[Scientific Articles]

Ronchi A. M.
Is It All Gold That Glitters? The "New Normal"

IS IT ALL GOLD THAT GLITTERS? THE "NEW NORMAL"

Ronchi A. M.

Professor at Politecnico di Milano, Secretary at EC MEDICI Framework Foundation

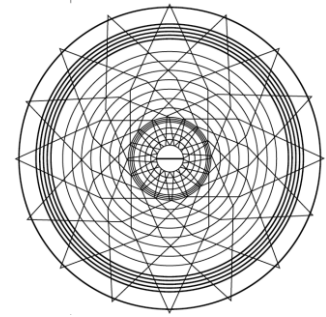(Milan, Italy)

alfredo.ronchi@polimi.it

Abstract:

Within the general framework of "Internet for social good" the paper offers an insight into the potential impacts and drawbacks in lieu of the ongoing digital transformation. It analyses some of the key facts and events that characterised the recent past and contributed to identifying the digital transition as the natural evolution of our society. It looks at cyber technology from the humanities side, considering the mid- and long-term impact on society. Our "world" is being reshaped by cyber technology, government procedures, production and supply chains, general services and more as they all are based on cyber technology and platforms. Platforms are mainly private, and the key ones are concentrated in a few countries creating a kind of oligarchy. The "control buttons" of our daily lives are often outside the control of our nation-state. Many a time, the double nature of "cyber", though contributes to improving resilience, because of its pervasive nature, it can be the target for attacks. In the "analog" world we had different "channels" to perform our activities. In the cyber world the whole "system" depends on cyber technology. This represents a significant risk, both in case of malfunction or hackers' attack and, in case of a top-down decision, to switch off. A plan B in such a situation will require a long time to be implemented. Social media and global content providers are "training" young generations by offering a "unified global" approach. This will impact future generations and their cultural identity. The recent pandemic boosted the digital transition. An increasing number of "digitally divided" citizens are forced to "go digital". This generated a significant impact on cybersecurity. We are surrounded by "critical infrastructures" managed by cyber components that, in case of attacks, may create major or minor impacts on our daily lives. On the social side, we are wrapped in our cyber-sphere in a kind of symbiotic relationship. Citizens experience the world, thanks to a cyber device-mediated approach. The "new reality" is the one delivered by devices. The 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. The "new normal", is this what we aim for?

Keywords: Internet for social good, digital transformation, cyber technology, platforms, cybersecurity, digital transition, critical infrastructure

Introduction

It is a common understanding that we are now facing the fourth industrial revolution, the first in the middle of the 18th century enabled the mechanization of activities, thanks to steam energy; the second added electric energy to this scenario; the third was activated by computers and the large amount of data generated; and the fourth is based on a portfolio of enabling technologies ranging between cyber, nano and bio.
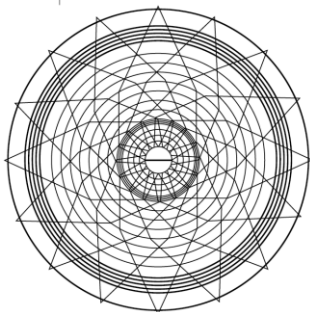
Internet for social good, in short, we can interpret it as "web technology for social good". These two terms can be used as synonyms. This technology flourished in the consumer and home markets in 1995, thanks to Microsoft's motto "Where do you want to go today?" outlining the idea of a small world entirely connected online. Personal computers since that time moved from the sleeping room of nerds to the living room and kitchen as household appliances. The extended use of computers overlapped any activity generating an impact on society. Let's underline that innovation per se without any positive impact on society is useless.

Digital transformation and other trends

For a couple of decades, we witnessed an improving role of digital procedures and tools reshaping the activities to evolve in the so-called digital transition or probably more meaningful "digital transformation".

"Transformation" gives a better understanding of the outcome as society is deeply impacted by this process. The economic model pursued in the recent past shows its limits as globalisation has its side effects. Nowadays more often we consider de-globalisation as a scenario and the re-discovery of local "values" and "identities". We do not like anymore the same sandwich or merchandise all over the world.

