Information & Security

A. Ronchi
vol. 53, no. 2 (2022): 221-239
https://doi.org/10.11610/isij.5315

Published since 1998
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Human Factor, Resilience, and Cyber/Hybrid Influence

Alfredo M. Ronchi (✉)

Politecnico di Milano, Milano, Italy, http://www.polimi.it

ABSTRACT:

The aim of this article is to depict some of the impacts of the ongoing digital transition on security, considering human factors, resilience, cyber and hybrid threats. After a short description of literature and related works, the article focuses on the term "security" to better clarify the meaning, then introduces the process of digital transition and related aspects including "datafication" and potential harms to cybersecurity and the potential resilience breaches due to the concentration of tasks based on digital technology including production chains and digital manufacturing.

Recently, the digital transformation has had a considerable impact on cybersecurity due to the boost generated by the pandemic and the increasing number of "digitally divided" citizens forced to "go digital" and related need to foster a culture of cybersecurity since the primary schools. This section includes an overview of different approaches to the "securitisation" of cyberspace. Back to security in a broad sense freedom of expression is the first aspect considered, including hate, fake news and propaganda, influence on opinion dynamics potentially applicable to the social and political sectors, as a kind of technological extension the combined use of big data and machine learning to activate nudging as a silent weapon, the risks directly connected to the concentration in few countries of online platforms directly connected with the last topic that is the emerging Internet of behaviour that thanks to the incredible amount of users' data can monitor ad address citizens' behaviours.

The list of impacts included will simply provide an idea about some of the potential threats, but they are not limited to this set.

ARTICLE INFO:

RECEIVED: 15 JUNE 2022
REVISED: 20 AUG 2022
ONLINE: 23 SEP 2022

KEYWORDS:

cyberwarfare, hybrid threats, soft concerns, artificial intelligence, machine learning

✉ Corresponding Author: Tel.: +39 393 0629373; E-mail: alfredo.ronchi@polimi.it

Related Work and Literature Review

Some previous papers like "21st Century cyberwarfare", "Hybrid Threats: defence line from the grassroots" and "'Soft' but still concerns" presented some threats to security due to cyber technology and much more specifically threats in the actual phase of digital transition. The document entitled "The Impact of digital transition on society and economy" included in the outcomes of the WSIS Forum 2022 complete the analysis of the impact of digital transition. Concerning the concept of "security" there are several papers and volumes considering security from different standpoints the key assumption relating security to assets and threats is the basic introduction to any cybersecurity course.

Resilience, a keyword recently discovered by governments and media, extended its original meaning from the structural sector to any sector including education. Therefore, the literature is extremely wide even if, in our field, one of the key sectors is critical infrastructure resilience or cyber disasters resilience [i] [9].

The oversupply of information (info-obesity) [3], resulting in its devaluation and loss of trust to professional media; monopolization in the field of communication and polarisation;[ii] the transformation of the Internet from a space for the free exchange of ideas into a tool for supervision and management (Makkuni R.),[iii] with Internet companies turning into digital giants, moving from digital platforms to digital ecosystems and annexing not only cyberspace, but also real sector industries (monopoly and dominant position); the massive decrease in the level of critical thinking [21 – Peralta 2022] and the emergence of waves of information epidemics of national and global levels; with public perception shaped more by means of addressing feelings and personal opinion rather than actual facts, with fakes, clickbait, hypes and other tools introduced to form post-reality in the political and media culture; changing the system of values – with the new normal (semantic shifts, etc) [30 – Ronchi 2018], new ethics putting personal free will and freedom of choice under question; traditional cultural regulators of social relations and processes being displaced by automated social algorithms, increasing role of algorithms and ML [16 – Juul 2019]; blurring the borders between the real and the digital world, wide spread of simplified virtual mock-ups and simulacra; mass collection of data, the new oil, for managing people's behaviour, evaporation of privacy, data protection [39 - Williams 2013], formation of an appropriate economic imperative to direct the development for business, society and states; increasing the level of conflict

[i] 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.

[ii] Mainstream communication, freedom of speech, limited contraposition, fake fake-news.

[iii] See "The Betrayed IT Revolution" and related videos on Facebook, January 8, 2021.

in society between individuals and groups – haters, discrimination, and between states [27 – Ronchi 2018].

Society on the Move

Nowadays, there is a recurring buzzword: Digital Transformation (DX or DT) – it is an opportunity or a nightmare? The pandemic strengthened this trend, digital transformation helps to mitigate the effects of the crisis, improve resilience. "Resilience", by the way, another recurring term in the pandemic time. We all agree on the meaning of the term "transformation" but "digital" has different meanings. Jim Swanson, CIO of Johnson & Johnson says, "Digital is a loaded word that means many things to many people".

