The digital transformation “new normal”

Alfredo M. Ronchi
Politecnico di Milano
alfredo.ronchi@polimi.it

Abstract

The paper provides an overview on the "new normal" or "near future society" starting from the most significant events that characterised the evolution and pervasiveness of cyber technology. The impact on security and privacy due to the acceleration of the digital transition during the pandemic and the decision makers wills to go digital sometimes forgetting some wise principles. The goal is to digitise as much as possible reaching a cyber-based society relaying on “digital”, this pillar is quite fragile and subject to attacks or suitable for top-down discrimination. Additional potential drawbacks concerning loneliness due to lives spent in cyber-bubbles, cyber-mediation of human relations, mainstream influence on opinion dynamics and nudging, these are some of the additional aspects considered. Of course, this set of aspects do not cover the full range of impacts that may characterise the new normal but provides some relevant examples.

Preamble

To have a clear vision of the "new reality" and its trend, it is necessary to consider the technological evolution together with some relevant events and the impacts that these aspects have had and will have on society, then carrying out a "future back casting" exercise.

Recently, some messages strengthened their impact on society as a mix of incumbent tragedies and an ongoing full reshaping of society, a kind of imminent “new global order”. On the one hand the global warming, climate change, the ozone hole, lack of food and water, the pandemic crisis and more have had a profound impact on society, generating a widespread feeling of risk for the survival of humanity. The “cancel culture” movement, and the negative impact of man on nature are pushing the most radical thinkers of the 20th-century to stop facing the prospect of the actual extinction of Homo Sapiens. This perspective, as the endpoint of the Anthropocene the faith of anti-humanism, begins not with a political program but with a philosophical idea. The flip side, Transhumanism glorifies some of the same things that anti-humanism decries—scientific and technological progress, the supremacy of reason. Some transhumanists believe that genetic engineering and nanotechnology will allow us to alter our brains and bodies so profoundly that we will escape human limitations such as mortality and confinement to a physical body. Others are adamant that general artificial intelligence design will improve itself to think faster and deeper, then the improved version would improve itself, and so on, exponentially. Both trunks of thoughts basically consider humans’ disappearance, on one side extinction on the other cyborg.

There are some key events that have characterised the recent period, one of these is the so-called digital transformation considered the natural evolution of the current society in the light of a pervasive technology like digital technology.

Digital technology is intertwined with almost all the life sectors. Since the dawn of digital technology, the number of application and solutions based on such technology had a surprising rate of growth. Transistors, originally conceived to fight against deafness, were the sparkling light of several new devices, followed by integrated circuits. Computers became ten times smaller and powerful being ten times cheaper. Nowadays there is no field of human knowledge that doesn’t take advantage or is based on digital: communication, education, government, health, energy, mobility, etc.

The full settlement of such pervasive technology is termed digital transformation (DT or DX), governments, international organisation, private companies are all together promoting and facilitating

this switch from analog to digital. We are increasing leaving the analog, face to face, paper-based world to enter the intangible digital mediated one. Many years ago, in the 1980s, it was held multidisciplinary panel to discuss about the ontological aspects of digital to approach this sector properly. The outcomes were that digital objects represent a completely new class of objects they enable the opportunity to be here and there, clones perfectly equal to originals, shared among an illimited number of owners, "immortal" in theory and more. It is all gold what it glitters?

The turning point

In the 1980s the increasing diffusion of mobile phones and in the middle of the 1990s the advent of the World Wide Web disclosing to citizens the existence of the cyber dimension can be considered the key tuning point of the digital revolution sealing the merge of telecommunication and information technology. The Microsoft motto "Where do you want to go today?" represents the open gate to the cyber world. Personal computers left the desktop of students and moved to the living rooms for the benefit of the whole family. Last significant tile of this process was the diffusion of smart phones and tablets, location aware and always on-line.
Since more than two decades we are wrapped in our personal cyber-sphere in a kind of symbiotic relation. Citizens experience the world thanks to a cyber device mediated approach; the "new reality" is the one delivered by devices. Internet and Web technology gave to citizens the opportunity to reach multitude of people before reachable only by radio and television, this "one to many" or "many to many" exchanges of ideas opened a completely new scenario both in positive and negative sense.
Social media completed the transition toward a completely new way of human relations.

