

INDUSTRY CONNECTIONS REPORT



DIGITAL RESILIENCE IC ACTIVITY

FOUNDATIONAL PRINCIPLES FOR DIGITAL RESILIENCE FRAMEWORK

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGEMENTS

Special thanks are given to Prof. Salma Abbasi (eWorldwide Group) who authored the document, and to the following reviewers from inside and outside the Digital Resilience Industry Connections Activity:

1. Aida Karazhanova, Economic Affairs Officer, United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)
2. Ashirwad Tripathy, Cofounder and Executive Director (Educating Nepal)
3. Mohamed Abida, Acting Head, Islamic Development Bank (IsDB)
4. Nicholas Napp, Co-Founder, xMark Lab
5. Prof. Bong-Keun Jung, Associate Professor, Seoul National University (SNU)
6. Prof. Stefan Sauermann, Program Director Medical Engineering and eHealth, University of Applied Sciences Technikum Wien
7. Raja Segaran, Head, Strategy and Research, Malaysia Digital Economy Corporation (MDEC)
8. Rezwanul Jami, Head of eCommerce, Aspire to Innovate (a2i) Programme
9. Rony Soerakoesoemah, Head, Sub Regional Office for South-East Asia, Economic Affairs Officer, United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)
10. Samia Melhem, Lead Policy Officer, the World Bank (WB)
11. Sanjay Srivastava, Chief, Disaster Risk Reduction, Economic Affairs Officer, United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)
12. Sunghee Chung, Consultant, United Nations Lecturer, Chinese University of Hong Kong
13. Paul Lam, Strategy and Policy Officer (Digital and Technology), Asian Infrastructure Investment Bank (AIIB)

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. December 2021. Printed in the United States of America.

PDF: STDVA25101 978-1-5044-8192-2

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: <http://standards.ieee.org>.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association (“IEEE SA”) Industry Connections publication (“Work”) is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied “AS IS” and “WITH ALL FAULTS.”

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at <http://standards.ieee.org/about/sasb/iccom/>.

This Work is published with the understanding that IEEE and the ICom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

FOUNDATIONAL PRINCIPLES FOR DIGITAL RESILIENCE FRAMEWORK.....	5
1. INTRODUCTION	5
2. PURPOSE	6
3. CRITICAL MULTI-SECTOR STAKEHOLDERS.....	7
4. FOUNDATIONAL PILLAR	7
4.1. HOLISTIC DIGITAL INFRASTRUCTURE.....	7
4.2. NETWORKS AND INFORMATION SYSTEMS RESILIENCE	8
4.3. INTEROPERABLE AND COMPATIBLE SYSTEMS AND DATA.....	9
4.4. ACCESSIBILITY, AFFORDABILITY, AND INCLUSION OF VULNERABLE COMMUNITIES.....	9
4.5. CYBERSECURITY AND RESILIENCE	10
4.6. DIGITAL IDENTITY	10
4.7. DATA ECOSYSTEM	11
4.8. ETHICAL AND INCLUSIVE DESIGN PRINCIPLES.....	11
5. HUMAN-CENTRIC PILLAR	12
5.1. SAFETY, SECURITY, AND PRIVACY.....	12
5.2. DATA OWNERSHIP AND AGENCY	13
5.3. DATA SOVEREIGNTY AND TRUST.....	14
5.4. DIGITAL SKILLS AND KNOWLEDGE	14
5.5. EMPATHY	15
6. ENVIRONMENTAL PILLAR.....	15
6.1. URBAN, RURAL, AND HARD-TO-REACH COMMUNITIES.....	16
6.2. CULTURAL, TRADITIONAL, SOCIAL, AND SOCIETAL.....	16
6.3. PROMOTING THE UPTAKE OF DIGITAL SERVICES	17
7. THEMATIC AREAS.....	18
7.1. DISASTER AND CRISIS MANAGEMENT	18
7.2. FOOD SECURITY AND INTEGRATED AGRICULTURE VALUE CHAIN	18
7.3. HEALTHCARE ACCESS AND TELEMEDICINE	19
7.3.1. MEDICAL SUPPLIES, TESTING, TRACING, TRACKING, AND VACCINATION DISTRIBUTION	19
7.3.2. MENTAL WELLNESS AND ADDICTION	20
7.4. RESTORING AND RECALIBRATING SOCIAL SECURITY SYSTEMS	20
7.5. BUSINESS CONTINUITY, TELECOMMUTING, AND TELEWORKING.....	21
7.6. EDUCATION, KNOWLEDGE, AND TELE-LEARNING	22
7.7. PEOPLE-CENTRIC ECONOMY.....	22
7.7.1. FINANCIAL INCLUSION	23
7.7.2. INNOVATION AND ENTREPRENEURSHIP	24
7.8. DIGITAL AND SOCIAL MEDIA AND NEWS	24
7.9. ENTERTAINMENT.....	25
7.9.1. EGAMING.....	26
7.9.2. EGAMBLING	26
7.9.3. ESPORTS	27
8. CONCLUSION.....	27

