Global Happiness Council
Thematic group: Digital Well-being

Policy Brief 2
Resilience in Turbulent Times

Luca De Biase
Reimagine Europa, Brussels, Belgium

Keegan Mc Bride
Hertie School Centre for Digital Governance Berlin, Germany
Mohammed Bln Rashid School of Government Dubai, UAE

Gianluca Misuraca
Inspiring Futures SA, Lausanne, Switzerland
Politecnico di Milano, Department of Design, Milan, Italy

Stefano Quintarelli
Copernicani NPO, Milan, Italy
Advisory group on advanced technologies UN/CEFACT, Geneve, Switzerland

Key messages:

- We are living in a network society where technological relationships are increasingly defining our day-to-day existence.
- Technology has a key role to play in improving resilience, but only when done in cooperation with organizations, regulations, structures, and other stakeholders.
- Technological systems of the future must be oriented first towards resilience and antifragility, rather than efficiency and cost effectiveness.
- For technological systems to be increasingly resilient, attention must be given to data and archiving, interoperability, digital identities, and flexibility.

Introduction

Rediscovering the Network Society

The title of this policy brief is "Resilience in Turbulent Times", in order to start an exploration and discussion on this topic we must first provide definitional clarity for three concepts: our current time and the structure of the network society that characterize it, turbulence, and resilience.

First, we look to our current societal time. The society of today is a network society, an information society. To Manuel Castells, the network society's "chief characteristic … is the spread of networks linking people, institutions, and countries"[1] and that these "networks do not stop at the border of the nation-state, the network society constituted itself as a global system, ushering in the new form of globalization characteristic of our time."[2] In this society, networks and information reign supreme, cities grow in importance as central network nodes, but so too do suburbs and smaller towns and cities as technology enables new organizational structures, remote work, and a transition to new forms of "informational labor."[3]

It should be no surprise, then, that there is new found attention being paid to organizational "hub-and-spoke" models for businesses of the future.[4] The COVID-19 pandemic has certainly helped to speed such transitions along, with many employers and employees both realizing the potential for remote based work in terms of efficiency, effectiveness, quality of life, and other material benefits. Around the world, the COVID-19 pandemic has rapidly increased movement to rural and suburban areas from urban environments.[5]

Turbulence in times of crisis

The second concept to explore is that of turbulence. As the COVID-19 pandemic has shown, crisis can strike at any moment and change our normal operating environment in an instant. Such turbulence is inevitable. Yet, statistics appear to show that the world, or at least society, is becoming less turbulent than at any other point in history. However, there are new forms of turbulence emerging and the world is more networked and interconnected than at any point in history before. Society is completely dependent on technology and networks.

Our digital systems have been built to drive efficiency, decrease costs, and increase profits. Our technology tracks what we do, what we watch, how we live, listens to our conversations, and, while often times improving our lives, opens up new possibilities for exploitation, privacy violations, and other aspects detrimental for our well-being.

Information technologies need stability, interoperability, and order. If something changes, or does not behave as expected, entire systems can fail. Such failures may rapidly permeate throughout the entire global ecosystem almost instantaneously. A clear example of this is the effect that WannaCry had on the global economy and critical institutions, such as the UK's NHS which was brought to a standstill in a matter of minutes.

However, turbulence is necessary for evolution, innovation, and improvement. This point serves as a logical prelude to the third concept, that of resilience.

Resilience in the digital society

The concept of resilience can be explored at a number of scales. It is possible to discuss an individual's resilience, the resilience of a specific IT system, the resilience of an organization or business, the resilience of an ecosystem, or the resilience of a society.

