore, the more priority communications is implemented, the lower the development cost per country for such capabilities at both the international and national levels.[92]

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

3-1. Network operators reach out to their respective government stakeholders to encourage their support of PIC capabilities.

3-2. Network operators and governments convene PIC-planning meetings to establish priority capabilities, identify funding sources and develop interface policies with international networks.[93] [94] [95]

3-3. Network operators work collaboratively with their peers to promote broad deployment of priority capabilities, both nationally and internationally.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Network operators implement PIC interfaces with international peers.

B. Governments conduct periodic testing of PIC capabilities.

C. When a major crisis occurs, this enables robust Priority International Communications to authorized users, saving lives and property.

#3
Network operators should provide leadership, cooperating with each other and governments to implement and maintain Priority International Communications capabilities in their networks.

[92] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*

[93] The agenda for such meetings should include ASPR for the mapping of priority levels, trust chain, authorization, authentication, accounting, security, abuse, and expectations for reserve capacity for national use. Key Observation 15, *Complete ASPR for optimizing PIC.*

[94] Key Observation No. 36, *There are three basic components for priority communications.*

[95] Key Observation No. 40, PIC deployment has special *market considerations.*

4.4 Technology Deployment Leadership

Purpose

This recommendation calls to action the few major network equipment suppliers that are the source of the technology and systems on which PIC will be provided.

Background

The variability of payload is an underappreciated reality of emerging networks, and as a technical challenge, equipment suppliers are in the best position to deal with it.[96] This recommendation calls on equipment suppliers to provide network equipment that can perform essential functions under stress.[97] Since current technologies present increasingly sophisticated challenges for bandwidth management, the systems must include priority capabilities.[98] Integrating these capabilities is no different from providing reliable hardware or quality software.[99] To minimize costs and optimize long-term value, such capabilities should be designed from the beginning using international standards.[100]

Major equipment suppliers do the "heavy lifting" when it comes to technology development. Because PIC will work with existing end-user devices and network systems, the primary deliverable for equipment suppliers is software that will reside on existing network equipment.[101] Several equipment suppliers have already programmed their systems with standards-based software to support countries that have a national-level priority capability. [102, 103] In fact, one benefit of more coordination on priority communications at the international level is that the overall costs for an individual country can be expected to decrease as the benefits of higher volumes in the marketplace come into play.[104]

It is essential that the capabilities described here be funded, as real resources will be needed to design, develop and test these capabilities. As with other software features, there is a lifecycle of support required by equipment suppliers.[105] Once the investment to provide PIC is made, it is important to keep the capability current by updating it with the most recent protocols and standards. [106]

RECOMMENDATION FOUR

Network equipment suppliers should provide international standards-based software within their systems to support Priority International Communications capabilities.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- □ Network equipment suppliers must be committed to building network systems with priority communications capabilities.
- □ International standards development organizations (SDOs) must be committed to keeping Priority International Communications capabilities updated as new technologies and services emerge.
- □ Network equipment suppliers must be committed to providing upgrades to priority communications capabilities as standards evolve for new technologies and services.
- □ Governments must be committed to providing funding that effectively supports the equipment suppliers in their upgrades to PIC.[107]

[96] Key Observation No. 23, *Payload is "the new software."*

[97] Key Observation No. 25, *Robustness is the word.*

[98] Key Observation No. 18, *Communication services are more than voice.*

[99] Key Observation No. 23, *Payload is "the new software".*

[100] Key Observation No. 17, *Following standards is wise.*

[101] Key Observation No. 29, *PIC is software.*

[102] Section 2.4 *Existing Capabilities.*

[103] Key Observation No. 4, *National-level priority schemes are field-tested and effective.*

[104] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*

[105] Key Observation No. 36, *There are three basic components for priority communications.*

[106] Key Observation No. 16, Applications and services will *continue to evolve.*

[107] Key Observation No. 34, *There is a range of funding architecture options.*

Alternatives and Their Consequences

Alternatives to this approach include the following:

- ○ Network equipment suppliers do not implement PIC capabilities in their equipment . . . resulting in inadequately robust networks.
- ○ Network equipment suppliers implement non-standards-based protocols to support PIC . . . resulting in incompatibility between different networks..
- ○ Network equipment suppliers make an initial deployment of a PIC capability but fail to update with evolving standards . . . resulting in limited capabilities, as new services and applications emerge.

Benefits

The cooperation of the major network suppliers is essential for PIC to be realized. However, once PIC is developed and deployed in the major global suppliers' global equipment, it will be easier for these suppliers to recover their cost, as the larger market can support lower prices, further expanding the market opportunities.[108] Also, by deploying PIC, countries without a national-level priority capability will be better able to acquire it. In addition, a standards-based capability would result in lower development costs because of re-use, as well as increased interoperability and reliability.

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

4-1. Network equipment suppliers review international standards for PIC and work with SDOs to confirm correct interpretation.
4-2. Network equipment suppliers provide cost estimates to network operators and governments.[109]
4-3. Governments make commitments for funding PIC.
4-4. Network equipment suppliers develop the software to implement PIC capabilities within their systems.[110]
4-5. Network equipment suppliers work with their respective network operators to plan for deployment and network and end user testing of PIC features.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Network equipment suppliers develop PIC capabilities in their major network elements, as appropriate.
B. Network equipment suppliers work with each other, network operators and SDOs to promote the continued evolution of PIC standards that will track emerging applications and services.
C. When a major crisis occurs, PIC is used to enable robust communications across borders.

#4
Network equipment suppliers should provide international standards-based software within their systems to support Priority International Communications capabilities.

