IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT

DIGITAL RESILIENCE IC ACTIVITY

SUSTAINABLE, SECURE, AND INCLUSIVE DIGITAL RESILIENCE (DR)

IEEE

Documents
Document Sharing Hub

Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

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: STDVA25100 978-1-5044-8191-5

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.

Copyright © 2021 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

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 ICCom 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.

Copyright © 2021 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

TABLE OF CONTENTS

1. INTRODUCTION 7
2. HOW IS DIGITAL RESILIENCE BEING DEFINED? 8
3. WHAT ARE THE RISKS AND CONSEQUENCES OF ADOPTING A NARROW VIEW OF DIGITAL RESILIENCE? 12
4. WHY DO WE NEED A HOLISTIC APPROACH TO DIGITAL RESILIENCE? 16
5. CONCLUSION AND RECOMMENDATIONS 19
6. REFERENCES 20

Documents
Document Sharing Hub

Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

SUSTAINABLE, SECURE, AND INCLUSIVE DIGITAL RESILIENCE (DR)

ABSTRACT

A clear lesson from the COVID-19 crisis is that it is not guaranteed that the future will become less disruptive—new trends and shocks will continue to affect people's lives, which is why resilience-building is more crucial than ever. The response to this unprecedented crisis demonstrates another clear lesson—the importance of digitalization and digital resilience as the world becomes more dependent on digital systems and technologies to cope, recover, adapt, and transform in this new reality.

A systematic review of national and organizational policies and strategies on digital resilience over the past decade reveals that their narrow focus on developing and protecting digital infrastructures, systems, data, and products from external threats such as cyberattacks and disasters, has been inadequate for responding to the COVID-19 pandemic.

The focus on the physical and technical aspects of digital resilience risks leaving out the human aspects, particularly, in maximizing the opportunities of digital innovations to meet the diverse needs of communities and individuals, while minimizing the barriers and harms caused by these digital technologies on vulnerable and marginalized groups with limited resources and capabilities.

For instance, a research study illustrates that the UK policy focus on provision of access to broadband is crucial but as it has not been sufficiently linked to inclusion and multi-stakeholder participation strategies, individuals have not been able to fully reap the potential of broadband to strengthen their resilience.

This paper calls for a radical shift in mindset for a holistic people-centered approach to digital resilience, otherwise future crises could further intensify poverty, hunger, and inequalities, and could reach levels beyond our capacity to recover. This broadening of perspective requires engagement with the digital ecosystem—i.e., the stakeholders, systems, and enabling environments that together empower people and communities to use digital technology to pursue economic and social opportunities, while taking steps to reduce risks.

Reflecting and leveraging on the debates, discussions, and current climate, a thirteen-point agenda was developed by the eWorldwide Group as a useful framing that focuses on: (1) information and communications technology (ICT) infrastructure resilience; (2) cybersecurity, digital privacy, and trust; (3) disaster and crisis management; (4) food security and smart logistics; (5) healthcare and telemedicine; (6) mental wellness and addiction; (7) education and skills development; (8) decent work and teleworking; (9) innovation and entrepreneurship; (10) digital access and inclusion; (11) financial inclusion, fintech, and blockchain; (12) data and statistics; and (13)

Copyright © 2021 IEEE. All rights reserved.