Therefore, in the Western world, that recently discovered to be the absolute minority on the planet Earth, there is an evident lack of values and beliefs, a clear feeling that there is something "wrong", so, in such an uncertain environment without clear references, young generations are discovering new "gurus" and trends. Such as the "cancel culture" movement together with the "politically correct" re-evaluation of history and facts in the light of today's trends and thoughts. The negative impact of man on nature considered the origin of main disasters is generating a widespread feeling of risk for the survival of humanity. Global warming, the Antarctic ozone hole, increasing levels of oceans, lack of food and water and last but not least the pandemic or pandemics, sometimes interpreted as the self-defence reaction of nature. All these aspects impacted society as a mix of incumbent tragedies and an ongoing full reshaping of society, a kind of imminent "new global order".

We face the contraposition of Anti-humanism vs. Transhumanism, the end of Anthropocene, General artificial intelligence will improve itself to think faster and deeper, then the improved version will improve itself. Then the improved version will improve itself. Are we going to face what happened in the science fiction movie 2001: A Space Odyssey due to HAL[1]? Both trunks of thoughts consider humans' disappearance and extinction, on one side, and cyborgs, on the other.

This feeling pushed society to look for a "new normal" based on the mitigation of climate change, circular and green economy, and more. The omnipresent digital technology was considered one of the building blocks of this "new normal", even thanks to the relevant contribution that this technology provided to one of the recent crises: the pandemic. Hence, the vector of this change was associated with the so-called Digital Transition or Digital transformation (DT or DX).

As Klaus Schwab wrote in the preface of his book "Shaping the Fourth Industrial Revolution", in 2016 (Schwab, 2016):

> *The world is at a crossroads. The social and political systems that have lifted millions out of poverty and shaped our national and global policies for half a century are failing us. The economic benefits of human ingenuity and effort are becoming more concentrated, inequality is rising, and the negative externalities of our integrated global economy are harming the natural environment and vulnerable populations the stakeholders least able to absorb the cost of progress.*

Furthermore, more recently we started to discuss the Global Digital Compact. This was one of the key topics on the WSIS Forum 2023 together with AI tools and their developments. "The Global Digital Compact that would set out principles, objectives and actions for advancing an open, free, secure and human-centred digital future, one that is anchored in universal human rights and that enables the attainment of the Sustainable Development Goals." The debate aims to shape a shared vision of digital cooperation by providing an inclusive global framework for a sustainable digital future. We hope that the outcome of this debate will fully represent what is expressed in the statement above.

"The road ahead[2]"

The incredibly rapid success of the World Wide Web gave a boost to the globalisation trend, a shift toward uniformity, jeopardising diversities, and cultural identities. Starting from the first decade of the twenty-first century, several Governmental Agencies,
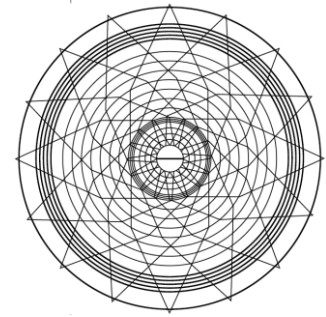
---

[1] The spaceship officer Dr. Dave Bowman used to interact with HAL by voice calling "Hello, HAL. Do you read me, HAL?"—HAL: "Affirmative, Dave. I read you.", Dr. Dave Bowman: "Open the pod bay doors, HAL", HAL: "I'm sorry, Dave. I'm afraid I can't do that" . . . We all know what happened later.
[2] Let's recall the title of book written by Bill Gates: Gates, B. (1995). The road ahead. Viking Penguin.

Institutions and Private Enterprises from all over the world, both in industrialised and developing countries, invested time and resources in e-services (Ronchi, 2019). The key element of this success was the cyber element called "platform", the main component of any kind of service or information delivery. Platforms are mainly "populated" by users, even if they do not pay any fee, considered as customers[3]. A relevant part of digital transformation relies on platforms and standards (Ronchi, 2020).

This development has profoundly affected society. Citizens are increasingly using platforms to buy and sell goods online, and book trips and holidays. They also now enjoy social media and several other services, unthinkable before the Internet, from extremely vertical services to crowd services (Surowiecki, 2004) or funding. Platforms were the real "silver bullet" that created major opportunities and a real impact on society and the economy. Following the schema of some previous revolutions, the idea was: that digital technology is disruptive cancelling several businesses, but new businesses will be created. The key point is that the specific nature of digital technology is creating fewer jobs than the ones eliminated. The visible effect now is an increasing number of workless people replaced by software and robots. In some fields, the transition is carried out by adding some digital intelligence to optimize workers' activity to evolve later to fully robotized systems. In addition, today digital tools are blurring the boundary between personal and professional lives. This effect is often termed "time porosity" or "spillover".