It is also worth noticing that the term has now emerged as a popular construct in several disciplines, and in general it can be defined as "*the ability to face shocks and persistent structural changes in such a way that societal well-being is preserved, without compromising the heritage for future generations.*"[6] Here, however, we are particularly interested to the concept of digital resilience.[7] Borrowing it from the field of cyber-security and expanding in a broader perspective it can in fact be argued that "*in a constantly evolving digital environment, organizations must be able to move quickly and seamlessly to adopt new digital technology solutions and then to recover, rebound and move forward if things go wrong.*"[8] To this end it could be of interest to elaborate more on the implications of the definition of the ISO 22316, an international standard for "Security and resilience — Organizational resilience — Principles and attributes". In this standard, resilience is defined as "the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."[9] At other scales, the meaning holds true, resilience is the ability to meet and overcome

crisis or chaos and continue to function. And as we are embedded in an increasingly digital world, many organizations – both public and private - are still unaware of the extent to which they rely on digital technology and the risks that come with it.[10]

While resilience is important, some question whether resilience on its own is enough. For instance, to Nassim Nicholas Taleb, it is not. Systems should, rather, be "antifragile."[11] They must learn and adapt and when facing challenge and adversity, they must thrive. Such a conceptualization is well encapsulated by president Joe Biden's promise to "Build Back Better" made during his presidential campaign.

EXAMPLES

Data and Digital Archives

Turbulence can manifest in a number of different ways, and, therefore, a number of different responses have been sought to protect against such turbulence and improve resilience. Data and digital archives are one clear and important pillar of digitally enabled resilience. There are a number of clear contemporary and relevant examples.

In Estonia, it has been argued that there is a need for "digital continuity" and that this should ensure that there is "a solution whereby the Estonian state would endure even despite an occupation of its territory."[12] The solution was a digital embassy, which maintains a copy of Estonia's critical data and allows for seamless provision of digital services should the country be occupied. This represents not only technical resilience, but societal resilience as well.

GitHub has launched the "GitHub Arctic Code Vault", which archived every active public open-source GitHub repository 250 meters deep in Svalbard, ensuring that, in the future, open-source computer code could always be revisited.

There are initiatives to maintain important cultural and heritage aspects of society from how to make pasta by recording Italian grandmothers to genealogy to music to language and to a number of other dimensions.

The existence of data and archives in such forms relates to resilience in two ways and the importance of data and archives for resilience cannot be understated.

- First, it ensures that there is always a digital copy that can be brought back and utilized in future digital systems.
- Second, it provides opportunities for cultures to be resilient and regain potentially lost knowledge.

Digital Identity

A second key aspect of digitally enabled resilience is that of a digital identity. In the United Nations' Sustainable Development Goals, SDG 16.9 highlights the necessity for all people to have a legal identity. One of the clearest ways to reach such a goal is through widespread availability and adoption of digital identities.

Digital identities are necessary for a user to identify and authenticate themselves securely online and for a society to truly digitalize, the availability of an online digital identity is a necessity. Such digital identities not only improve resilience of society, but also for technical systems themselves. Digital identities:

- enable increased levels of technical and cyber security,
- enable new forms of innovation and delivery,
- enable new forms of economic advancement and innovation,
- support community and human development,
- and provide a number of new ways for societies and communities to prosper and thrive.

In today's world, there is a rapidly expanding availability of digital identities from both public governments and private sector providers in today's society.

At the public level, one can look to the EU where the eIDAS regulation has been implemented to set in place the rules and regulations for digital identity in Europe and thereby enables the cross-border exchange and validation of such identities.

For the private sector, digital identities are the ultimate competitive asset, as those entities controlling the identity can exert a high degree of control of the relationship with the user.[13] Companies such as Facebook have become instrumental to the identity ecosystem by enabling businesses and organizations to allow customers and clients to sign up for services using Facebook's SSO (Single Sign On) toolset.

Yet, in many countries, the availability of a legal identity is still hard to obtain. As the world becomes increasingly digital, and more of life moves into the digital, the presence and availability of a digital identity will become increasingly important. Thus, the absence of such identities has implications for the continuance and furtherance of systemic inequality and limits opportunities for advancement and development. To compound on this, there are also a number of clear potential risks for widespread adoption of digital identities, and it is therefore paramount that such initiatives are trustworthy.[14]

Interoperability

A third key aspect of digitally enabled resilience is that of interoperability.

Interoperability implies that different systems can exchange, use, and display the same information and data. Interoperability requires common standards, vocabularies, mappings, definitions, schemas, and dictionaries.