[108] Key Observation No. 39, *National-level emergency preparedness interests will also benefit.*

[109] Key Observation No. 34, *There is a range of funding architecture options.*

[110] Key Observation No. 40, *PIC deployment has special market considerations*

5. Conclusion

This report presents the case for urgent private and public sector attention and action to implement priority communications at the international level. The case is made based on technologies that have proven effective on the national level, sound business fundamentals, international standards and security considerations that will help governments around the world protect lives and property.

This report further calls upon both the private and public sector to step up to new leadership roles and take new steps. To this end, specific commitments that are required of both the private and public sector are clearly presented in the report's four recommendations.

We cannot predict the times, locations and nature of future catastrophes. However, we can greatly improve our response to these disasters because the solution is at our fingertips.

Mike Lemanski

KEY TERMS

This section provides important information for critical areas of emphasis for PIC. Each of the terms defined below are critical for articulating and understanding the PIC concept capability, value proposition, expected performance and implementation.

Authorization

For the PIC capability presented in this report, nation-state governments are recognized as the entities empowered to assign priority communications to individuals, devices or functions. In practical terms, what this often means is that qualified organizations apply for priority communications services for specific critical functions.

Availability

The PIC capability is designed to be available continuously (24 hours per day, 7 days per week). Since PIC will depend upon the public and private networks of the given countries where it is deployed, it will be limited by the reliability of these networks, which typically have availability performance in the order of 99% to 99.999% uptime.[111]

Communications

This term includes traditional (i.e. voice) and emerging communications (i.e. data, video) that are being used by individuals supporting critical functions for public safety, economic stability and national security.[112] Some of the services may be real-time sensitive, near real-time sensitive or non-real-time sensitive.[113]

Gateway

A gateway is a network node that leads to another network. This other network may use different protocols, or may be under a different jurisdiction, like that of another country. Gateways perform important functions to ensure compatibility. An international gateway serves as an interface between the networks of country A and other countries (Figure 14).

Industry Roles

The types of organizations involved in implementing PIC include the following:

- Equipment suppliers that design and develop the hardware or software for the elements that are the building blocks of networks and the devices used by subscribers.[114]
- Network operators that build and operate communications networks with the network elements produced by equipment suppliers.[115]
- Service providers that provide the communications services to which end users subscribe, and that are often, but not always, the same as the network operators.[116]
- Standards Development Organizations (SDOs) that develop consensus technical standards and protocols.[117]
- Governments that provide regulatory oversight of their respective communications industry, ensure emergency preparedness communications capabilities are current, negotiate international peering agreements with other countries, and authorize priority privileges to qualified users.[118]

[111] These range endpoints are also known as "2 9's" and "5 9's", respectively. 99% uptime means that a system is available for all but 5,000 minutes (3.5 days) per year; 99.999% uptime translates to 5 minutes of downtime per year. The higher end performance is associated with the landline networks of developed countries, where as the lower range performance is associated with wireless networks in developing countries.

[112] Section 2.5, *Scope*.

[113] Key Observation No. 27, *Services and time orientation matters.*

[114] e.g. Ericsson, Huawei, Microsoft.

[115] e.g. AT&T, Reliance, Vodafone.

[116] In addition to those immediately above, Bharti Airtel is an example,

[117] e.g. IEEE, IETF, ITU.

[118] Nation-state level governments

International

International means taking place between two or more countries. Priority communications at the international level ultimately means that the most important communications can get through between users in different countries. PIC should be viewed as an extension of national priority schemes.[119]

Priority

The key term in PIC is "priority." It means that some calls (or more generally, communications) are more important than others.[120] It further means that, based on that relative importance, they will be treated differently—i.e. more importantly—under specific conditions, namely network congestion.[121]

Priority is complicated at the international level because it is expected that there will be different views on what "priority" should be. There are technical solutions that help manage the anticipated difference between countries.[122]

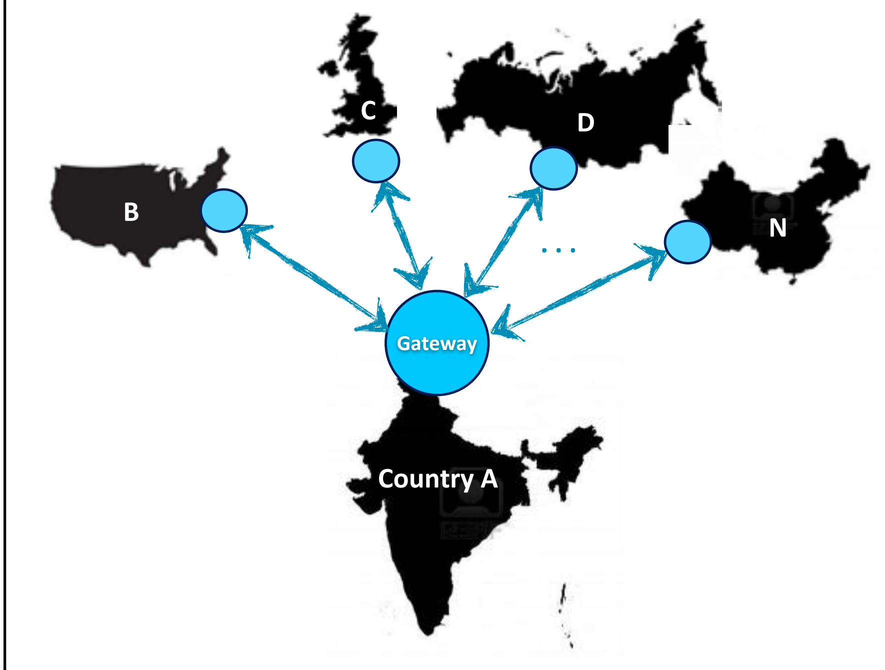


Figure 14. International Gateways

Robustness

The PIC capability is a classic example of robustness. Robustness is the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions.[1] In the case of PIC, the conditions are extreme traffic loads, reduced network capacity, or both. Robustness of the world's communications networks means that the most important functions—in this case the most important communications—still complete during times of stress that exceeds normal operating conditions.[2]