Cyber Tech Pervasiveness

The increasing role of cyber technology and key services in our everyday life increases, at the same time and even more, the vulnerability and risk of cyber-attacks. We already faced several cyber infrastructure malfunctions and relevant attacks due to hackers, some targeting Governmental or Law Enforcement Agencies and Institutions, some targeting critical infrastructures, others targeting big companies. Financial markets may be influenced or tilted by cyber-attacks. Smart cities and grid models must carefully consider cyber security issues; we don't appreciate the "rebellion" of elevators or the unwanted locking of all the entrance doors of our company headquarters. As much as we install IoT and other cyber devices and services as much the risk to be cyber-attacked increases. This mainly because such devices were and are many times not designed to be "secure".
What about industrial machinery today fully computerised, or critical infrastructure management; in a cyber warfare scenario it might be enough to dispatch on the network a code name like "1024 millibar" to collapse the whole target infrastructure[1]. Recently on the World Economic Forum it has been foreseen the possibility a global cyber-attack that will take us back to the stone age.
Today even cars may be subject to cyber-attacks as it was already demonstrated[2] in the United States; if on one side the regular car service or recall for update can be performed through the permanent car connection to the Internet, no more requiring to physically take the car to be serviced, on the other side, in case of cyber-attacks, our car might behave in an unpredictable way.
This to do not mention aircrafts, ships, trains, metro, and any other transportation means, the PLCs[3] and more in general software programs are easily hacked, this even because they were designed in and for a hacking free environment mainly not connected online. Industrial cyber security experts find themselves facing, in addition to the direct threats of cybercrime, also difficult situations in which obsolete technologies cannot be updated or implemented with security systems. Sometimes industrial automation solutions left some PLC "open" to ensure the opportunity to activate remote maintenance.

1 This to do not mention Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwer gwea.com

2 This was a demonstration to outline the potential threats due to pervasive use of digital technology in the automotive sector.

3 Allison D. at al. ( ) PLC-based cyber-attack detection: a last line of defence, https://conferences.iaea.org/event/181/contributions/15513/attachments/9194/12424/CN278_PLC-based-Detection.pdf IAEA as part of the CRP J02008 on Enhancing Computer Security Incident Analysis at Nuclear Facilities

We all remember some examples of cyberattacks to lock machineries or energy pipelines. We are surrounded by "critical infrastructures" managed by cyber components that, in case of attacks, may create mayor or minor impact on our daily life. We don't mean only typical critical infrastructures like communication, energy, water, health, transportation, and last but not less important nowadays financial services; we consider information services, social media, geo-positioning, home automation, smart cities, safety, and security devices, and more. It will not surprise if in few years big service platforms will be considered critical infrastructures[4]. In addition, there is a clear need to reconsider supply chains and their resilience. As a first impression the whole cyber environment including CCTV, IoT, tracking tools will ease everyday life and improve security but on the other side the alleged total dependence from the cyber domain represents a significant weakness blending with the widespread lack of digital literacy and cybersecurity awareness among citizens. We will consider other potential drawbacks later, this time not due to hackers but to top-down implementation of reduction or cancellation of access to services and rights.

Digital Transition and Security

The actual trend is to transfer to the digital domain as much as possible any "traditional" process and document, so in a glimpse government procedures and citizens documents and data will flow in the format of bit streams, sometimes, under the pressure of critical events, this process wasn't designed to ensure security. As an example, the impact of Digital Transition on cybersecurity due to the boost caused by the pandemic and the increasing number of "digitally divided" citizens forced to "go digital" generated the need to foster a diffuse culture of cybersecurity since the primary schools. Consequently, the more we become digitalised, the more we are vulnerable to hackers and hybrid threats. Of course, the overall scenario includes many other aspects and "shades".