"Say 'digital' to persons and they think of going paperless; another might think of data analytics and artificial intelligence; another might picture Agile teams; and yet another might think of open-plan offices". A comprehensive definition of the term digital transformation should be the integration of digital technology into all areas of activity, from business to public sector, fundamentally changing how we operate and deliver value to customers or citizens. The adoption of digital technology represented a true competitive advantage, literally "Competitive advantage refers to factors that allow a company to produce goods or services better or more cheaply than its competitors. These factors allow the productive entity to generate more sales or superior margins compared to its market competitors."

It is evident that digital transformation it is not a process "one size fits all", each specific sector and even activity requires a particular approach and custom solution; this starting from the three main branches: citizens, companies, public administrations. Because digital transformation will look different for every company, it can be hard to pinpoint a definition that applies to all. Sometimes this means walking away from long-standing business processes that companies were built upon in favour of relatively new practices that are still being defined. In such a situation the "trial and error" finding by continues improvements the optimal solution is the practical approach.

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. After having briefly introduced potential benefits, let's now try to depict some of the potential tangible or intangible effects of DT that may jeopardise security. Of course, the following one is not a complete list of impacts but provides a first glance. Let's start from the term security itself.

Total Security or Different Levels of Insecurity?

This paper focus on how human factor, resilience & cyber/hybrid attacks influence security in a broad sense at personal, social, and national level. 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".[iv] 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" quoting Salman Rushdie.[v] Why we say, "level of insecurity"? Because there is not total security or better "*There is no such thing as perfect security, only varying levels 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,[vi] risk assessment, probability,[vii] 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.

Resilience Based on Digital Resources

As mentioned before, on the pandemic cyber technology offered a valuable contribution to ensure "business" continuity; government services, justice, health sector, education not forgetting supply chains 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 license, Bank Account, ID Pay, etc.), and certifications (vote certificate, vaccinations, etc.). Biometric 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 tested on the field has shown some weakness. All the rest of our personal data are already stored somewhere in our

[iv] 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.

[v] Iranian / British writer recently suffered an attempt to kill him in NYC.

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

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

country or abroad thanks to our "buddies" like our smart phone or smart watch. Some of the survival "almost" traditional documents will be soon enforced by cross validation thanks to our digital ID.[viii]

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 supposed total dependence from the cyber domain represents a significant weakness that merges with the extended lack of digital literacy and cybersecurity awareness on the citizens' side.

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 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. 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.[ix]

Cyber Attacks

The increasing role of cyber technology in our everyday life and key services increases at the same time and even more the risk of cyber-attacks. We already faced several relevant attacks due to hackers, some targeting Governmental or Law Enforcement agencies and Institutions, some targeting critical infrastructure, 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.[x]

[viii] 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".

[ix] Source: The World Bank archive.

[x] This to do not mention Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

Today even cars may be subject to cyber-attacks as it was already demonstrated[xi] 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, PLC[xii] 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. If you remember the so called "Cross" system based on EPROM and nowadays IIoT (Industrial IoT) you have a comprehensive idea about the evolution of technology in Industrial Automation. Some automation solutions are even equipped with the runtime environment available at that time when TCP/IP protocol was available, but the Internet was not yet available, and the term and concept of "cybercrime" was far to be coined [5- Dow, 2020].

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.

Cybersecurity, AI and Cybersovereignty

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[xiii] [8 - European Union 2016]. Of course, the

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

[xii] 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.

[xiii] https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

overall scenario includes many other aspects and "shades" [xiv] [9 - European Defence].

"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 mean 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'. To build a sounding information society we must efficiently counteract cyber-criminality and establish a clear vision on legal behaviours in the cyber-world" [35 - Ronchi 2022].

The number of breaches grows steadily, with the incident response and attack defence techniques being time-critical, as many compromises (87%) occurring within minutesv.[xv] This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks.

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.

Nowadays the key concept is "holistic security", a "global" approach to security integrating all the different aspects and problems. A specific interest is devoted to digital security breaches that caused, in 2021, 6 trillion-dollar losses and accordingly to Cybersecurity Ventures will cost the world 10,5 trillion-dollar annually by 2025.

Digital security is more than focus on software or tools, integrating emotional well-being, personal and organizational security. Good implementation of digital security tools and tactics requires attending to the practitioners' psychosocial capacities to recognize and respond dynamically to different threats to themselves and to participants related to project data collection and communications (intimidation, social engineering.) accordingly with Leonardo 85% of successful cyber-attacks is due to human errors.