The key aspects of robustness are the ability to maintain critical functions, but not all functions, within the context of both internal and external challenges, that are of any degree of variability from expected conditions. In addition, robustness expectations should diminish with increased stress. [3][A1]

[1] IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

[2] Definitions of robustness may vary in the emphasis they place on (a) where the challenges come from - internal (e.g., component failure) or external (e.g., environmental), (b) the degree to which such challenges are anticipated - ranging from conditions slightly beyond what is expected to anything unexpected, and (c) the level of stability of functionality maintained during the period of stress. Rauscher, Karl F., Availability and Robustness of Electronic Communications Infrastructure (ARECI) Report, European Commission, March, 2007, ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .

[3] Ibid.

[119] There is a lifecycle of critical *international* activities that are needed to support PIC that include (a) negotiating priority levels, (b) electronically transmitting priority levels between countries, (c) periodically testing the international capability and (d) properly treating priority communications in-country when presented at a gateway.

[120] Key Observation No. 1, *Some information is more important than other information.*

[121] Interestingly, if there is no network congestion, a priority call will be treated differently, but in this case the call may take slightly longer to complete because of the additional checks required. However this difference is on the order of milliseconds.

[122] See Key Observation No. 14, *PIC accommodates different priority levels*, and Figure 11.

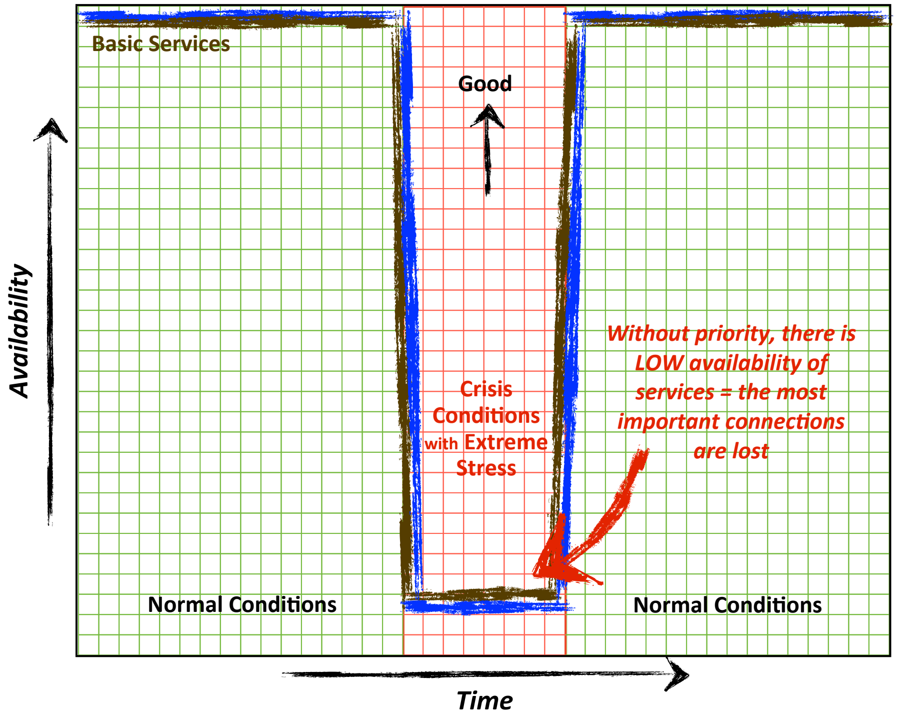

Basic Services
Good
Availability
Crisis Conditions with Extreme Stress
Without priority, there is LOW availability of services = the most important connections are lost
Normal Conditions
Normal Conditions
Time

Figure 15. No Robustness: Critical Service Availability Failure without PIC

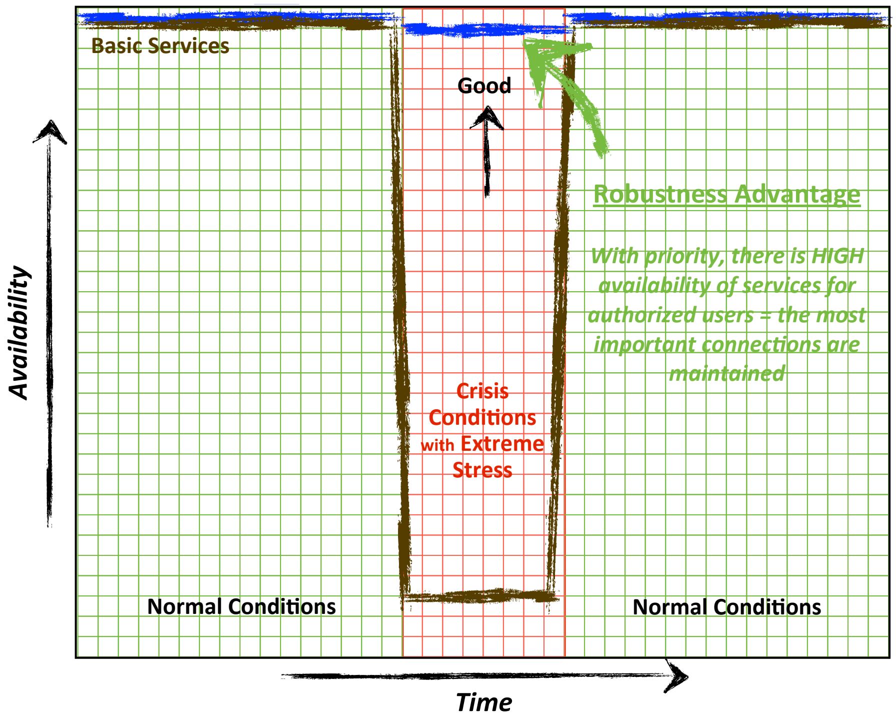

Basic Services
Good
Availability
Robustness Advantage
With priority, there is HIGH availability of services for authorized users = the most important connections are maintained
Crisis Conditions with Extreme Stress
Normal Conditions
Normal Conditions
Time