The internet, at its core, is all about interoperability, and, therefore, the global network society is all about interoperability. Increasingly interoperable systems will hasten the development of innovation and digital advances, increase resilience, but, simultaneously, open up poorly designed networks for risks in times of chaos or crisis.

Interoperable systems allow for organizations to communicate with each other, enable the rapid spread of information, lead to better dissemination of knowledge, and drastically improve the efficiency and effectiveness of systems.

It is for this reason that many new technological developments and advances place interoperability at their core. This has given rise to the "API-first" mentality, where interoperability, enabled by APIs, is placed at the core of all developments. Recent developments in cloud architectures and containerized applications have also hastened the development of interoperable systems.

These developments are happening at all levels and in all sectors.

In the EU, there is now initiatives to connect governmental databases and enable the cross-border exchange of governmental data using a federated architecture and piloted in projects such as TOOP.

In healthcare, initiatives such as openEHR has developed a set of open specifications for e-Health projects.

Cities, in the aim of becoming 'smart', have begun to work on interoperable public transport systems, where private methods of transport, taxis, ridesharing, bicycling, and other methods are integrated with governmental and urban transport networks.

Governments have also begun to experiment with the concept of "rules as code", which allows for rules to be understood and consumed by technological systems, thus improving compliance and regulation via interoperable standard.

In November of 2020, eu-LISA, the EU organization responsible for the management and organization of large-scale IT projects and systems, organized an event titled "Interoperability as the Essential Building Block for Digital Resilience."[15] Clearly, interoperability is important for resilience.

One of the clearest ways that interoperability enables resilience is associated with the large number of governances, regulatory, legal, societal, and technical changes that must be made to create truly interoperable digital societies and digital systems.

Additionally, resilience is enabled as interoperable systems can, during times of crisis, be integrated, adopted, changed, or innovated at a quicker pace. This not only allows for digital systems to meet crises and turbulence from a stronger position, but also bounce back, recover, and innovate after the crisis has passed.

Flexibility

A final key aspect of digitally enabled resilience is that of flexibility.

One of the great advantages of digital technologies is that new and innovative services, infrastructures, innovations, and solutions can be developed and implemented quickly – if done correctly.

A clear example of this can be seen from the global "Hack the Crisis" event where thousands of technical prototypes were built to respond to the COVID-19 pandemic in a number of days.[16] While not all solutions ended up in use, many were brought on board by governmental organizations and aided in the fight against the pandemic.

In many countries, schools quickly moved to digital education methods, utilizing already existing software such as Microsoft Teams, Skype, Zoom, or Google Hangouts. While this was not the initial intended purpose of such software, it further demonstrates how technical tools, once built, can often times be easily pivoted to fit other needs.

One way to ensure that such services or other technical programs can remain flexible, agile, and adaptive is through the use of cloud computing which enables services to scale horizontally and vertically almost instantaneously, helping to ensure that they do not fail.

Cloud computing enables services to be readily and remotely accessible at any size or scale for a cheaper cost. By centralizing cloud hosting in data centers, it is possible to provide better security and maintenance for cheaper. In this way, services running on the cloud are often more resilient and secure than those not hosted on the cloud.

Many cloud providers, such as Amazon Web Services or Microsoft Azure, have demonstrated throughout the crisis the key role in which their cloud infrastructures play for enabling resilience. For example, Amazon recently released a report titled "How Governments can Build Resilience" and highlighted a number of public sector use cases where cloud infrastructure played a critical role for governmental organizations and resilience covering everything from healthcare to education to finance to unemployment.[17]

Though the cloud is important for enabling flexibility in the digital age, it is certainly not the only way. Other strategies to improve flexibility of digital systems are related to the use and development of free and open-source software (FOSS) and adopting modular software development methods.

FOSS projects put flexibility at their core by allowing any and all developers to change, improve, or innovate their software, they can be adapted or used for any purpose. Another strategy is related to modularity.

Modular systems break up their core components into different modules, which can be built by different teams, or substituted with different modules, and rapidly drive innovation and improve flexibility.[18]

By adopting such approaches to improve flexibility, it follows that resiliency will also improve as flexible systems will be better able to adapt or continue to function during turbulent times.