We usually consider "security" as a seamless part of our life, apparently something cost-free, no need to invest or care about it. This seems to be true till we face minor or big problems. Pickpockets take our wallet, thief stole our car or take some of the goods we have at home, hackers kidnap our data or any other event that infringe our "convincement" of "feeling safe[5]". Therefore, we start to be concerned about security, it is no more a cost-free "commodity", we need to invest some resources to reach a certain level of "insecurity".

Security is tightly related to different parameters: the asset or assets to be secured, the specific context, the range of potential threats, and more. As the general concept of security evolved through time even the concept of national security evolved as well as homeland security and, the same happened in case of potential targets and threats. State actors face a very complicated scenario trying to match with the current and future developments of threats based on intelligence, information flow analytics[6], risk assessment, probability[7], and projections. Many times, in this complex and risky scenario, the best or less harmful solution is to refer to the game theory and how to maximise the gain minimizing risks, that doesn't mean to choose the maximum absolute gain. This may led to choices motivated by contradicting goals.

Cyber Tech Resilience

Resilience, a keyword recently discovered by governments and media, extended its original meaning from the structural sector to any sector including education. Therefore, literature is extremely wide even if, in our field, one of the key sectors is critical infrastructure resilience or cyber disasters resilience[8] On the pandemic cyber technology offered a valuable contribution to ensure "business" continuity; government services, justice, health sector, culture, education not forgetting supply chains

4 The one we know as GAFAM (Google, Amazon, FaceBook/Meta, Apple, Microsoft) and NATU (Netflix, Tesla, Airbnb, Uber)

5 We did different studies together with our partners from behavioural psychology including tests based on VR simulation of different environments recalling increasing level of insecurity.

6 E.g. Ronchi Alfredo M., (2018),, TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

7 Risk assessment and probability cover even natural risks scenarios that can impact security (e.g. critical infrastructure).

8 Ronchi Alfredo M., 2021, Cyber Resilience, Cyber Disaster Management: The Way Forward, Cyberlaws, Cybercrime, Cybersecurity, ICCC, New Delhi, volume Cyberlaws, Cybercrime, Cybersecurity, New Delhi, India

and more, they all switched to online procedures. It is true that probably our present and future after the pandemic is and will be different mainly due to the progresses in digital transition and the outcomes of the experience on smart working and video conferencing: less travels, less need to provide offices, and more. Governments are planning to transfer, or complete the transfer of, key documents and certificates in digital format thanks to QR codes or digital wallets installed on smart phones collecting documents (ID, Social Security, Medical Folder, Driving licence, Bank Account, ID Pay, etc.), and certifications (vote certificate, vaccinations, etc). The increasing number of different passwords we learned to manage every fifteen days is now almost obsolete, bio metric is gaining more and more relevance in the sector of secure identification, from fingerprints to eye and, more recently, face, even if early face recognition systems tested on the field shown some weaknesses. All the rest of our personal data are already stored somewhere in our country or abroad thanks to our "buddies" like our smart phone or smart watch. The survived "almost" traditional documents will be soon enforced by cross validation thanks to our digital ID[9].

In the "analogue" world we had different pipelines and "channels" to perform, thanks to different tools and means, our activities, in the cyber world the whole activity depends on a single "bottleneck": cyber technology. Therefore, even if we use cyber-ranges and simulations of any potential cyber-attack there are always new threats due to the creativity of "cyber warriors".

There is a strong need to identify back-up solutions and procedures, some countries kept a paper-based version of key documents in bunkers, other usually create a parallel independent recovery network "sealed" in secure locations or segmented in different domains. It is not by chance that one of the first tasks of The World Bank on risky scenarios is to back up national archives and key documentation[10]. Nowadays the key concept is "holistic security", a "global" approach to security integrating all the different aspects and problems. There is a diffuse need to foster a "culture of cyber-security" starting from kids disseminating sensitive information online to improve their Facebook or Instagram profiles or to download latest games on their smartphones of tablets. Apps are asking the permission to access our address book, phone, camera, mike and more, they basically take almost full control of what we consider our vault hosting business information, bank account, digital identity, etc. The increasing diffusion of cyber devices offers an extended attack surface that requires a similar dissemination of awareness and knowledge.