The platforms sector can be considered a kind of monopoly not yet regulated - a kind of grey zone. So, in the digital transition, despite antitrust laws, there is a potential risk of falling under the control of a few key players. The concentration of such players in a few countries and their private nature may cause serious troubles in case of unavailability of platform access, both due to malfunctions and top-down decisions. This means being unable to feed our supply chain with some goods once provided only by these platforms. A plan B in such a situation will require a long time to be implemented.
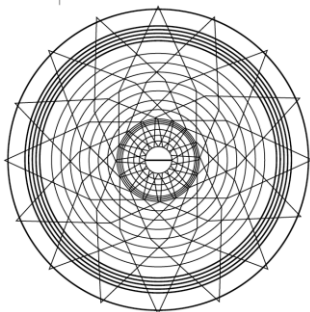
As an example, Google has a share of around 85.53 percent of the global search engine market and advertising. Meta stated that 3.81 billion people were using at least one of the company's core products (Facebook[4], WhatsApp, Instagram[5], or Messenger). Amazon holds 37.8 per cent of the market share[6]. Shall we call it "oligarchy"? A relevant

---

[3] They, as "customers", increase the market value of the platform in the media market because of the advertisements and the ability to analyse data and resell customers' profiles.

[4] The activity of the social media is recognized as extremist and prohibited on the territory of the Russian Federation, the data here and further are used for research purposes and are not aimed at approving extremist activities.

[5] The activity of the social media is recognized as extremist and prohibited on the territory of the Russian Federation, the data here and further are used for research purposes and are not aimed at approving extremist activities.

[6] Source of data: http://www.statista.com

side effect of such monopoly will impact actual and future generations that will grow up fed by the same "culture" inoculated via social media, entertainment, general content, and online delivery of goods.

Cyber Tech Pervasiveness and Security

Nowadays digital technology is intertwined with almost all life sectors. Since its dawn, the number of applications and solutions based on such technology had a surprising rate of growth and at the same time, or even more, the vulnerability and risk of cyber-attacks and hybrid threats have increased. Currently, no field of human knowledge takes advantage of or is based on digital: communication, education, government, health, energy, mobility, etc. We are increasingly leaving the analog, face-to-face, paper-based world to enter the intangible digitally mediated one.

The impact of data transfer 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 right from the primary schools.

We usually consider "security" as a seamless part of our life, apparently something cost-free, with no need to invest or care about it. This seems to be true till we face minor or big problems. Pickpockets take our wallet, thieves steal our car or take some of the goods we have at home, and hackers hijack our data or any other event that infringe our "convincement" of "feeling safe[7]". Therefore, we started to be concerned about security. It is no more a cost-free "commodity». We need to invest some resources to overcome a certain level of "insecurity"[8]. The concept of "security" is not an absolute and permanent status, but we can identify it as a "dynamic balance" between a specific "asset" or "assets" to be secured, the specific context, sometimes for a specific period, and the range of potential threats, and more. We focus on the double nature of "cyber", many times it contributes to improving resilience. Because of its pervasive attitude, it can be the target for attacks and generate the "perfect storm".

What about industrial machinery or critical infrastructure management that is today fully computerised in a cyber warfare scenario (Ronchi, 2018)? Recently the World Economic Forum 2023, remembering the millennium bug, WannaCry and Petya, has foreseen the possibility of a global cyber-attack that will take us back to the stone age.

Cyber Tech Resilience and Digital Fragility

Resilience is a keyword recently discovered by governments and media. One of the key sectors of resilience is critical infrastructure resilience or cyber disaster resilience.

---

[7] 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.
[8] Quoting Salman Rushdie an Indian-born British writer recently suffered an attempt to kill him in NYC.