In relatively recent times cybersecurity has reached the ranking of a homeland security component. An increasing number of regions and countries have established cybersecurity reference units like CISA (Cybersecurity Agency – US), Incident response centre like CSIRTs, CERTs, CIRTs, or SOCs that have a

[xiv] Ronchi A.M., Soft but still concerns, proceedings International Conference on 'Homeland' Security Emerging Trends, Challenging Aspects - Hasan Kalyoncu University, Turkey 2021.

[xv] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_ execsumm ary_en_xg.pdf

broader function covering both security and cyber security. More specifically in the domain of homeland security we found the United States Cyber Command (USCYBERCOM), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCCOE) located in Tallin that issued two editions of the so called Tallin Manual shaping the protocols of cyberwarfare including the rules of engagement. More recently NATO announced the establishment of the Cyberspace Operation Centre (CYOC) by 2023. Of course, each country has created specific structures to deal with cyber threats usually tightly connected with defence industries. The European Commission issued different documents among them the European Cybersecurity Strategy and related documents [8 - European Union; 9,10,11 -European Commission]

Artificial Intelligence and Machine Learning are playing a relevant role even in this sector as AI v/s AI. Some country even devoted a specific ministry to Artificial Intelligence. To underline the interests in AI on October 2017 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”. Their strategy is to double the contribution of the digital economy to the UAE’s non-oil GDP from 11,7 per cent to over 20 per cent within the next ten years (source Ministry of AI – UAE).

India is particularly interested in enforcing cybersecurity and hosts every year the International Conference on Cyberlaws, Cybercrime, Cybersecurity. The government of India launched ten initiatives on cybersecurity.[xvi]

Russian Federation: Leonid Todorov, Deputy Director of the Coordination Centre for TLD RU, on the Russian Country workshop at WSIS Forum 2013 gave a contribution entitled “*Fostering the Multistakeholder-Based Model*”. The implementation of the Internet governance in Russia is considered as “*The Internet as a Test-bed for Multi-stakeholderism*”. Chapter 5, Clause 26 of the Federal Act “On communications” (7 July 2003), states: “*The multi-stakeholderism process is supported by platforms for the nation-wide debate*

[xvi] 1) establishment of the Indian Computer Emergency Response Team (CERT-In); 2) The Cyber Surakshit Bharat and initiative of the Ministry of Electronics and Information Technology that aims to create a robust cybersecurity ecosystem in India; 3) the establishment of the National Critical infrastructure Protection Centre; 4) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre; 5) National Cybersecurity Strategy; 6) Appointing Chief Information security Officers; 7) Plan of Action for Crisis Management; 8) Website Audit to conduct an audit on all the governmental web sites; 9) Drills and Training to simulate, thanks to CERT, drills and other tests to improve training; 10) Protection Against Malware in addition to Cyber Swachhta Kendata additional tools to protect from malware are provided care of government.

such as the Russian Internet Forum,[xvii] *activated in 1997. RIF is one of the major platforms for ICT & Internet businesses grouping some 8000 participants."*

China, in the 1980s, under the Chairmanship of Deng Xsiaoping (鄧小平), announced the concept of a Chinese Great Firewall (GFW); it was the time of the economic reform of China and the concerns about the potential influence due to the Internet's indiscriminate access was exemplified by the phrase "*If you open the window for fresh air, you have to expect some flies to blow in.*"

The GFW is a combination of technologies and legislative actions aimed to regulate the Internet domestically. The system blocks access to forbidden content (e.g., pornography) and slows down international communication in general and in particular with selected Internet servers and services (e.g., Google). The GFW favoured the creation of Chinese versions of the most popular services, and social apps. The Chinese contribution on the Internet at global level is the World Internet Conference, organized by government agencies to discuss Internet issues and policy, to be held in Wuhzen every year since 2014. On that occasion an unknown party distributed a draft joint statement affirming the right of individual nations to develop, use, and govern the Internet. Participants received a copy of the statement; some of them objected to the proposal so there was no mention of it on the conference's final event. The Chinese leader Xi Jinping (習近平) calls "cyber sovereignty" the concept outlined in that statement [2 – Baezner 2018]. The World Internet Conference (WIC), which is sometimes translated into English as the World Forum on Internet Governance, may be considered the Chinese answer to the United Nations Internet Governance Forum (IGF).

In 2017, the foreign ministry and cyber-space affairs officials unveiled China's first cyber policy paper while stating that China would beef up its cyber-warfare capacities to defend against foreign threats [12 – Franzese 2009].