FOUNDATIONAL PRINCIPLES FOR DIGITAL RESILIENCE FRAMEWORK

1. INTRODUCTION

Holistic digital resilience helps individuals, organizations, communities, and nations recognize and effectively manage the wide variety of risks emanating from natural disasters and extreme climate events, health crises like the COVID-19 pandemic, and online threats.

A clear lesson from COVID-19 is that the future will continue to be disruptive—new trends and shocks will continue to affect lives—which is why resilience building is more crucial than ever. Another clear lesson is the importance of digitalization and digital resilience as the world becomes more dependent on digital systems and technologies to cope, recover, adapt, and evolve in this new reality.

Today, people are growing up in an increasingly digital world, and digital technologies are present in most areas of life. Despite the digital divide among different sections of society, digitalization overall is increasing and contributing to our interconnectedness. Furthermore, the rapid rise of Digital Transformation and the Fourth Industrial Revolution are driving the widespread adoption of these technologies. The 2030 Agenda for Sustainable Development firmly positions digital technologies as enablers to achieving the Sustainable Development Goals (SDGs) by stimulating innovation and enhancing efficiencies.¹ For example, digital technologies have extended healthcare to remote areas, improved agricultural productivity and farmers' access to markets, and promoted financial inclusion through mobile money. More recently, digital technologies have been playing a vital role in supporting COVID-19 response and recovery.

At the same time, COVID-19 has exposed how vulnerable our interconnected systems are at every level. The world has experienced the downside of being dependent on global supply chains to fulfil local demand for medical protective equipment, common household supplies, and even basic food supplies. There has also been a rise in cyberthreats and online fake news with very real impacts on public health and safety. The most critical lesson from the pandemic is that it is imperative to rethink and redesign our strategy for enhancing digital resilience and adopt a holistic approach to solving these problems.

The systemic nature of the transformation that is needed post-COVID-19 has significant consequences for public policy, i.e., if governments address each new crisis as it arises, with the same growth narrative and perverse

¹ United Nations General Assembly, "Transforming our world: The 2030 Agenda for Sustainable Development," seventieth session, agenda items 15 and 116 (A/RES/70/1), https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.

incentives as before, there will be a similar disjointed response and again face similar disruptions, undermining development gains and the capacity to protect and enhance quality of life.

**“THE ADOPTION OF HOLISTIC
DIGITAL RESILIENCE BY DESIGN,
NOT BY DISASTER, IS ESSENTIAL
POST-COVID-19.”**

A review of national and organizational policies and strategies on digital resilience over the past decade reveals that their narrow focus on the physical and technical elements of protecting digital infrastructures, systems, data, and products from external threats such as cyberattacks and disasters, has been inadequate for responding to COVID-19. Furthermore, as recent cyber-attacks have shown, even with such a narrow focus many of these policies and strategies have been utterly ineffective. They have left out the human, economic, societal, and environmental elements, particularly, in increasing the opportunities of digital innovations to meet the diverse needs of communities and individuals, while reducing the barriers and harms caused by these digital technologies on vulnerable communities and individuals with limited resources and capabilities.

The adoption of holistic digital resilience by design, not by disaster, is essential post-COVID-19. This will require involvement at all levels of the social fabric including government, the private sector and civil society. An integrated “people, planet and prosperity” recovery model² and concerted investment in research, digitalization and innovation-led transformation will allow the world to emerge from this pandemic more resilient as individuals, as organizations, and as communities.