Impact on Society

We said "it is not all gold what it glitters" so let's consider some potential drawbacks we are still facing, or we will face soon. Digital technology in general had and still have a strong impact on society and the pandemic accelerated and amplified such impact especially on young generations. Leveraging on laziness and relaxation citizens spend less time outside home, they have shopping online, they buy food and drinks directly delivered on their table, "meet" friends on Zoom or WhatsApp, interact with the "outer environment" though the mediation of social media and video clips. These aspects are even more evident in young generations that add to the social media the gaming dimension. Of course, such trends are even amplified by other media such as television and news. Cultural enjoyment is nowadays often mediated by cyber technology, so we enjoy concerts, operas, libraries, museums, and galleries thanks to their digital proxies. This is probably good to ensure continuity in case of troubles but will never surrogate the pleasure to enter a library and smell the scent of books and wooden bookshelves or invest some quality time sitting on a bench in front to a Renoir.

9 E.g. Horizon Europe call CL3-2022-BM-01-02 "Enhanced security of, and combating the frauds on, identity management and identity and travel documents"

10 Source: The World Bank archive

Metaverse and parallel universes

The concept of Metaverse probably dates back in the 1990s when Bruce Damer[11] introduced the Digigardener the Avatar of a gardener remote controlled by humans, more recently the movie Avatar[12] outlined this idea to create digital "proxies" operating in a cyber universe.
In the nineties Interactive Virtual Reality already embraced the "Metaverse" sometimes even more advanced than todays' approach; the key limitations at that time were due to technology and the lack of big key players investing relevant resources to make the "Metaverse" dream come true.
Metaverse and virtual reality are inter-twined, but they are not the same. The metaverse is a platform that is still under development and its final form is unclear, it could improve or even replace the Internet, while virtual reality is a known technology that allows you to live and experience virtual worlds. The Metaverse today offers a simplified representation of the "reality" as conceived by programmers, of course many times very astonishing, it is accessible thanks to personal computers, tablets and smart phones via virtual reality and even enhanced reality. One of the technologies often merging with metaverse is NFT (Non-Fungible Tokens) the blockchain based shared "property" of digital "objects" as it is foreseen for Web 3.0. If, as its sponsors hope, the metaverse will succeed, we will face parallel universes with rules and citizens …. recreating typical issues of societies. Some thirty years ago, we remember Habbo Hotel social game, players stored assets as in a kind of digital Monopoly game, even in this scenario thief used to act stealing virtual furniture and cloths. So, in case this new universe will become a relevant "reality" we must start thinking the extension of the existent laws or new cyberlaws. We already faced and still face relevant problems due to the need to extend or set new rules to properly manage the digital domain.
Long time ago, in the cyber time scale, virtual reality was considered the way to escape from physical reality and create its twin, several other technologies from videogames to shared universes and platforms like Second Life offered something similar. Sometimes these technologies were even applied to cultural heritage as it happened in the case of the Forbidden City by IBM. Products in between digital movies and videogames offered the opportunity to play some action movie scenes and save the video clip as a shoot of a real movie, reality blurring the border with virtuality.
There is an increasing interest in promoting the metaverse as a kind of "new frontier" a territory potentially rich of opportunities for the forerunners / settlers. Key players are putting their flags on this territory in a kind of gold rush. Not only software players but even hardware companies are investing in this new opportunity and the range of involved firms is not limited to traditional cyber hardware producers. More than twenty-five years ago Zeiss developed an enhanced reality platform supporting car services, world class sunglasses companies like Ray Ban are entering this market starting with intelligent glasses taking pictures reacting to voice commands and more. Recent evolution of Oculus HMD offers immersive experiences to video-gamers or added value services to tour operators and real estate companies.

Immersivity

All these technologies promise immersivity in the cyber world, what does it mean immersivity? We need to specify the meaning of "immersion", does it mean "emotionally involved", "blurring reality with virtuality"? There are different experiences that can be labelled "immersive", reading a book, watching a movie, attending a concert or opera, experiencing wild nature, spiritual experiences and more. The ability to feel "immersed" differs from person to person some people are unable to feel immersed even if they experience the most immersive situation, they keep the two environments separated.