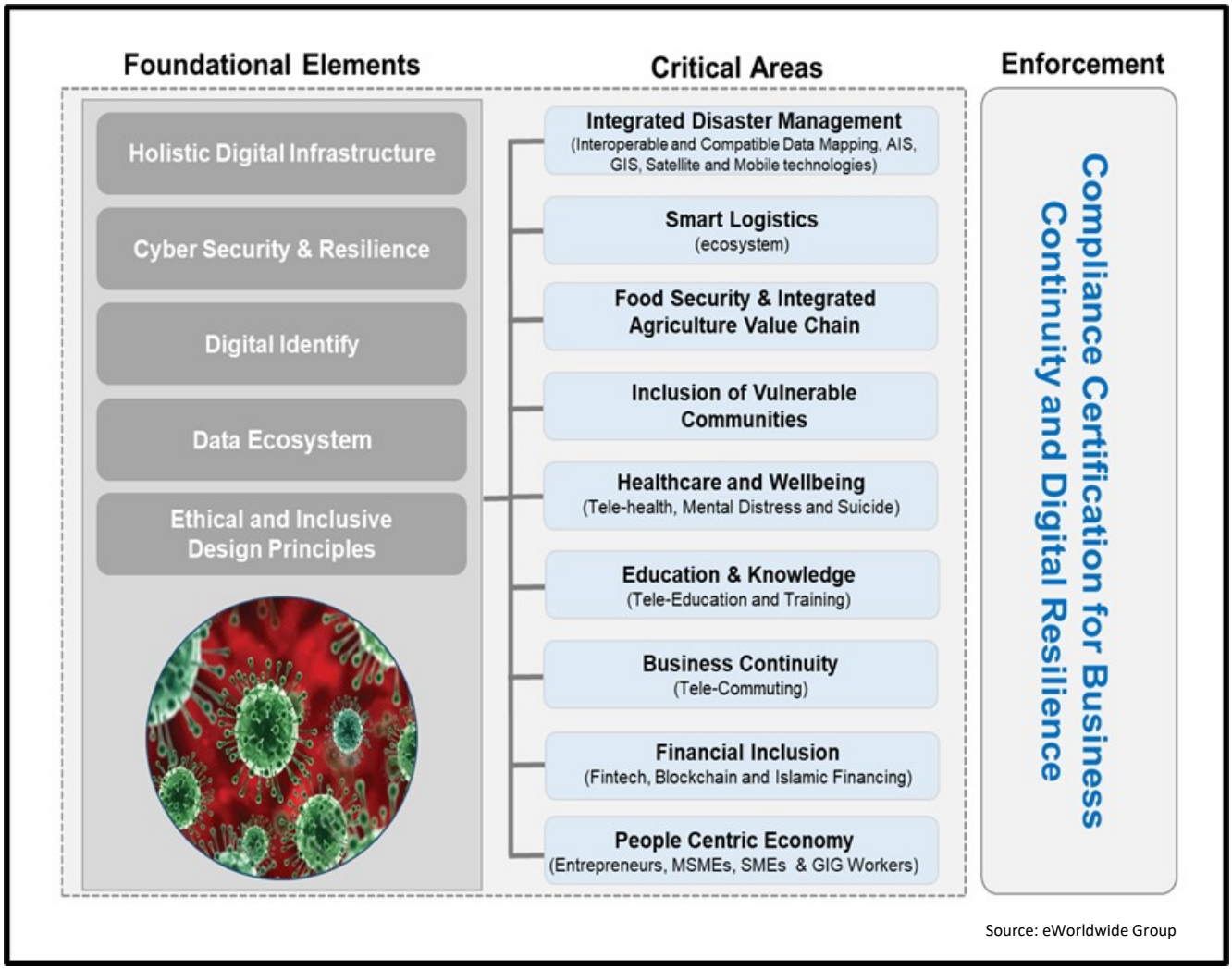
Documents
Document Sharing Hub

Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

communication and digital media.

Implementing the agenda that can drive transformational change towards achieving the Sustainable Development Goals will undoubtedly be a challenge. As next steps, the following actions are recommended: (1) appoint a thought leader/champion with multidisciplinary skills capable of delivering a holistic vision and leading multi-stakeholder collaborations in digital resilience to facilitate dialogue and partnerships; (2) engage in dialogue and partnerships with multiple stakeholders across traditional silos, strengthen understanding, identify shared values, and co-create solutions in building digital resilience; (3) include the participation of marginalized and vulnerable groups; (4) adopt a resilience lens in policymaking and include the local contexts and perception of risks of marginalized and vulnerable groups in decision-making, policies, and plans; (5) provide incentives and financing for accelerating holistic digital resilience interventions that are multi-sectoral and inclusive; and (6) invest in global data interoperability, compatibility, and streamlining to allow effective and resilient response to the COVID-19 pandemic and other crises. A holistic overview of the components is given in FIGURE 1.

FIGURE 1 Holistic overview of components



Copyright © 2021 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

1. INTRODUCTION

Digital resilience has recently been elevated to a global priority for governments, businesses, development agencies, and society at large, due to the vital and versatile role technology is playing to support COVID-19 response and recovery. In this new reality, resilience building is fundamental as disruptions and uncertainties will increase in frequency and magnitude due to future public health crises, climate-related disasters, and geopolitical events.

Resilience can be defined as the ability of nations, communities, organizations and, individuals to withstand, recover from, adapt to, and potentially transform amid change and uncertainty [40].[1] Resilience includes looking at the ability to "bounce back better" or "bounce forward" by improving the physical, economic, social, political, and environmental conditions during the recovery process to further strengthen resilience and agility.