Challenges and Risks

While it is clear that digital technologies have a key role to play in improving resilience, there are a number of challenges and risks that need to be taken into account.

First, in order for digital technologies to be taken advantage of fully, they need access to information. At the governmental level, this would imply that services have access to a vat amount of personal, private, and sensitive information.

Due to the digitalized nature of such data, there are new risks when it comes to data privacy or data leaks due to improperly configured servers or due to malicious actors. Similarly, as data becomes increasingly digitalized, it becomes easier for organizations, private and public alike, to improperly use, watch, or monitor personal data.

A second risk is related to the interconnectivity necessary to make most large-scale technological systems function and interoperable. Small changes in data or the environment can cause major breakdowns in systems. Even if the technologies themselves are able to be changed or innovated upon in response to change, it may take time for such changes to spread throughout the entire ecosystem.

A third challenge is an over-reliance on technology. Technology is good for solving many problems, but, on its own, it is not enough. As the world becomes more accustomed to the use of technology for resilience and for maintain most of the world's day to day operations, there is the potential for loss of our own individual capacities. This, then, would potentially weaken resilience in the long run.

A final weakness is related to the necessity of digital identities for the long-term resilience and antifragility of the information society. Such identities are needed, but

there is also a clear right to privacy. Thus, if done improperly, some digital identities may reveal too much information and enable discrimination or persecution.

In order to counteract such risks, the EU has recently begun to explore the idea of "qualified anonymity" which allows users to authenticate and utilize online services under legally accepted pseudonyms.

Conclusions and Recommendations

Our global – networked - society is increasingly defined by the technologies, interactions, and networks between us. Technology has allowed for a rapid restructuring of how the world works, the ways in which we live, how we work, and even how value is created.

There is an increasing importance being given to technology in managing and organizing our lives. In many ways, the things we do in our day-to-day activities have been completely restructured to better serve technology, so that it can better serve us. The digital dimension has become the major user interface of the physical dimension of the world.[19] Such transformations are often related to small changes that enable easier or better data collection or reduce the complexity for the technical systems to make decisions. Undoubtedly these developments have driven increased in prosperity, human development, and well-being but, with the present regulation and its technological embodiment, at the cost of our well-being and personal privacy.

While technological solutions are often proposed and touted as being key to overcoming chaos, crises, or turbulence, this may not always be the case. In this short policy brief, it was highlighted that for technological systems to be more resilient, emphasis and focus must be paid to at least four key aspects: data and archiving, digital identities, interoperability, and flexibility.

It is not enough just to have one or the other. For systems to be truly resilient, they must tackle all four of these components not in isolation, but together.

The creation of new flexible, innovative, and modular solutions that ensure proper backups of information and the continuance of critical data combined with widespread interoperability, secured by legally verifiable digital identities will likely aid in driving resilience.

However, there is also a number of risks and threats that accompany our rapid societal technological transformation. Thus, there is a clear need for clear regulation and governance mechanisms that strike a balance between creating a digital infrastructure that is robust, antifragile, and resilient, but takes human rights and values fully into account.

In order to accomplish this, a number of initial points are offered below:

- Digital technologies cannot and will not stop crises, we will continue to experience shocks and turbulence. An over reliance on technology, and an under reliance on structure, regulation, and human networks will reduce resilience. Thus, for resilience, it is important to take a holistic approach to technological developments.
- It is not possible to look at the digital dimension and society separately, they are connected, socially constructed, and directly intertwined. Digital technologies may provide new tools to fight back against shocks, crises, and turbulence, but only as part of a broader and systemic response.
- Due to the potential for privacy violations, surveillance, and abuse any new digital transformation initiative must pay attention to the potential ethical, well-being, morale, and other negative effects.
- There is a need for increased interoperability rules, standardization, and data governance. By adopting user-centric technological solutions such as *Self Sovereign Identity* frameworks and by increasing the uptake of data vocabularies and standards, it is possible to rapidly scale interoperable systems and support the cross-border exchange of data at the global level, while protecting user privacy.
- Backups and maintenance are important, for new digital developments ensure sufficient funding is providing for future maintenance and support. The absence of such funding can rapidly reduce the resilience and robustness of technological systems.
- Put interoperability and flexibility at the core of new technological developments to improve resilience. Focusing on these characteristics first, rather than on efficiency or cost, will likely lead to stronger systems that are more resilient, anti-fragile, and, in the long run, provide a greater benefit.