[11] Avatars: Exploring and Building Virtual Worlds on the Internet https://www.digitalspace.com/avatars/book/
[12] 2009 American epic science fiction film directed, written, produced, and co-edited by James Cameron

Purchasing and living in the Metaverse

Virtual goods can be created, purchased, and owned, the foreseen evolution of the Metaverse in the field of commerce requires the clear identification of the counterparts both the human and the machine this even in case of machine-to-machine transactions, so it is needed to assign a digital identity not only to the humans, as it is already done, but even to machines, software modules and avatars. On the side of the cybershop the system must identify the customer thanks to his/her digital ID checking the picture with the capture image of the face of the customer, this check must be iterated through time during the session to ensure that the buyer is still the same person. This hard real time task if usually in charge to an AI module connected with a computer vision module extracting the features from the video image of the customer and comparing it with the one on the digital ID. This need to certify the identity of the counterpart is of course needed in different services including government, health and more.

Some "historical" application of IVR recreated relaxing scenarios like remote tropical islands very similar to the touristic cyber-locations proposed by another science fiction movie Total Recall[13], will the future development of Metaverse offer relaxing vacations in such cyber environments? This is a short description of the potential applications of Metaverse but let's consider even the potential impact and, why not, drawbacks.

Meta-drawbacks

Accordingly with the actual perspective the Metaverse will progressively create a clone of our environment, but it will not be limited to this goal, creativity will extend this universe without limits apart from imagination. Cyber-loneliness, one of the foreseeable risks is a kind of addiction to this "parallel life" training users to shift from real to Meta-life blurring the border between them, this may happen as much as the number of services and duties will be transferred on the other side of the Alice's mirror. Meta-life can propose a new normal that once accepted in the Meta-life might be accepted in the real life. The same of course is valid for information and opinion dynamics, especially if perceived as real and trustable.

The challenges for the upcoming years are the ways to sustain the human's role and the inviolable right to freedom and personal privacy in an era of unlimited information gathering. Once again, the need to find a proper balance between humanities and technologies is omnipresent. Social sciences and humanities must establish a tight cooperation in designing or co-creation of cyber technologies always keeping humans in the focus.

Impact on opinion dynamics in social networks

We already mention the incredible power of digital information sharing and social media. Opinion formation is a complex and dynamic process mediated by interactions among individuals in social networks, both offline and online. Social media have drastically changed the way opinion dynamics evolve, in any case, they provide a reservoir of data for the study of opinion dynamics on social networks. Social media have become a battlefield on which opinions are, often violently, exchanged. In turn the behaviour of social media has become an important early indicator of societal change. In the "new reality" there is a concrete and present risk to manipulate opinions thanks to digital media as well as to impact the decision-making process. The extensive use of Artificial Intelligence, Machine Learning and Big Data, apart from several ethical issues, can led to some relevant drawbacks. As an example, let's consider "nudging". The concept of nudge is already used in digital systems even if the nature of the mechanisms that characterise it is not always consistent, and some uses overflow into practices already prohibited by current legislation. In fact, the use of even "slight" and often morally irrelevant manipulations of the architecture of the decision is constrained both in the use of personal data to be able to construct a nudge mechanism[14] and if the desired result falls

[13] 1990 American science fiction action film directed by Paul Verhoeven

[14] by the GDPR

within the category of fraudulent transactions[15]. The progress of AI has made it possible to develop much more powerful nudge mechanisms thanks to the effectiveness of statistical and inferential AI systems. The impact of AI powered technology on human autonomy is huge. AI-enhanced nudges reinforce the ability to achieve the designer goals using cognitive biases, emotional impulses, and other human behavioural mechanisms both intentionally and unintentionally.

