Cyber Resilience, its Relevance, and Cyber Capacity Building

Alfredo M. Ronchi
alfredo.ronchi@polimi.it

Abstract:

The aim of this paper 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 paper focus on the term "security" to better clarify the meaning, than 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.
The impact of DT 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 on different approaches to the "securesation" of the cyber space. 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.

Resilience, a keyword recently discovered by governments and media, extended its original meaning from the structural sector to any sector including education. Therefore, literature is extremely wide even if, in our field, one of the key sectors is critical infrastructure resilience or cyber disasters resilience1 [9 – European Commission 2017].

The oversupply of information (info-obesity) [3 - Bohn 2009], resulting in its devaluation and loss of trust to professional media; monopolization in the field of communication and polarisation[2]; the transformation of the Internet from a space for the free exchange of ideas into a tool for supervision and management (Makkuni R. 2018[3]) , 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

1 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

2 Mainstream communication, freedom of speech, limited contraposition, fake fake-news

3 The betrayal of IT revolution: https://m.facebook.com/Sacred-World-Media-530888080655133/videos/the-betrayed-it- revolution/192288409296674/?__so__=permalink&__rv__=related_videos

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 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.

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.

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[4]". Therefore, we start to be concerned about security, it is no more a cost-free "commodity", we need to invest some resources to reach a certain level of "insecurity". Security is tightly related to different parameters: the asset or assets to be secured, the specific context, the range of potential threats, and more.

As the general concept of security evolved through time even the concept of national security evolved as well as homeland security and, the same happened in case of potential targets and threats. State actors face a very complicated scenario trying to match with the current and future developments of threats based on intelligence, information flow analytics[5], risk assessment, probability[6], 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

4 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.

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

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

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 licence, Bank Account, ID Pay, etc.), and certifications (vote certificate, vaccinations, etc). Bio metric is gaining more and more relevance in the sector of secure identification, from fingerprints to eye and, more recently, face, even if early face recognition tested on the field shown some weakness. All the rest of our personal data are already stored somewhere in our country or abroad thanks to our "buddies" like our smart phone or smart watch. Some of the survival "almost" traditional documents will be soon enforced by cross validation thanks to our digital ID[7].
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[8].

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[9].
Today even cars may be subject to cyber-attacks as it was already demonstrated[10] 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.

7 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"

8 Source: The World Bank archive

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

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

This to do not mention aircrafts, ships, trains, metro, and any other transportation means, PLC[11] 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.

Cyber security, A.I. 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[12] [8 - European Union 2016]. Of course, the overall scenario includes many other aspects and "shades"[13] [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 minutes[14]. 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.

11 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

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

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

14 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsumm ary_en_xg.pdf

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 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[15].
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 such as the Russian Internet Forum[16], activated*

15 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.

16 http://russianinternetforum.ru, last accessed January 2019.

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*".