2. PURPOSE

Keeping in view the need to redesign systems, the intent is to develop a holistic Digital Resilience Framework. To that end, foundational principles have been developed that will be reflected in the framework, which will guide individuals, organizations, and communities in assessing and crafting a strategy to address the immediate threats of COVID-19 and build long-term resilience in a holistic and integrated manner across society, the economy, and the environment. The framework comprises 25 elements across four interrelated pillars: (1) foundational; (2) human; (3) environmental; and (4) cross-cutting themes. They are essential for strengthening communities and countries against future shocks and crises, and enabling citizens to fully reap the benefits of digital technologies and improve their lives.

This framework is for use by all individuals, private organizations, and government agencies involved in ensuring the well-being of society as a whole and its individual segments through digitalization in the face of disruptions caused by catastrophes like COVID-19. The implementation of this framework should be viewed as a supplement to existing resilience ecosystems. In addition, close consideration should be given to the role of this framework in safeguarding the most vulnerable sections of society.

² European Commission, “Protect, prepare and transform Europe: Recovery and resilience post COVID-19,” ESIR Policy Brief No. 1, May 2020, https://ec.europa.eu/info/sites/info/files/research_and_innovation/groups/esir/ec_rtd_esir-recovery-resilience-covid19.pdf.

3. CRITICAL MULTI-SECTOR STAKEHOLDERS

The successful implementation of the Digital Resilience Framework requires the involvement of a variety of stakeholders including governments and regulatory authorities, industries and the private sector, United Nations agencies, development banks, universities and research institutions, civil society, and non-profit organizations, and most importantly citizens and communities.

It is clear that no one sector, group, or country can address the complexities of current and future crises and challenges alone. Cooperation and collaboration among multi-sector stakeholders are important in building holistic digital resilience to help ensure coordinated response and recovery in future crises and disasters. Collaborative efforts range from mobilizing and sharing knowledge, expertise, and technological innovations, to investments and financing at local to global levels.

This means bridging traditional sector silos and merging different disciplines, establishing interoperability, forming partnerships, and ensuring that no one is left behind.

The United Nations Secretary-General's High-level Panel on Digital Cooperation calls for multi-stakeholder collaboration that involves a more diverse spectrum of stakeholders and more diverse voices, "particularly from developing countries and traditionally marginalized groups such as women, youth, indigenous people, rural populations, and older people." ³

4. FOUNDATIONAL PILLAR

To help ensure holistic digital resilience, it is necessary to build-up the foundational infrastructure and systems to allow everyone access to fast, reliable, and low-cost digital services.

4.1. HOLISTIC DIGITAL INFRASTRUCTURE

A resilient digital infrastructure is necessary to support the platforms of a digital economy and society. The digital infrastructure is the physical hardware and related software that enables end-to-end information and communications systems to operate. It includes the Internet backbone, fixed-broadband infrastructure (fiber-optic cable networks), mobile communications infrastructure and networks, broadband communications satellites, data and cloud computing facilities, end-user equipment [computers, IEEE 802.11 (Wi-Fi), IEEE 802.15 (Bluetooth) networks], software platforms, and network edge devices (sensors, robots).

Advanced digital economies have leveraged frontier technologies, such as artificial intelligence, big data, blockchain, the Internet of Things and robotics to tackle COVID-19, facilitate physical distancing, accelerate recovery, and promote growth. However, to fully reap the potential of frontier technologies, countries need

³ United Nations Secretary-General's High-level Panel on Digital Cooperation, "The Age of Digital Interdependence," June 2019, <https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf>.

high-speed broadband connectivity. Yet, many middle- and low-income countries continue to lack readiness to adopt and apply frontier technologies because of their inadequate digital infrastructure preparedness. This includes the lack of availability and coverage of digital infrastructure, particularly in rural and remote regions that are not commercially viable, and the low speed and reliability with which data flows in these economies.

Additionally, there are growing interlinkages and interdependencies between critical infrastructures, including with transport and energy infrastructures, which are needed to support global supply chains and help ensure food security. Without reliable power grids and micro-grids, power digital solutions cannot be powered. At the same time, critical infrastructures are becoming digitalized and made “smart” through the roll out of smart grid, smart city, and intelligent transportation system projects, which further increase our reliance on a resilient digital infrastructure.

“EFFORTS TO ENHANCE NETWORKS AND INFORMATION SYSTEMS’ RESILIENCE INCLUDE PROMOTING RESILIENCE-BY-DESIGN BY ENSURING REDUNDANCY AND DIVERSITY OF NETWORK ROUTES AND EQUIPMENT IN THE DIGITAL INFRASTRUCTURE; AND INCREASING THE SPEED AND SCALE AT WHICH RESOURCES CAN BE MOBILIZED AND ACCESSED FOR RESTORATION OF SERVICES WHEN ATTACKED OR HIT BY CRISES OR DISASTERS.”