Digital resilience, as we will see in the next section, is often defined as the ability of information and communications technology (ICT) systems to withstand and recover from external threats such as cyberattacks and disasters ([53], [3], [19], [36], [55], [18]) However, digital resilience can also mean the application of digital systems and technologies to holistically build resilience in the local context. In fact, digital systems and technologies are already recognized as critical for achieving the United Nations Sustainable Development Goals (SDGs) ([69], [75], [45], [72]). The COVID-19 pandemic has further marked their indispensability—as a lifeline for individuals and organizations, and as an essential force in curbing the spread of COVID-19 and accelerating research in treatments and vaccines.

At the same time, the pandemic has clearly exposed the inequalities in access to digital technologies and major technological challenges that have yet to be addressed. Women, older persons, persons with disabilities, ethnic minorities, indigenous groups, migrants, refugees, internally displaced persons, and poor people living in rural and remote areas are disproportionately without access to digital technologies and are "left behind" as education, work, and public services move online.

"We will focus on enabling countries to plan, adopt, and benefit from seamless and secure technologies that provide effective clinical and public health solutions to accelerate the achievement of the health and well-being related SDGs. This means leaving no one behind—children or adults, rural or urban, with digital solutions to improve their health and well-being."

~ World Health Organization [21]

As people, organizations, information, and services are becoming more interconnected globally, we must address digital resilience in a holistic manner for the benefit of humanity. Frontier technologies like 5G, artificial intelligence (AI), blockchain, big data analytics, cloud computing, and the Internet of Things (IoT) are bringing enormous opportunities for transformation, but also significant challenges, especially related to access, privacy, security, and trust, and these challenges should not be unfairly borne by poor and vulnerable people.

[1] Numbers in brackets refer to bibliographical references found in Section 6.

Copyright © 2021 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021

Health data and digital technologies, for example, are essential for improving global health outcomes. However, the lack of global standards that promote interoperability and integration prevent governments, researchers, and enterprises, particularly those from the least developed countries, from leveraging health data and technologies to improve the quality and delivery of healthcare services and achieve the SDGs. This is compounded by the lack of legal, ethical, and accountability systems in place to protect people against maligned and inappropriate use of data and technologies, with implications on people's rights, safety, and well-being. Social media platforms have become the vehicle that many people use to obtain information, but they have also been misused by some to spread dangerous disinformation, and to fuel discrimination, xenophobia, and racism.

These challenges cut across various sectors, contexts, and scales, yet they are largely tackled in silos. The interlinkages between the various risks and their compounding effects are often not considered. The COVID-19 pandemic has provided us with an opportunity to rethink and reformulate our strategies for digital resilience towards current and future threats and crises. The Republic of Korea's comparatively successful COVID-19 response has been attributed to its holistic approach through close collaboration between the government, the scientific community, and the private sector, the release of open data related to COVID-19, strong protection of data privacy and security, and transparency in reporting and tracking ([41]). Similarly, in New Zealand, emphasis was placed on cooperation, government transparency, quick decisive action based on scientific data, and the holistic people-centered deployment of interventions ([51], [6], [74]).

A critical crossroad has been reached and it is imperative that action is taken now to bring about transformative and accelerated change to achieve the SDGs (i.e., societies that are digitally resilient). The next section examines the ways in which digital resilience has been narrowly defined at the national, organizational, and individual levels, and is followed by a look at the risks and consequences of adopting this narrow view of digital resilience. Section 4 provides justification for a holistic approach to digital resilience, and the paper concludes with some recommendations for the way forward.

2. HOW IS DIGITAL RESILIENCE BEING DEFINED?

Digital resilience has been considered at the individual, organizational, and national levels.

At the individual level, digital resilience is recognized as an essential "21st century skill" that centers on the ability of individuals to recognize and deal with the risks they come across when they socialize, explore, or work online ([23], [56]). This includes building resilience to extremist grooming and propaganda on social media ([8], [57], and to the massive spread of online disinformation [42].

The UK Government defines individual digital resilience as: (1) understanding when one a person is at risk online and can make informed decisions about the digital space one is in; (2) knowing what to do to seek help from a range of appropriate sources; (3) learning from experiences and is able to adapt future choices; and (4) recovering when things go wrong online by receiving the appropriate level of support to aid recovery [23].

Copyright © 2021 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Sustainable, secure, and inclusive digital resilience (DR) 2021