Long Zhou, coordinator for the foreign ministry's cyber affairs division, said "*Cyber-attacks, cyber espionage, surveillance have become major issues confronting all countries*". Describing the Internet as rife with subversive thought, religious extremism, pornography, fake news and financial scams, Long said China "*stands ready to work together with pa*rtners", as well as other countries on new governance measures. The Communist Party leadership's claim that countries should wield sovereign authority over all cyber- related matters within their territory, the so-called "cyber sovereignty" [14 – Irion 2012]. Long said "*Every country needs to decide on the balance between freedom and order, and we have to respect how each country reaches that decision*".

Back to security in a broad sense

Having depicted the transition from the analogue world to the digital one as a complex process boosted by the pandemic, compressing the time devoted to evaluate pro and contra related to some solutions and having outlined that the

[xvii] http://russianinternetforum.ru, last accessed January 2019.

concept of “security” it is not an absolute and permanent status but we can identify it as a “dynamic balance” between a specific “asset” to be secured against specific threats sometimes for a specific time span, we posed the focus on the double nature of “cyber” many times it contributes to improve resilience but because of its pervasive attitude it can be the target for attacks and generate the “perfect storm”. Let’s now consider some specific aspects concerning the impact of digital transition on human factors, resilience & cyber/hybrid attacks.

Impact on Freedom of Expression [xviii]

If the early stage of Internet communication was based on the so-called “netiquette,” a kind of Galateo or Bon Ton of Internet users, the advent of Web X.0 and the social web requires more specific rules addressing first the field of ethics and privacy [6 – Duggal 2018]. The cyber revolution ignited by Xerox PARC’ Alto system, Apple II and IBM PC addressed the popularisation of computer resources and sense of freedom. Once connected online, Gopher and Veronica first, and Web Technology later amplified this sense of freedom to connect, to exchange, to reach and communicate with a broad audience, the reference market itself changed from scientists and nerds to citizens.[xix] Of course, freedom of expression is one of the most appreciated opportunities offered by the network and it is already evident that any kind of top-down censorship or control fails even if the concept of Cyber Sovereignty, exists and is promoted.[xx] The evident vocation toward freedom of expression is many times a direct cause of governmental censorship forbidding social applications in some countries. So it happens that Twitter, Facebook, Instagram, YouTube or even some thematic websites are not allowed. Here apart from political, ethical, and philosophical issues may come to the fore the economic and financial aspect of entering that market adhering to the requested censorship or not.

Freedom of expression is usually associated with the terms hating, online libel, hoax, fake news this because the improper use of freedom of expression can generate such negative behaviours. Of course, such extensive and negative interpretation of freedom might generate some reactions that can be even worse than the problem itself. We must distinguish between two main branches “hating, online libel“ and “hoax, fake news”, the first branch must be censored as it was at the time of Netiquette, the second, if not related to the first, is much more critical to be managed without the risk of infringing freedom of expression. A typical and sometimes concrete example of infringement of freedom of expression is the establishment of a “commission” in charge for the

[xviii] Freedom of expression or freedom of speech is one of the key aspects of the human rights, UN, UNESCO, CoE, Amnesty International and more consider this as a fundamental right.

[xix] In 1995 the motto for the whole family was “Where do you want to go today?”

[xx] VPN and foreign smart phones SIM are the basic tools to escape.

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.

These aspects are sometimes related with the so called “mainstream communication” due to business or political interests, other times, as we will deal with in the following paragraphs, is related to other countries propaganda or global finance interests and more. In the meantime, private Internet companies, growing into an almost unregulated sector, are turning into digital giants, moving from the monopoly of digital platforms, having the right to silence alternative views, to digital ecosystems and annexing not only cyberspace, but also real sector industries (monopoly and dominant position).

Some of the suggestions to minimize the risks are stated within the UNESCO IFAP International Conference [xxi]: “*The society’s attitude to information is gradually changing. We used to perceive it as an important semantic resource for individual decision-making, but today the main resource is the primary digital data array produced by humans and devices in the process of life. Online platforms, which were originally aimed at facilitating human communication and accelerating interaction, now enclose individuals in filter bubbles and echo chambers due to their recommender systems designed to enhance users’ engagement. This situation boosts the radicalization of society, provoking conflicts between people, social groups and even states. These phenomena are accompanied by a massive decrease in the level of critical thinking and the emergence of waves of information epidemics of national and global scale. While value paradigms are also changing, theories reflecting doubts in personal free will and freedom of choice are actively spreading.*

Proposition:

Auditing online platforms’ recommender and moderation systems to ensure that they do not infringe upon freedom of expression and information.

Supporting up-to-date media, social and information platforms pluralism, independence, inclusiveness, relevance including by permitting journalists to investigate independently, with adapted protection and appropriate funding.

Recommend Member States to agree on global regulations on technologies potentiality framing humans like intelligent algorithms, sensors, connection always on, and tracing tools active 24/7.”