Figure 16. Robustness: Critical Service Availability Failure with PIC[123]

Related terms include reliability, dependability, resilience and survivability. Network security relates to the subject matter in that compromises of security can cause infrastructure failures, and vice versa.

Figures 4 and 5 show the difference that PIC can have. Figure 4 shows that critical services are unlikely to complete during the times when most needed (i.e. during a crisis resulting in network congestion). In contrast, figure 5 depicts the completion of the most critical communications with PIC, even during a crisis that has caused network congestion.

[123] PIC does not increase the absolute bandwidth size. This diagram holds true for when the critical service calls are a small percentage of basic service calls.

ACRONYMNS

3D	Three Dimension
3G	Third Generation Mobile Communications
4G	Fourth Generation Mobile Communications
8i	Eight Ingredient (Framework for Information and Communications Technology Infrastructure)
ACCOLC	Access Overload Control
AI	Artificial Intelligence
ARECI	Availability and Robustness of Electronic Communications Infrastructure (Report for EC)
ASCII	American Standard Code for Information Interchange
ASPR	Agreements, Standards, Policies and Regulations
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BWA	Broadband Wireless Access
C7 SS7	Signalling System 7
CDMA	Code Division Multiple Access
DDoS	Distributed Denial of Service (Attack)
DHS	Department of Homeland Security (U.S.)
DOCSIS	Data Over Cable Service Interface Specification
DoS	Denial of Service (Attack)
DSCP	Differentiated Service Code Point
DSP	Digital Signal Processing
EC	European Commission
eMLPP	3GPP, enhanced Multi Level Precedence and Pre-emption service
ENISA	European Network and Information Security Agency
ETS	Emergency Telecommunications Service
EU	European Union
EWI	EastWest Institute
FCC	Federal Communications Commission (U.S.)
FEMA	Federal Emergency Management Agency (U.S.)
FTPAS	Fixed Telecommunications Privileged Access Scheme (U.K.)
GETS	Government Emergency Telecommunications Service
GSM	Global System for Mobile Communication
GTPS	Government Telephone Preference Scheme (U.K.)
GUCCI	Global Undersea Communications Cable Infrastructure
ICT	Information and Communications Technology

ACRONYMNS

IEEE	Institute of Electrical and Electronics Engineers
IEPS	International Emergency Preparedness Scheme
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol v4 and v6
PIC	Priority International Communications
ISP	Internet Service Provider
ITU	International Telecommunication Union
LTE	Long Term Evolution
MTPAS	Mobile Privileged Access Scheme (U.K.)
NCS	National Communications System (U.S.)
NGN	Next Generation Networks
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee (for the U.S. president)
PCN	Pre-Congestion Notification
RFC	Request for Comments
PSAP	Public Service Answering Point
RPH	Resource Priority Header
SCP	Service Control Point
SDH	Synchronized Digital Hierarchy
SDO	Standards Development Organization
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SONET	Synchronized Optical Networking
TDM	Time-Division Multiplexing
TETRA	Terrestrial Trunked Radio
UMTS	Universal Mobile Telecommunications Service
UN	United Nations
WCI	Worldwide Cybersecurity Initiative
WERT	Wireless Emergency Response Team
WIFI	Wireless Fidelity IEEE 802.11
WIMAX	Worldwide Interoperability for Microwave Access IEEE 802.16
WLAN	Wireless Local Area Network
WPS	Wireless Priority Communications Service

REFERENCES

3GPP, *Access Class Barring and Overload Protection (ACBOP)*, TR 23.898 , http://www.3gpp.org/ftp/Specs/html-info/23898.htm.

3GPP, *enhanced Multi Level Precedence and Pre-emption service (eMLPP)*, TR22.067, http://www.3gpp.org/ftp/Specs/html-info/22067.htm .

Caples, Ingrid, Wade, Jerry, *Planning for NS/EP Next Generation Network Priority Services during Pandemic Events*, The Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 7 Final Report, December 2010.

Carpenter, Guy, *The World Catastrophe Re-Insurance Market: Steep Peaks Overshadow Plateaus,* Guy Carpenter & Company, Inc., 2006.

Chandrashekhar, R., *Report of the Working Group on Information Technology Sector Twelfth Five Year Plan (2012-2017)*, Government of India Ministry of Communications & Information Technology Department of Information Technology.

Berz, Gerhard, Loster, Thomas and Wirtz, Angelika, *Natural Catastrophes – January to September 2002,* Munich Reinsurance Company, 2002.

Call Traffic Surge Jammed Mobile Phone Networks, The Times of India, July 14, 2011.

Damas, J., Graff, M.,and Vixie, P., *Extension Mechanisms for DNS,* Internet Systems Consortium.

European Network and Information Security Agency (ENISA), www.enisa.europa.eu.

Folts, H, and Ohno, H., *Functional Requirements for Priority Services to Support Critical Communications,* IETF 2000.