[Scientific Articles]

Ronchi A. M.
Is It All Gold That Glitters? The "New Normal"
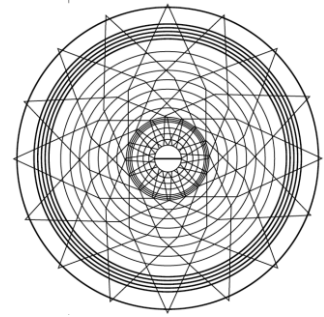
During the pandemic cyber technology offered a valuable contribution to ensure "business" continuity; government services, justice, health sector, culture, education, not forgetting supply chains and more, they all switched to online procedures. Governments are planning to transfer or complete the transfer of key documents and certificates in digital format thanks to QR codes or digital wallets installed on smartphones collecting documents (ID, Social Security, Medical Folder, Driving licence, Bank Account, ID Pay, etc.), and certifications (vote certificate, vaccinations, etc).

All the rest of our data is already stored somewhere in our country or abroad, thanks to our "buddies" like our smartphone or smartwatch. The "almost" traditional documents that survived DT will be soon enforced by cross-validation, thanks to our digital ID.

In the "analog" world we had different "channels" to perform, thanks to different tools and means, our activities, in the cyber world the whole "system" depends on a single "bottleneck": cyber technology. This dependence represents a significant weakness blending with the widespread lack of digital literacy and cybersecurity awareness among citizens. If this pillar fails due to malfunctions or is switched off, our life will suffer sometimes unpredictable problems: no cyber and, consequently, physical identity, no bank account and social security, no service delivery, no news, and connection with other "entities".

We are surrounded by "critical infrastructures" managed by cyber components that, in case of attacks, may create a major or minor impact on our daily lives. We don't mean only typical critical infrastructures like communication, energy, water, health, and transportation, but also important are financial services, information services, social media, geo-positioning, home automation, safety, security devices, smart cities, and more. It will not be a surprise if in a few years big service platforms like Amazon, Deliveroo, etc., will be considered critical infrastructures. In addition, there is a clear need to reconsider supply chains and their resilience.

There is a diffuse need to foster a "culture of cyber-security" starting from kids disseminating sensitive information online to improve their Facebook, Instagram or TikTok profiles or to download the latest games on their smartphones or tablets. Apps are asking the permission to access our address book, phone, camera, mike and more, they 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. In addition, the Internet, blockchains, and the quick deployment of number crunching applications are emphasizing energy consumption. At the same time, the rapid pace of innovation in the field of consumer devices produces a significant amount of waste to be recycled or disposed of. Consequently, can cyber technology be considered green and resilient?
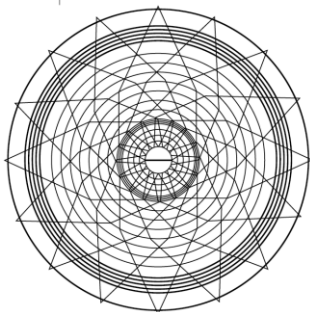
General aspects, ethics, human rights, and potential drawbacks

Considering the ontology point of view Cyber Technology is a new entity, a new class of objects. In the last decade, philosophers and humanists started to professionally deal with computer scientists and innovators (Stuckelberger, 2018). These scholars usually considered the medium and long-term impacts of technologies on society. The emerging technological trend in autonomous vehicles, robots, machine learning and artificial intelligence may pose significant ethical problems to innovation.

In addition, we observe the massive decrease in the level of critical thinking and the emergence of waves of information epidemics, both at the national and global levels (mainstream communication, limited contraposition, censorship, and fake news). Post-truth, in its heyday, with public perception, shaped more through addressing feelings and predetermined opinions, rather than facts, with fakes, click baits, hypes and other tools introduced to form post-reality in the political and media culture (Makkuni, 2018). Post-reality is changing the system of values with the "new normal" (semantic shifts, etc.), of course, maybe politically correct. New ethics is putting personal freewill and freedom of choice under question; traditional cultural regulators of social relations and processes are being displaced by automated social algorithms (increasing role of algorithms and ML). Widespread simplified virtual mock-ups and simulacra are not only blurring the borders between the real and the digital world but also leading to a mass collection of data for managing people's behaviour (evaporation of privacy, data protection). It has also been contributing to the increasing level of conflict in both society (between individuals and groups – haters, discrimination) and among states (XXI Century warfare (Ronchi, 2018), soft concerns (Ronchi, 2021), and more (European Union, 2019).