Impact on opinion dynamics in social networks

This paragraph will outline the potential role of digital media in shaping the opinions, they represent a relevant part of how we perceive reality and interpersonal relations. The ability to influence the shaping of opinions can promote collective action, influence democratic processes, modify citizens’ behaviour.

[xxi] Third International Conference Tangible and Intangible Impact of Information and Communication in the Digital Age. UNESCO IFAP, Khanty-Mansiysk, Russian Federation, 17–18 June 2021.

Opinion formation is a complex and dynamic process mediated by interactions among individuals both “de visu” and online[xxii]. Researchers in the social and natural sciences have analysed this phenomenon trying to describe how shifting individual perspectives can lead to the outcome: consensus, polarization, or dispersion [18 – Martins 2009].

In the “analog” era opinion dynamics were influenced by radio and television news and debates, newspaper titles, clustering of citizens in public spaces. Sometimes to deeply influence the opinion fake news were disseminated as journalistic scoops or gossip propagation. Time dimension was a key aspect, the opportunity to counterbalance the opinion’s trend was offered by the next TV round table or a newspaper interested in publishing the defence thesis. In the cyber era opinions can be influenced several times the same day, tweets, posts, videoclips can feed the battleground in real time.

Human factors are of course deeply in the loop, social media can play a relevant role in shaping the public opinion nowadays much more that press and television did in the past even if they are both part of the “toolkit” to shape opinions. “*They can elicit the will to change the government, to feel oppressed or damaged by other countries, to join a different country because of economy, culture, etc…*”[xxiii]. 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 [21 - Peralta 2022]. Social media have become a battlefield on which opinions are, often violently, exchanged, and aimed fake news and propaganda disseminated. In turn the behaviour of social media has become an important early indicator of societal change.

Opinion dynamics research has developed models of opinion formation, adjustment, and exchange for over 60 years. The main mechanisms in these models are positive social feedback, opinion, and status homophily, negative social feedback, and the structure of the social network.

These models share the property that opinions are modelled as binary variables, finite sets, or low-dimensional vectors. The typical graph is a net of nodes and relations, each node has a binary value (0,1) and is connected to other nodes, let’s consider that all the nodes have threshold equal to 0,3 if more than 30% of the connected node is set to 1 even our node will choose 1. This may propagate quickly if the other nodes are “conformist” so they accept the mark that is expressed by the majority, but if there is a “hipster” in the group, he will adopt the minority opinion taken from previous confrontations. This scrambles the model and can even led to a minority opinion dominate the scene [16 – Juul 2019].

While this is sufficient for toy models and allows to reproduce interesting qualitative behaviours, such as opinion cascades, opinion bottlenecks, gatekeepers, and opinion leaders, it is too coarse a description to connect these

[xxii] CIRPA Interuniversity Research Centre in Environmental Psychology - University la Sapienza Roma member of S2D2 JRC.

[xxiii] Excerpt from Ronchi A.M., “21ST Century Cyber Warfare”.

models to data from social media. Replacing these extremely coarse opinion representations by the devices that computer scientists use to represent opinion anyhow: knowledge graphs it will be easier to analyse opinion dynamics.

More specifically, opinion dynamics in social networks can be studied by large-scale analysis of social media using state-of-the-art methods of natural language semantic analysis and machine learning technology to identify recurring patterns that provide the entry points for opinion dynamics.

Recent events demonstrated how simple is to shape public opinions and build consensus thanks to the combined action of different apparently independent media and channels. Citizens are flooded by apparently different information targeting a unique goal, different communication channels apparently nonrelated provide a kind of cross-proof of credibility. The basic rule of journalism, check three different sources before publishing the news is no more used, there is no time to check otherwise you lose the momentum and pace.

Impact on decision making

The extensive use of AI, ML 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 (by the GDPR[xxiv]) and if the desired result falls within the category of fraudulent transactions (thanks to the UCPD[xxv]). 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.

In other words, a set of goals defined by human agents may be reached using decision-making mechanisms, recommendations, or other interaction influences. In addition, some nudge mechanisms are built unintentionally by the system to achieve its ends. This process may generate several ethical risks for individuals, groups, or society. We know that a "*moral harm can result from good intentions*". However, AI-enhanced nudges do not have an intention of their own but use inferential rules to obtain the most efficient result for a given purpose. Using a wide approach, AI-enhanced nudging mechanisms may include all gradations of decision incentives not-designed by human agents: namely, when the creation does not take place in the design phase, but is an automatic process influenced by personal behaviours, collected data and the

[xxiv] General Data Protection Regulation (2916/679).