Goldman, Stuart, O., *Primer on the International Aspects of the International Priority Communications Policy.*

Government Emergency Telecommunications Service Fact Sheet, U.S. Department of Homeland Security, Press Office, Washington, D.C.

Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) User Council Meeting Report, Department of Homeland Security, National Communications System, January 2012.

Gunn, J., et al*. Requirements for SIP Resource Priority Header in SIP Responses,* October, 2007 (Work in progress).

IEEE CQR Workshop on Priority Communications on Public Networks Workshop (Proceedings of the), Bratislava, Slovakia, September 2008, http://committees.comsoc.org/cqr/Slovakia.html .

IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

Influenza Pandemic: Sustaining Focus on the Nation's Planning and Preparedness Efforts, GAO-09-334, February 2009.

Internet Engineering Task Force (IETF), www.ietf.org .

International Telecommunication Union (ITU), www.itu.int.

Inventory and Analysis of Protection Policies in Fourteen Countries, An, International Critical Information Infrastructure Protection (CIIP) Handbook 2004, Swiss Federal Institute of Technology.

ITU-T Rec. E.106, "International Emergency Preference Scheme for disaster relief operations (IEPS)."

ITU-T Rec. H.460.4, "Call priority designation for H.323 calls"

ITU-T Rec. H.460.14, "Support for Multi-Level Precedence and Preemption (MLPP) within H.323 Systems"

ITU-T Rec. J.260, "Requirements for Emergency/Disaster Communications over IPCablecom Networks"

ITU-T Rec. J.pref, "Specifications for Emergency/Disaster Communications over IPCablecom Networks." (work in progress)

ITU-T Rec. H.460.MB, "Message Broadcast for H.323 Systems" (Work in progress).

ITU-T Rec. M.3350, "TMN service management requirements for information interchange across the TMN Xinterface to support provisioning of Emergency Telecommunication Service (ETS)."

ITU-T Q-series Recommendations, "Emergency services for IMT-2000 networks – Requirements for harmonization and convergence." Supplement 47.

ITU-T Rec. Y.1271, "Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packed-switched networks."

ITU-T Rec. Y.NGN-ET-Tech "Next Generation Networks—Emergency Telecommunications –Technical Issues"

Kaithal, A., Klecha, J., and Polk, J., IANA Registration of the UC and CUC Session Initiation Protocol (SIP) Resource-Priority Namespaces, Cisco Systems, July, 2011 (Work in progress).

Krock, Richard, E., Priority Emergency Communications, McGraw-Hill 2011 Yearbook of Science & Technology.

Mase, K.; Azuma, N.; Okada, H., *Development of an Emergency Communication System for Evacuees of Shelters*, Wireless Communications and Networking Conference (WCNC), IEEE, 2010.

Moncaster, T., Briscoe, B., Menth, M, *A Pre-Congestion Notification (PCN) Encoding Using 2 Differentiated Service Code Points (DSCP)s to Provide 3 or More States,* IETF RFC: 2012.

Murphy, S., BGP Security Vulnerabilities Analysis, Sparta, Inc., January, 2006 (Work in progress).

Murphy, Sandra and Badger, Madelyn, *OSPF with Digital Signatures*, Network Working Group, June, 1996. (work in progress)

Murphy, Jr., T., Rieth, P., and Stevens, J., *iSeries Telnet Enhancements*, IBM Corporation, January, 2004. (work in progress)

National Communications System, U.S. Department of Homeland Security, NCS Video, April 2008, gets.ncs.gov/docs.html .

Pacific Telegraph Act - An Act to Facilitate Communication between the Atlantic and Pacific States by Electric Telegraph, Chapter 137, U.S. Statutes, 36th Congress, 1st Session, 1860.

Polk, James, IANA Registration of New Session Initiation Protocol (SIP) Resource-Priority

Namespaces October, 2008 (Work in progress).
Polk, James*. IANA Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*, ECRIT Working Group July, 2007 (Work in progress).

Privileged Access Schemes: *MTPAS, FTPAS and Airwave,* U.K. Cabinet Office, www.cabinetoffice.gov.uk/content/privileged-access-schemes-mtpas-ftpas-and-airwave .

Procedural Outage Reduction: Addressing the Human Part, ATIS Network Reliability Steering Committee (NRSC), Washington, D.C., May 1999.

R Q-Series Supplement 53 "Signaling support for International Emergency Preferential Scheme (IEPS)"

Rauscher, Karl F., *Availability and Robustness of Electronic Communications Infrastructure (ARECI)* Report, European Commission, March, 2007, ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .

Rauscher, Karl Frederick, *Mutual Aid for Resilient Infrastructure in Europe, (MARIE)* Phase I Report), ENISA, 2011.

Rauscher, Karl Frederick, *ROGUCCI Study and Global Summit Report*, IEEE Communications Society, 2010.

Resilient Communications, U.K. Cabinet Office, www.cabinetoffice.gov.uk/content/resilient-communications.

Samaritan's Purse International Relief, www.samaritanspurse.org .

Telecom Regulatory Authority of India, *Priority Call Routing in Mobile Networks for Persons Engaged in 'Response and Recovery' Work During Emergencies*, New Delhi, November 2011.

Schulzrinne, H., Communications Resource Priority for the Session Initiation Protocol (SIP), February 2006. *Work in progress*.

Signalling for IEPS support in ISUP: Q.761 Amd.3, Q.762 Amd.3, Q.763 Amd.4, and Q.764 Amd.4

Signalling for IEPS support in BICC: Q.1902.1 Amd.2, Q.1902.2 Amd.3, Q.1902.3 Amd.3, and Q.1902.4 Amd.3

Signalling for IEPS support in DSS2: Q.2931 Amd.5

Signalling for IEPS support in ATM AAL2: Q.2630.3 Amd.1

Signalling for IEPS support in CBC: Q.1950 Amd.1 Annex G

USTDA Supports India's Efforts To Expand Integrated Emergency Communications System, U.S. Trade and Development Agency, March 2011.