Cyber security, and AI

The pace of innovation in the field of digital transition is pushing previously termed "digitally divided" citizens into the digital loop. They are mainly not literate in digital technology. So, they and their assets are exposed to cyber risks. Consequently, the more we become digitalised, the more we are vulnerable to hackers and hybrid threats (European Union, 2016). Of course, the overall scenario includes many other aspects and "shades" (Ronchi, 2021), (European Defence, 2017).

The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario where the malicious use of digital technologies is becoming a new business opportunity not only as a direct means to steal 'assets' and take control of smart objects but even under the format of 'cyber-crime as a service', at the same time terrorists found in cyber technology the best mean both to run their activity and to enrol new 'adepts'. (Ronchi 2022)
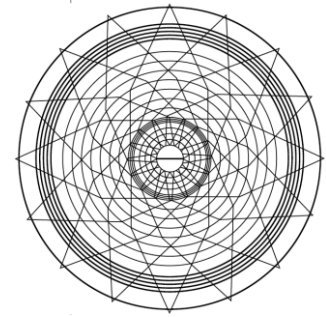
Artificial Intelligence and Machine Learning are playing a relevant role even in this sector as AI v/s AI. Some countries even devoted a specific ministry to Artificial Intelligence[9]. Let's now consider some of the potential impacts of DT on Society.

Impact on Society

Digital technologies in general had and still have a strong impact on society, especially on the young generations. Apart from the already mentioned "unified/global training" due to online media, leveraging on laziness and relaxation citizens spend less time outside the home, they shop online, buy food and drinks directly delivered to their table, "meet" friends on Zoom or WhatsApp, interact with the "outer environment" through the mediation of social media and video clips. A short and incomplete list of impacts on society[10] due to DT may include freedom of expression[11], opinion dynamics and social networks[12], decision making[13], business[14], and commerce[15].

Loneliness, Metaverse and parallel universes

For more than two decades we have been 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. Metaverse and virtual reality are intertwined, but they are not the same. Digital technology till now has mainly acted as a human isolation technology, through computer-mediated human relations or even a "loneliness relation" with your terminal, a smartphone, gaming console

---

[9] The Vice President and Prime Minister of the UAE and Ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum established the State Ministry of Artificial Intelligence and appointed as Minister Omar Sultan Al Olama. Under this Ministry United Arab Emirates are developing several initiatives to promote AI studies and expertise as "Learning Artificial intelligence" and "The National AI Strategy 2031".

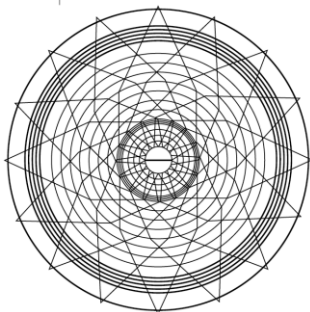[10] Refer to: (Juul, 2019), (Martins, 2009), (Peralta, 2022).

[11] A typical infringement of freedom of expression is the establishment of a "commission" in charge for the fight against fake news, the one owning the "truth", the risk in an "information society" is to cancel debates, silence alternate views and take a dangerous drift towards the "Pensée unique" or single thought in addition to the "single training".

[12] The potential role of digital media in shaping the opinions, they represent a relevant part of how we perceive reality and interpersonal relations.

[13] 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.

[14] Traditional digital technology offered the opportunity to create and test 3D models turning physical object into digital data sets the fourth industrial revolution enables the reverse from digital data sets we can print out in 3D physical objects.

[15] An outcome of the merge of big data analytics and behavioural psychology is Internet of Behaviours (IoB) (Joinson, 2004). A very rough description of the IoB is the mash-up of three disciplines: Cyber Technology, Data Analytics, and Behavioural Psychology (Emotions, choices, augmentations, and companionship) (Egger, 1996).

or laptop. It happens that friends sitting around a table at breakfast or lunch do not interact among themselves but watch their smartphones sending messages or browsing websites. It is time to develop digital technology to improve socialisation, taking citizens out of their apartments and joining the variety of agora, and public spaces in city squares, theatres, and stadiums. The Metaverse today offers a simplified representation of the "reality" as conceived by programmers.

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 to the other side of Alice's mirror. Metaverse 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.