[xxv] Unfair Commercial Practices Directive 2005/29/EC.

use of static models. Several science fiction movies outlined this shift from positive outcomes to software self-identified goals[xxvi]. During this process the system becomes a multi-agent system in which the initial well-intentioned purpose of the developers can be misrepresented and create damage to individuals, groups of people or the whole society. An example of this is fake news, for which it is often not their ethical nature that is in question, but their AI-enhanced method (i.e., using statistical models to empower the recommendation system of social network) of massive distribution over a long period of time to a specific group of people that can have large-scale social and economic implications. Impacts may be disrupting for society and democracies by limiting representativeness in the democratic process, augmenting social exclusion thank to the reinforcing recommendation mechanisms based on available personal data, decreasing diversity in executives' roles by reducing the opportunity to be recruited due to the lack of information that can be used to infer a profile, etc. The European Commission is asking for contribution in the field of depicting the future of democracy, AI impact on democratic processes and more. In short, although some nudges may be used positively, monitoring the consequences of AI-enhanced nudging mechanisms is crucial to mitigate possible risks in European societies and democracies.

Impact on businesses

Change in technology and user profiles cannot avoid impacting businesses and markets. The market is evolving in a very significant way. The diffusion of platforms if on one side creates new opportunities on the other side "kills" several existent businesses. If on one side platforms open the "global" market to small and micro enterprises offering them a "window" on the globe, the access to global service platforms creates a shortcut between offer and demand cutting out major part of the traditional added value chain, as it was long time ago because of malls it is now because of platforms.

Platforms are the real "silver bullet" that created major opportunities and a real impact on society and the economy. A relevant part of digital transformation relies on platforms and standards [25 – Ronchi 2020], these aspects are directly linked with the "owners" of such platforms and standards, this can be considered a kind of monopoly not yet regulated, a kind of grey zone, so in the digital transition there is a potential risk, despite antitrust laws, to fall under the control of few key players. This aspect was recently outlined by the censorship action of some platforms that cancelled user profiles and entire video channels opening the discussion on the balance of the rights between the owner of the platform and the user of the platform. This aspect can lead to the infringement of the human right "freedom of expression" as we have already seen.

Following the schema of some of previous revolutions the idea was: digital technology is disruptive cancelling several businesses, but new businesses will

[xxvi] E.g., the science fiction movies: Wargames, Eagle eye, Stealth.

be created, the key point is that the specific nature of digital technology is creating less positions than the one 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 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 “spill over”.

The big difference, compared to the past, is that you don’t need to invest relevant capitals to feed your business, the key investment is the creation of the digital platform, the asset you own is the number of users both on the offer and demand side, this to do not consider the fiscal benefits they usually enjoy compared with the traditional retail system.

As mentioned above, several global key players are monopolising some sectors of the market pulling out of business competitors so because of the concentration in few countries of such players and their private nature there is a risk to be cut out from the platform unilaterally, this means to be unable to feed our supply chain with some goods once provided only by that platform.

Furthermore, everyone experienced in “ICT based innovation” knows that “*It is not only a matter of technology*”. Human factors are an essential tile of the whole process as well as a re-thinking of the whole organisation and process. We must keep humans in the loop and carefully consider the social and economic impact due to digital transition.

Impact on commerce

An outcome of the merge of big data analytics and behavioural psychology is Internet of Behaviours (IoB) [15 – 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).

From a behavioural psychology standpoint, the IoB tries to comprehend the data acquired from users’ online activities sometimes merged with IoT data [1 – Babel 2015]. This mix offers important information on client behaviours, interests, and preferences. Consumer data may be gathered from a range of sites and technologies, including a company’s website, social media profiles, sensors, telematics, beacons, health monitors, and a variety of other devices. When we accept “cookies” without checking them it may happen that some of them will “profile” our interests, other times the application offers the opportunity to save a “wish list”. Cross referencing searches[xxvii] and queries the system can extrapolate the expectations of customers. It aims to answer the question of how to interpret data and how to use that knowledge to develop and promote new goods, all from the perspective of human psychology.

The term “IoB” refers to a method of analysing user-controlled data from a behavioural psychology standpoint. It aims to answer the question of how to

[xxvii] Mc Guigan L. (2021) This tool let’s you confuse Google’s ad network, and a test shows it works, MIT Technology Review.

interpret data and how to use that knowledge to develop and promote new goods, all from the perspective of human psychology. The findings of that study influence new ways to create a user experience (UX), search experience optimization (SXO), and how to advertise a company's final products and services. Both Google and Facebook utilize behavioural data to provide ads to users on their sites [7 – Egger 1996]. This enables companies to interact with their target consumers and measure their behaviour in response to advertisements via "click rates." Of course, the aim or this analysis is may not limited to business and commerce but is suitable to understand and address the expectations of citizens on social and political behaviours. This branch of technology poses some Ethics and Legal concerns, how far can technology manipulate humans, who is going to protect citizens from misuse and abuse of this potentially powerful tool/weapon?