U.S. Federal Communications Commission (FCC), www.fcc.gov .

U.S. President's National Security Telecommunications Advisory Committee (NSTAC), The, www.ncs/gov/nstac .

Wireless Emergency Response Team (WERT), www.wert-help.org .

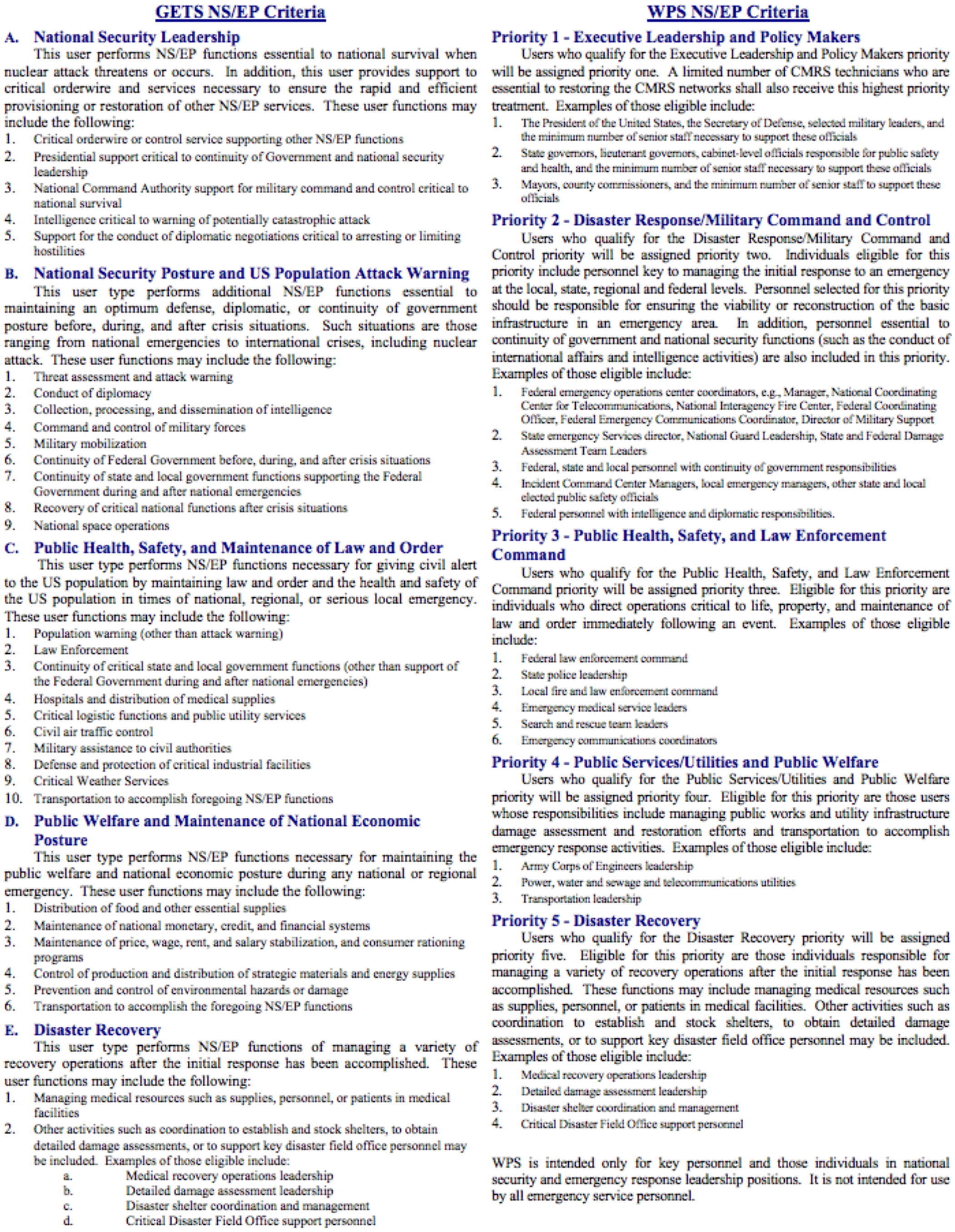
Wireless Priority Service Fact Sheet, U.S. Dept. of Homeland Security, Press Office, Washington, D.C.

Workshop on Telecommunications for Disaster Relief, February 2003. http://www.itu.int/ITU-T/worksem/ets/program.html.

APPENDIX A

GETS and WPS Priority Level Assignment Criteria

The following description of prioritization levels is provided as a reference to enhance further understanding for how levels may be determined and managed. It compliments Key Observation 14, PIC accommodates different priority levels and Figure 8, Example of Mapping of Priority Levels.