New Normal

This is not a complete overview of the key aspects and trends that appeared in recent times in the realm of the Internet for social good. Of course, taking into consideration each single technology and trend, there are no specific concerns. Technology seems simple to ease our daily life, but by getting much more in-depth at every 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 technology, with all the potential risks it implies, on the other side cyber-world "rulers" can express a power that no one of the "rulers" in history had. Information and big data are the assets to be analysed, influenced, and reused. Some authors call them "the new oil" but this type of "oil" can be used, abused, and misused many times. As outlined in a previous document, the science fiction "Ingsoc [16][17]" or "Cyberdyne [18]" now rules thanks to "algorithms" and "neural networks[19]". The challenges for the upcoming years are the ways to sustain the human 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. In conclusion, don't you feel framed by such an "intelligent" environment? Is this the "new normal" we are aiming for? So, is it all gold that glitters?

---

[16] Recalling the George Orwell "Big Brother" (Ronchi,2022).
[17] "Ingsoc" is an acronym for "English Socialism" from Orwell, G. (1949). Nineteen Eighty-Four. Secker & Warburg.
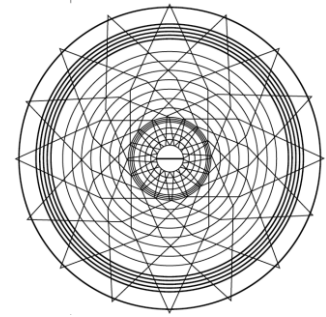[18] Recalling the science fiction movie "Terminator".
[19] Black boxes analysing big data, this process may generate unpredictable outcomes.

REFERENCES

Adam, J. (2004) Internet Behaviour and the Design of Virtual Methods, http://www.joinson.com/home/pubs/02%20Virtual%20methods021-34.pdf

Egger, O., & Rauterberg, G. W. M. (1996). Internet behaviour and addiction. Swiss Federal Institute of Technology.

EU Cyber Defence Policy Framework. (2018 update). Council of the European Union.

European Union. (2016). Joint framework on countering hybrid threats - A European Union response. https://www.eeas.europa.eu/node/46393_en

Juul, J. S., Porter, M. A. (2019). Hipsters on networks: How a minority group of individuals can lead to an anti-establishment majority. Phys. Rev. E 99, 022313. https://journals.aps.org/pre/abstract/10.1103/PhysRevE.99.022313

Makkuni, R. (2018, March 19). The Betrayal of the IT Revolution [Conference Session}. WSIS Forum, Geneva, Switzerland.

Martins, A. C. R., Pereira, C. de B., Vicente, R. (2009). An opinion dynamics model for the diffusion of innovations. Physica A 388, 3225–3232. https://doi.org/10.1016/j.physa.2009.04.007
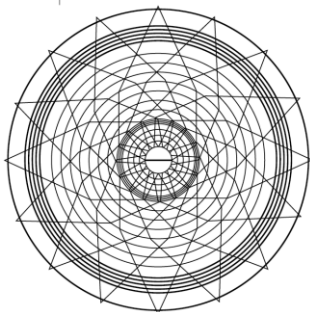
Peralta, A. F., Kertész, J., Iñiguez, G. (2022). Opinion dynamics in social networks: From models to data. Handbook of Computational Social Science.

Ronchi, A. M. (2018). 21st century cyber warfare. Information and Security: An International Journal, 39, 390x

Ronchi, A. M. (2019). e-Citizens: Toward a New Model of (Inter)active Citizenry. Springer. https://doi.org/10.1007/978-3-030-00746-1

Ronchi, A. M. (2019). e-Democracy: Toward a New Model of (Inter)active Society. Springer. https://doi.org/10.1007/978-3-030-01596-1

Ronchi, A. M. (2019). e-Services: Toward a New Model of (Inter)active Community. Springer. https://doi.org/10.1007/978-3-030-01842-9

Ronchi, A. M. (2020). Digital transformation. ICCC, New Delhi, Cyberlaw.

Ronchi, A. M. (2021). "Soft" but still concerns. In M. Aslan (Ed.). International Conference on Homeland Security: Emerging Trends, Challenging Aspects. Hasan Kalyoncu University, Turkey.

Ronchi, A. M. (2022). From Ingsoc to Skynet it is not only science fiction: From novels and science fiction to quasi-reality. UNESCO IFAP Intergovernmental Council.

Schwab, K. (2016). Shaping the Fourth Industrial Revolution. World Economic Forum.

Sector, European Parliament Legislative Train. (2019, April).