Conclusions

Wrapping up, we depicted some of the impacts of the ongoing digital transition on security considering human factors that are one of the most common weaknesses, the concept of resilience recalling us both critical infrastructures today referring to a far wider range of assets and the entire cyber domain due to its central role in digital transition and innovation. Cyber and hybrid threats are the forefront of the innovation in political and economic conflicts.

Hybrid threats and soft concerns are a recent scenario to be explored and understood quickly to setup proper counter measures and mitigation plans. "Soft" weapons like manipulation of opinions dynamic, mainstream communication campaigns and propaganda, plus the application of AI to neutralise AI or activate nudging processes are some of the most recent tools to run undeclared "warfare". We are aware that each of the specific threats deserve a full paper exploring the full range of impacts, getting in technical details, and outlining the potential dynamic balance between measures and countermeasures. This will be the key tasks concerning future papers. Not all the potential threats have an ideal countermeasure anyway it is a paramount to foster required awareness and foster at the same time a culture of cybersecurity from the grassroots.

Future trends

First, one growing opportunity is the appropriate use of ICTs for development and for inclusivity of nations and regions. But as the Internet and its providers are transboundary entities, national access, or denial of access – inclusion or exclusion -- within any country also affects an entire region and beyond. The impacts of digital exclusion are now seen upon individual citizens, but also upon international markets, financial institutions, and regional economic development.

Second, work on hybridity – the potential of ICTs and of tech in general – to work non-hegemonically with populations that have and wish to maintain their traditional technologies, shows great potential. Further discussions of "low-tech no-tech" and "low-code no-code" showcase opportunities to benefit all societies, not only the least-developed. In addition, hybridity between ICTs and traditional tech can assist in sustaining the impetus for democratization and decolonization of technology.

The challenges for the upcoming years are the ways to sustain the humanitarian part and the inviolable right to freedom and personal privacy in an era of unlimited supply of information and technological ventures. The need to find a proper balance is omnipresent. Social sciences and humanities must establish a tight cooperation in designing or co-creation of cyber technologies always keeping humans in the loop.

References

1. Chris Babel, "Tackling privacy concerns is key to expanding the internet of things," Wired Innovation Insights, February 2015.
2. Marie Baezner and Robin, Patrice, "Trend Analysis: Cyber Sovereignty," *CSS Cyberdefense Reports*, 2018, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314398/Cyber-Reports-201801.pdf?sequence=1&isAllowed=y.
3. Roger E. Bohn and James E. Short, "How Much Information?" Global Information Industry, Center University of California, San Diego, 2009.
4. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," JOIN (2013) 1 final, 2013.
5. Mike Dow, "Preparing for Next-Generation Cyber Attacks on IoT," Silicon Labs, 2020.
6. Pavan Duggal, *Cyber Law 3.0: An Exhaustive Section Wise Commentary on The Information Technology Act Along with Rules, Regulations, Policies, Notifications Etc* (Gurgaon, India: LexisNexis, 2018).
7. Oliver Egger and Matthias Rauterberg, "Internet behaviour and addiction," *Work & Organisational Psychology Unit (IfAP), Swiss Federal Institute of Technology (ETH) Zurich*, 1996.
8. European Union, "Joint Framework on countering hybrid threats a European Union response," 2016.
9. European Commission, "Resilience, Deterrence and Defence: building strong cybersecurity for the EU," JOIN (2017) 450 final, 2017.
10. "EU Cyber Defence Policy Framework (2018 update)," Council of the European Union, 2018.
11. "European Defence Action Plan: Towards a More Competitive and Efficient Defence and Security Sector," European Parliament Legislative Train 04.2019, 2019.
12. Patrick W. Franzese, "Sovereignty in Cyberspace: Can it exist?" *Air Force Law Review* 64 (2009): 1–42, https://go.gale.com/ps/i.do?id=GALE%7CA212035708&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00948381&p=AONE&sw=w&userGroupName=anon%7Eba90e7b6.

[13] High Representative of the European Union for Foreign Affairs and Security Policy "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," JOIN (2013) 1 final, 2013.

[14] Kristina Irion, "Government Cloud Computing and National Data Sovereignty: Government Cloud Computing and National Data Sovereignty," *Policy & Internet* 4, no. 3-4 (2012): 40–71, https://doi.org/10.1002/poi3.10.

[15] Adam Joinson, "Internet Behaviour and the Design of Virtual Methods," 2004, http://www.joinson.com/home/pubs/02%20Virtual%20methods021-34.pdf.