GETS NS/EP Criteria

A. National Security Leadership

This user performs NS/EP functions essential to national survival when nuclear attack threatens or occurs. In addition, this user provides support to critical orderwire and services necessary to ensure the rapid and efficient provisioning or restoration of other NS/EP services. These user functions may include the following:

1. Critical orderwire or control service supporting other NS/EP functions
2. Presidential support critical to continuity of Government and national security leadership
3. National Command Authority support for military command and control critical to national survival
4. Intelligence critical to warning of potentially catastrophic attack
5. Support for the conduct of diplomatic negotiations critical to arresting or limiting hostilities

B. National Security Posture and US Population Attack Warning

This user type performs additional NS/EP functions essential to maintaining an optimum defense, diplomatic, or continuity of government posture before, during, and after crisis situations. Such situations are those ranging from national emergencies to international crises, including nuclear attack. These user functions may include the following:

1. Threat assessment and attack warning
2. Conduct of diplomacy
3. Collection, processing, and dissemination of intelligence
4. Command and control of military forces
5. Military mobilization
6. Continuity of Federal Government before, during, and after crisis situations
7. Continuity of state and local government functions supporting the Federal Government during and after national emergencies
8. Recovery of critical national functions after crisis situations
9. National space operations

C. Public Health, Safety, and Maintenance of Law and Order

This user type performs NS/EP functions necessary for giving civil alert to the US population by maintaining law and order and the health and safety of the US population in times of national, regional, or serious local emergency. These user functions may include the following:

1. Population warning (other than attack warning)
2. Law Enforcement
3. Continuity of critical state and local government functions (other than support of the Federal Government during and after national emergencies)
4. Hospitals and distribution of medical supplies
5. Critical logistic functions and public utility services
6. Civil air traffic control
7. Military assistance to civil authorities
8. Defense and protection of critical industrial facilities
9. Critical Weather Services
10. Transportation to accomplish foregoing NS/EP functions

D. Public Welfare and Maintenance of National Economic Posture

This user type performs NS/EP functions necessary for maintaining the public welfare and national economic posture during any national or regional emergency. These user functions may include the following:

1. Distribution of food and other essential supplies
2. Maintenance of national monetary, credit, and financial systems
3. Maintenance of price, wage, rent, and salary stabilization, and consumer rationing programs
4. Control of production and distribution of strategic materials and energy supplies
5. Prevention and control of environmental hazards or damage
6. Transportation to accomplish the foregoing NS/EP functions

E. Disaster Recovery

This user type performs NS/EP functions of managing a variety of recovery operations after the initial response has been accomplished. These user functions may include the following:

1. Managing medical resources such as supplies, personnel, or patients in medical facilities
2. Other activities such as coordination to establish and stock shelters, to obtain detailed damage assessments, or to support key disaster field office personnel may be included. Examples of those eligible include:
   a. Medical recovery operations leadership
   b. Detailed damage assessment leadership
   c. Disaster shelter coordination and management
   d. Critical Disaster Field Office support personnel

WPS NS/EP Criteria

Priority 1 - Executive Leadership and Policy Makers

Users who qualify for the Executive Leadership and Policy Makers priority will be assigned priority one. A limited number of CMRS technicians who are essential to restoring the CMRS networks shall also receive this highest priority treatment. Examples of those eligible include:

1. The President of the United States, the Secretary of Defense, selected military leaders, and the minimum number of senior staff necessary to support these officials
2. State governors, lieutenant governors, cabinet-level officials responsible for public safety and health, and the minimum number of senior staff necessary to support these officials
3. Mayors, county commissioners, and the minimum number of senior staff to support these officials

Priority 2 - Disaster Response/Military Command and Control

Users who qualify for the Disaster Response/Military Command and Control priority will be assigned priority two. Individuals eligible for this priority include personnel key to managing the initial response to an emergency at the local, state, regional and federal levels. Personnel selected for this priority should be responsible for ensuring the viability or reconstruction of the basic infrastructure in an emergency area. In addition, personnel essential to continuity of government and national security functions (such as the conduct of international affairs and intelligence activities) are also included in this priority. Examples of those eligible include:

1. Federal emergency operations center coordinators, e.g., Manager, National Coordinating Center for Telecommunications, National Interagency Fire Center, Federal Coordinating Officer, Federal Emergency Communications Coordinator, Director of Military Support
2. State emergency Services director, National Guard Leadership, State and Federal Damage Assessment Team Leaders
3. Federal, state and local personnel with continuity of government responsibilities
4. Incident Command Center Managers, local emergency managers, other state and local elected public safety officials
5. Federal personnel with intelligence and diplomatic responsibilities.

Priority 3 - Public Health, Safety, and Law Enforcement Command

Users who qualify for the Public Health, Safety, and Law Enforcement Command priority will be assigned priority three. Eligible for this priority are individuals who direct operations critical to life, property, and maintenance of law and order immediately following an event. Examples of those eligible include:

1. Federal law enforcement command
2. State police leadership
3. Local fire and law enforcement command
4. Emergency medical service leaders
5. Search and rescue team leaders
6. Emergency communications coordinators

Priority 4 - Public Services/Utilities and Public Welfare

Users who qualify for the Public Services/Utilities and Public Welfare priority will be assigned priority four. Eligible for this priority are those users whose responsibilities include managing public works and utility infrastructure damage assessment and restoration efforts and transportation to accomplish emergency response activities. Examples of those eligible include:

1. Army Corps of Engineers leadership
2. Power, water and sewage and telecommunications utilities
3. Transportation leadership

Priority 5 - Disaster Recovery

Users who qualify for the Disaster Recovery priority will be assigned priority five. Eligible for this priority are those individuals responsible for managing a variety of recovery operations after the initial response has been accomplished. These functions may include managing medical resources such as supplies, personnel, or patients in medical facilities. Other activities such as coordination to establish and stock shelters, to obtain detailed damage assessments, or to support key disaster field office personnel may be included. Examples of those eligible include:

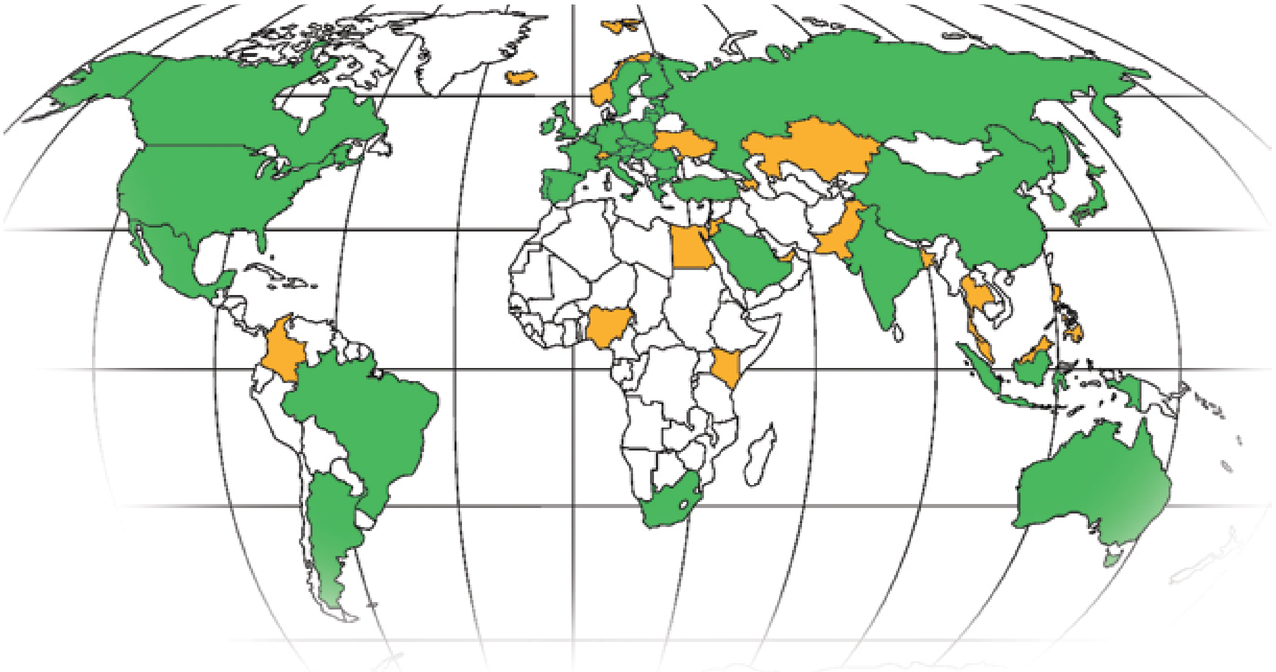
1. Medical recovery operations leadership
2. Detailed damage assessment leadership
3. Disaster shelter coordination and management
4. Critical Disaster Field Office support personnel

WPS is intended only for key personnel and those individuals in national security and emergency response leadership positions. It is not intended for use by all emergency service personnel.

APPENDIX B

EastWest Institute
Worldwide Cybersecurity Initiative

Cyber40
The G20 + the next most important nations in cyberspace



G20

Argentina
Australia
Brazil
Canada
China
France
Germany
India
Indonesia
Italy

Japan
Mexico
Republic of Korea
Russia
Saudi Arabia
South Africa
Turkey
United Kingdom
United States
European Union

+

Azerbaijan
Bangladesh
Cameroon
Colombia
Egypt
Iceland
Israel
Jordan
Kazakhstan
Kenya
Malaysia

Nigeria
Norway
Pakistan
Philippines
Qatar
Singapore
Switzerland
Thailand
Ukraine
United Arab Emirates

EWI Board of Directors

Angela Chen (U.S.)
Founder and Managing Director
Global Alliance Associates
Partner
Epoch Fund

Michael Chertoff (U.S.)
Co-founder & Managing Principal
Chertoff Group

David Cohen (U.K.)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman & Co-Founder
Planet Heritage Foundation

Adel Ghazzawi (U.A.E.)
Founder
CONEKTAS

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Emil Hubinak (Slovak Republic)
Chairman & CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference
Global Head of
Governmental Affairs
Allianz SE

Anurag Jain (India)
Chairman
Laurus Edutech Pvt. Ltd.

James L. Jones (U.S.)
Former U.S. National Security
Advisor

Haifa Al Kaylani (U.K.)
Founder & Chairperson
Arab International Women's Forum

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

Mark Maletz (U.S.)
Senior Fellow
Harvard Business School

Kevin McGovern (U.S.)
Chairman
The Water Initiative
Co-Founder
SOBE Beverages

T. Michael Moseley (U.S.)
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Tsuneo Nishida (Japan)
Ambassador Extraordiary &
Plenipotentiary
Permanent Rerpesentative of Japan
to the U.N.
Permanent Mission of Japan to the
U.N.

Ronald P. O'Hanley (U.S.)
President,Asset Management
and Corporate Services
Fidelity Invesments

Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab
Emirates in Washington, D.C.

Admiral (ret) William A. Owens
(U.S.)
Chairman
AEA Holdings Asia
Former Vice Chairman
U.S. Joint Chiefs of Staff

Sarah Perot (U.S.)
Director & Co-Chair for
Development
Dallas Center for Performing Arts

Louise Richardson (U.S.)
Principal
University of St. Andrews

John Rogers (U.S.)
Managing Director
Goldman Sachs & Co.

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
CEO
Bud Smith Organization Inc.

Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President & CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor & Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill Inc.

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

Founded in 1980, the EastWest Institute is a global, action-oriented think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) nonprofit organization with offices in New York, Brussels and Moscow. Our fiercely guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI New York Center
11 East 26th St.
20th Floor
New York, NY 10010
1-212-824-4100

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka St. 7/5,
Building 1, 6th Floor
Moscow 125009
7-495-2347797

EWI Washington Office
1069 Thomas Jefferson St. NW
Washington, DC 20007
1-202-492-0181

www.ewi.info