Stuckelberger, C., Duggal, P. (2018), Cyber Ethics 4.0: Serving Humanity with Values. Globethics.net. http://hdl.handle.net/20.500.12424/169317

Surowiecki, J. (2004). The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor.

Towards a More Competitive and Efficient Defence and Security. (2013). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:19020206_1
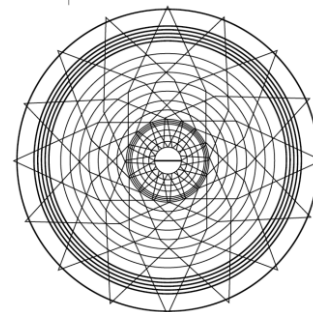
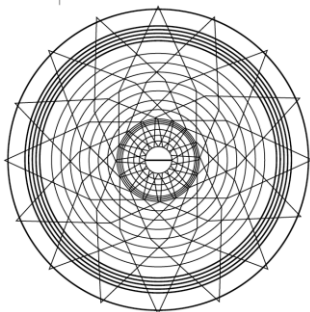# ВСЁ ЛИ ТО ЗОЛОТО ЧТО БЛЕСТИТ? РАССЖУДЕНИЯ О «НОВОЙ НОРМАЛЬНОСТИ»

Ronchi A. M.

профессор Миланского технического университета, генеральный секретарь EC MEDICI Framework Foundation (Милан, Италия)

alfredo.ronchi@polimi.it

Аннотация:

Не выходя за рамки концепции «Интернет на благо общества», в данной статье предложен взгляд на потенциальные последствия и, даже напротив, недостатки текущей цифровой трансформации. В ней проводится анализ некоторых ключевых фактов и событий, которые стали приметами недавнего прошлого и способствовали тому, что переход к цифровым технологиям был определен как естественная эволюция нашего общества. В статье представлен взгляд гуманитарных наук на кибертехнологии, который учитывает последствия для общества в среднесрочном и долгосрочном периоде. Наш "мир" меняется под воздействием кибертехнологий, правительственных процедур, цепочек снабжения и производства, общих служб и многого другого, поскольку все они основаны на кибертехнологиях и цифровых платформах. Цифровые платформы по большей части являются частными и ключевые сосредоточены всего в нескольких странах, в результате чего возникает некое подобие олигархии. «Пульт управления» нашей повседневной жизнью часто находится вне пределов контроля нашего национального государства. Во многих случаях двойственность «киберпространства» проявляется в том, что хоть оно и способствует повышению устойчивости всех систем, ввиду своего всеобъемлющего характера, может само стать мишенью для атак. В «аналоговом» мире у нас были разные «каналы» для нашей деятельности. В киберпространстве вся «система» зависит от кибертехнологий. Это представляет значительный риск, как в случае сбоя в работе или хакерской атаки, так и в случае принятия «решения сверху» об отключении. В такой ситуации для реализации плана Б потребуется значительное количество времени. Платформы социальных сетей и глобальные производители контента «подготавливают» молодежь, предлагая «единый глобальный» подход. Это окажет влияние на будущие поколения и чувство их культурной идентичности. Недавняя пандемия ускорила переход к цифровым технологиям. Всё большее число граждан, «оторванных» от цифровых технологий, вынуждены проходить «цифровизацию». Это оказало значительное влияние на кибербезопасность.

[Scientific Articles]

Ronchi A. M.
Is It All Gold That Glitters? The "New Normal"

Мы окружены элементами «критической инфраструктуры», управляемыми киберкомпонентами, которые в случае атак могут оказать как серьезное, так и незначительное воздействие на нашу повседневную жизнь. Что касается социальной сферы, то мы находимся внутри нашей киберсферы, в которой мы находимся в своего рода симбиотических отношениях. Люди познают мир посредством киберустройств. «Новая реальность» — это та реальность, которую создают устройства. Одиночество в киберпространстве — один из предсказуемых рисков — является своего рода зависимостью от этой «параллельной жизни», обучающей пользователей переходить от реальной жизни к мета-жизни, стирая между ними границы. Является ли «новая нормальность» тем, к чему мы стремимся?

Ключевые слова: Интернет на благо общества, цифровая трансформация, кибертохнологии, цифровые платформы, кибербезопасность, цифровой переход, критическая инфраструктура