[16] J. S. Juul and M. A. Porter, "Hipsters on networks: How a minority group of individuals can lead to an anti-establishment majority," *Phys. Rev. E, 99:022313*, 2019.

[17] "Joint Framework on countering hybrid threats a European Union response," European Commission JOIN (2016) 18 final, 2016.

[18] Andre C. R. Martins, Carlos de B. Pereira, and Renato Vicente, "An opinion dynamics model for the diffusion of innovations," *Physica* A 388 (2009): 3225–3232.

[19] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn manual 2.0 on the international law applicable to cyber operations* (Cambridge University Press, 2017).

[20] "Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society," UN, General Assembly, 2015, https://digitallibrary.un.org/record/ 814431?ln=en.

[21] Antonio F. Peralta, János Kertész, and Gerardo Iñiguez, "Opinion dynamics in social networks: From models to data," Handbook of Computational Social Science, 2022.

[22] Zachary N. J. Peterson, Mark Gondree, and Robert Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in: *Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing. Presented at the HotCloud'11, USENIX Association, Berkeley, CA, USA,* 2011, p. 5, https://www.usenix.org/legacy/event/hotcloud11/tech/final_files/Peterson.pdf.

[23] Dana Polatin-Reuben and Joss Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet," *4th USENIX Workshop on Free and Open Communications on the Internet*, 2014.

[24] Alfredo M. Ronchi, *WSIS Forum 2015: High Policy Statements* (Geneva, 2015), https://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf.

[25] Alfredo M. Ronchi, *Digital transformation*, proceedings ICCC (New Delhi: Cyberlaw, 2020).

[26] Alfredo M. Ronchi and Pavan Duggal, *WSIS Forum 2016 Outcomes* (Geneva: International Telecommunication Union (ITU), 2016), https://www.itu.int/net4/wsis/forum/2016/Outcomes/.

[27] Alfredo M. Ronchi, *Cybertechnology: Use, abuse and misuse* (Moscow, Russian Federation: UNESCO IFAP Interregional Library Cooperation Centre, 2018).

[28] Alfredo M. Ronchi, "21ST Century Cyber Warfare," *Information & Security: An International Journal* 44 (2020): 53-61.

[29] Alfredo M. Ronchi, (2018), "Hybrid treats: defence line from the grassroots," *Journal of Defence & Security Technologies* 3, no. 5 (2020): 84-95.

[30] Alfredo M. Ronchi, *"…1984 won't be like "1984"?"* (Milano: Politecnico di Milano, 2018).

[31] Alfredo M. Ronchi, *Thematic Workshop: ICTs for Safety, Security and Disaster Recovery* (Geneva (CH): International Telecommunication Union ITU, 2018).

[32] Alfredo M. Ronchi, *e-Citizens: Toward a New Model of (Inter)active Citizenry* (Springer (D), 2019).

[33] Alfredo M. Ronchi, *e-Democracy: Toward a New Model of (Inter)active Society* (Springer (D), 2019).

[34] Alfredo M. Ronchi, *"Soft" but still concerns, volume Homeland Security* (Ankara: Hasan Kalyoncu University Press, 2021).

[35] Alfredo M. Ronchi, "From Ingsoc to Skynet it is not only science fiction: From novels and science fiction to quasi-reality," UNESCO IFAP Intergovernmental Council, 2022.

[36] "Shared Vision, Common Action: A stronger Europe," European Union, June 2016.

[37] *Internet of Things: Visualise the Impact*, SAS report, 2022 https://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html.

[38] UNESCO, "Sustaining human progress: reducing vulnerabilities and building resilience," Human development report, 2014.

[39] Sarah Williams, Lucy Yardley, Gary B Wills, "A qualitative case study of LifeGuide: Users' experiences of software for developing Internet-based behaviour change interventions," *Health Informatics Journal* 19, no. 1 (2013): 61-75. https://doi.org/10.1177/1460458212458915.

About the Author

Alfredo M. Ronchi is a Professor at Politecnico di Milano (Engineering Faculty), Expert/advisor in e-Services, Head of the JRC S2D2 (Safety, Security, Defence, Disaster Recovery and Management) Politecnico di Milano, General Secretary of the EC-MEDICI Framework of Cooperation, delegate at UNESCO IFAP and active member of the WSIS since the establishment (2003- …). He cooperated as organizer or programme chair in W3C, ACM, IEEE conferences; since more than thirty-five years he organizes and manages international conferences and workshops. Author/contributor of more than 400 papers and various books on e-Culture, IPR, e-Government, and e-Services.
https://orcid.org/0000-0003-1230-4338