New Normal

This is not a complete overview on the key aspects and trends that appeared in recent times, off course taking into consideration each single technology and trend there are not specific concerns and technology seems simply to ease our daily life but getting much more in depth of each single innovation or putting together all the visible "tiles" of the "new normal" mosaic we can be concerned. If on one side the whole architecture is based on cyber tech, with all the potential risks it implies, on the other side cyber-world rules have can express a power that no one of the "rules" in history had, information and big data are the assets to be analysed, influenced, reused. Some authors call them "the new oil" but this type of "oil" can be used, abused, and misused many times. The science fiction "Ingsoc[16]" or "Cyberdyne[17]" now rule thanks to "algorithms" and "neural networks".

In conclusion, don't you feel framed by such an "intelligent" environment? Social and communication media complete the panorama adding a "private depth" to the general fresco, ad-hoc defined tweets or posts may collect and analyse users' feedbacks to guide or anticipate citizens' actions and feelings. In recent times crowd data collection, open data, and big data, more or less anonymised, have provided the big framework to collect all the different tiles. Online malls and delivery platforms offer, in addition, to analysing your browsing, the opportunity to save a "wish list" to better focus on the market trends. So, again don't you feel framed?

References

[1.] Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015

[2.] Bohn Roger E., Short James E. (2009), How Much Information? 2009, Global Information

[3.] Industry Center University of California, San Diego

[4.] Conditi Fabio (2023), Immaginare un futuro eutopico, Scenari Economici, 7 January 2023

[5.] Freccero Carlo (2022), Le élite sono il nuovo Mago di Oz, Europa, December 2022

[6.] Kirsch Adam (2022), The People Cheering for Humanity's End: A disparate group of thinkers says we should welcome our demise, The Atlantic, December 2022

[7.] Kurzweil Ray (2005), Singularity Is Near: when human transcend biology, ISBN 0-670-03384-7, Penguin Book

[8.] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13:

[9.] 978-0691138619, Princeton University Press 2009

[10.] Prensky Marc (2001), Digital Natives, Digital Immigrants, Part II: Do They Really Think

[11.] Differently? On the Horizon (NCB University Press, Vo 6, December 2001)

[12.] Riva Giuseppe et al. (2022), Mitigating negative emotions through virtual reality and embodiment, DOI https://www.frontiersin.org/articles/10.3389/fnhum.2022.916227/full Frontiers in human neuroscience

[13.] Riva Giuseppe et al. (2022), Humane Robotics. A multidisciplinary approach towards the development of humane-centered technologies, ISBN 9788834346181, Vita e Pensiero, Univ. Cattolica

[14.] Ronchi Alfredo M., The fourth screen, proceedings Global Forum 2010

[15] UCPD - Unfair commercial practices directive https://ec.europa.eu/info/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en

[16] George Orwell - 1984 big brother

[17] James Cameron's ruling organisation in Terminator

[15.] Ronchi Alfredo M. (2016), 1984 won't be like "1984"?, UNESCO IFAP Conference "Tangible and Intangible Impact of Information and Communication in the Digital Age, ISBN *978-5-91515-068-9, UNESCO IFAP, Moscow*
[16.] Ronchi Alfredo M. (2020), Hybrid threats: defence line from the grassroots, JDST vol. 3, no. 5, p84-p99, 2020
[17.] Ronchi Alfredo M. (2021), Rethinking the role of ICTs: Digital transformation and Culture enjoyment continuity, ISBN *978-0-9998551-5-7,* State Hermitage Museum - St. Petersburg State University
[18.] Ronchi Alfredo M. (2021), From Ingsoc to Skynet it is not only science fiction: From novels and science fiction to quasi-reality, ISBN *978-92-9189-075-0,* UNESCO IFAP, *Moscow*
[19.] Ronchi Alfredo M. (2022), Human factors, resilience, and cyber/hybrid threats, 53/2022 Information & Security
[20.] Surowiecki James (2004), The Wisdom of Crowds: Why the Many Are Smarter than the Few ISBN 978-0-385-50386-0, Doubleday; Anchor
[21.] Weiser Mark D. (1999), The Computer for the 21st Century, Scientific American Ubicomp Paper after Sci Am editing, 09-91sci Amer Weiser