4.2. NETWORKS AND INFORMATION SYSTEMS RESILIENCE

A system is resilient if it continues to serve its purpose efficiently and effectively in the face of adversity,⁴ that is, if it provides the required capabilities despite excessive stresses that can cause disruptions. Networks and information systems must be resilient to enable governments and organizations to effectively deal with disruptions caused by adverse events like COVID-19 and provide continuity of service. Government agencies, private entities, and individuals must share responsibility for developing and maintaining the resilience of systems necessary for timely provision of critical public services in difficult times and ensure that network systems are well maintained and administered through life.

Efforts to enhance networks and information systems’ resilience include promoting resilience-by-design by ensuring redundancy and diversity of network routes and equipment in the digital infrastructure; and increasing the speed and scale at which resources can be mobilized and accessed for restoration of services when attacked or hit by crises or disasters. This would require preparedness planning, establishment of cooperation mechanisms to facilitate emergency access to relevant resources and infrastructure sharing, and conduct of regular drills and tests of the emergency plans.

⁴ Donald Firesmith, “System Resilience: What Exactly is it?” Software Engineering Institute, Carnegie Mellon University, 25 November 2019, https://insights.sei.cmu.edu/sei_blog/2019/11/system-resilience-what-exactly-is-it.html.

4.3. INTEROPERABLE AND COMPATIBLE SYSTEMS AND DATA

Interoperability is the ability of digital content to perform all its functionalities in interaction with the digital environment.⁵ The interoperability and compatibility of digital systems can enhance data and information available to the public, foster transparency in the larger community and enhance collaboration with government agencies, the public, and non-profit and private entities involved in developing digital resilience during and post-COVID-19.

It is important that governments promote strong inter-state and inter-agency collaboration, develop interoperable digital content and standards for use by the collaborating agencies, and ensure implementation of these standards within existing government infrastructure, as well as develop tools and resources to assist the private sector in adopting the standards.

4.4. ACCESSIBILITY, AFFORDABILITY, AND INCLUSION OF VULNERABLE COMMUNITIES

Over half the world's population continue to have no or low bandwidth Internet access and are unable to reap its benefits.⁶ COVID-19 has exposed the depths of this gap. While enabling work, education, health, commerce, and cultural and social services to move online, the digital divide—the uneven access to and use of digital technologies between demographics and regions—has never been more pronounced.

Today, a third of the global population still do not have 3G coverage, which means they do not have access to a reliable Internet connection.⁷ Beyond coverage, there is a divide in adoption where those with coverage may not use the Internet due to lack of affordability. Although the cost of devices and data plans have fallen in recent years, they remain too high for many—nearly 2.5 billion people live in countries where the cost of the cheapest available smartphone is a quarter or more of the average monthly income.⁸ The COVID-19 crisis could make devices and data plans even less affordable with the disrupted supply chains and increased poverty, further aggravating existing divides.

Marginalized and vulnerable communities are often excluded because of inadequate infrastructure, the lack of affordability of devices and data plans, and the lack of relevant content and skills. Today, the majority (80%) of

⁵ Wolfgang Kerber and Heike Schweitzer, "Interoperability in the Digital Economy," *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 8, no. 1 (2017), <https://www.iipitec.eu/issues/jipitec-8-1-2017/4531>.

⁶ Mahe Bayireddi, "Access For All: Why Digital Accessibility Matters And What Tech Professionals Can Do About It," *Forbes*, 22 October 2019, <https://www.forbes.com/sites/forbestechcouncil/2019/10/22/access-for-all-why-digital-accessibility-matters-and-what-tech-professionals-can-do-about-it/?sh=70f74417b4ea>.

⁷ World Economic Forum, "Accelerating Digital Inclusion in the New Normal: Playbook," July 2020, http://www3.weforum.org/docs/WEF_Accelerating_Digital_Inclusion_in_the_New_Normal_Report_2020.pdf.

⁸ Teddy Woodhouse, "Mobile devices are too expensive for billions of people — and it's keeping them offline," World Wide Web Foundation, 6 August 2020. Available at <https://webfoundation.org/2020/08/mobile-devices-are-too-expensive-for-billions-of-people-and-its-keeping-them-offline/>.