Endnotes

[1] (Webster, 2006. p. 101)
[2] (Castells, 2011. p. 2)
[3] (Castells, 2011)
[4] (Laker, 2021)
[5] (Nordregio, 2021; Roper, 2021)
[6] (Giovannini et al., 2020).
[7] (UCL, 2018)
[8] (Misuraca, 2020)
[9] (ISO, 2017)
[10] (Misuraca, 2020)
[11] (Nicholas Taleb, 2014)
[12] (Kotka & Liiv, 2015. p. 152)
[13] (Stefano Quintarelli, 2019).
[14] (The Alan Turing Institute, 2021)
[15] (eu-LISA, 2020)
[16] (Garage48, 2020)
[17] (AWS, 2020)
[18] (Baldwin & Clark, 1997)
[19] (Stefano Quintarelli, 2019)

References

https://d1.awsstatic.com/WWPS/pdf/AWS_How_Governments_Can_Build_Resilience_Whitepaper.pdf

Baldwin, C., & Clark, K. (1997). *Managing in an Age of Modularity*. Harvard Business Review. https://hbr.org/1997/09/managing-in-an-age-of-modularity

Castells, M. (2011). *The Rise of the Network Society* (2nd ed.). John Wiley & Sons.

eu-LISA. (2020). *Interoperability as the Essential Building Block for Digital Resilience*. Eu-LISA. https://www.eulisa.europa.eu/Newsroom/PressRelease/Pages/eu-LISA---Interoperability-as-the-Essential-Building-Block-for-Digital-Resilience.aspx

Garage48. (2020). *Hack the Crisis*. https://garage48.org/hackthecrisis

Giovannini E, Benczur, P., Campolongo, E, Cariboni J., Manca, AR. (2020). Time for transformative resilience: the COVID19 emergency, EUR 30179 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-18113-2 doi:10.2760/062495.

ISO. (2017). *ISO - ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes*. International Organization for Standardization. https://www.iso.org/standard/50053.html

Kotka, T., & Liiv, I. (2015). Concept of Estonian Government Cloud and Data Embassies. In A. Kő & E. Francesconi (Eds.), *4th International Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2015)* (pp. 149–162). Springer International Publishing.

Laker, B. (2021, May 24). *Why Companies Should Adopt a Hub-and-Spoke Work Model Post-Pandemic*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/why-companies-should-adopt-a-hub-and-spoke-work-model-post-pandemic/amp

Misuraca G (2020) Rethinking Democracy in the “Pandemic Society” A journey in search of the governance with, of and by AI. In: CEUR Workshop Proceedings. CEUR

Nicholas Taleb, N. (2014). *Antifragile: Things That Gain from Disorder*. Random House Publishing Group.

Nordregio. (2021). *Will rural living become more desirable post-corona? | Nordregio*. Nordregio Magazine. https://nordregio.org/nordregio-magazine/issues/post-pandemic-regional-development/will-rural-living-become-more-desirable-post-corona/

Roper, W. (2021, January 19). *COVID-19: Americans want to swap city for rural areas*. World Economic Forum. https://www.weforum.org/agenda/2021/01/rural-life-cities-countryside-covid-coronavirus-united-states-us-usa-america/

The Alan Turing Institute. (2021). *Trustworthy digital identity* . The Alan Turing Institute. https://www.turing.ac.uk/research/interest-groups/trustworthy-digital-identity

University College London, (2018). Understanding the challenges of resilience in digital environments, available at https://shearwatergroup.com/digital-resilience-whitepaper/

Webster, F. (2006). *Theories Of The Information Society* (1st ed.). Routledge.