Cybersecurity Impacts of the Covid-19 Pandemic in Italy

Marco R.A. Bozzetti[1,2,3], Luca Olivieri[4] and Fausto Spoto[4]

[1]Associazione Italiana Professionisti della Sicurezza Informatica (AIPSI), Milano, Italy
[2]Information Systems Security Association (ISSA)
[3]Digital Attacks Observatory (OAD) Team, Italy
[4]University of Verona, Verona, Italy

Abstract

The Covid-19 pandemic has pushed companies to the extensive use of digital services, to implement home working and provide online services to people in lockdown. As a consequence, it is interesting to study how this has affected the number, kind and distribution of cybersecurity attacks. This paper gives an empirical evaluation of the cybersecurity attacks at the beginning of the Covid-19 pandemic in Italy, based on data collected from the questionnaires of the annual Digital Attacks Observatory. It shows that the overall number of attacks has not increased, but attacks have affected smaller companies than before. This can be explained with the fact that the Italian industrial scenario is mostly populated by small and medium enterprises, that have been obliged to a quick reconversion of their IT systems and typically lack the necessary cybersecurity culture.

Keywords

cyberattack, cybersecurity, Covid-19, SME

1. Introduction

The Covid-19 pandemic and consequent lockdowns have obliged companies to face new challenges such as smart working, remote work and digitalization, accelerating all previous efforts in that direction. As reported by Gartner [1], most organizations were already moving their digital agenda forward at a steady pace, but the Covid-19 pandemic required a significant leap in the development of digital products and services, with the goal of maintaining and fostering customer engagement. However, digitalization has generated many cybersecurity issues and the intensification of cyberattacks all around the world [2, 3]. In this scenario, Italy is an interesting case study since it is home of mostly small to medium enterprises (SMEs), active in different sectors, and can consequently highlight cybersecurity aspects that are different from those faced by larger companies of greater influence. This paper presents the status of the Italian scenario, to understand how cyberattacks and cybersecurity have fared during the ongoing COVID-19 pandemic. Section 2 presents the *Digital Attacks Observatory*, a survey that we have used to collect relevant information about cybersecurity and Italian organizations. Sections 3

ITASEC'21: Italian Conference on CyberSecurity, April 07–09, 2021
m.bozzetti@aipsi.org (M. R.A. Bozzetti); luca.olivieri@univr.it (L. Olivieri); fausto.spoto@univr.it (F. Spoto)
https://www.aipsi.org/ (M. R.A. Bozzetti)
0000-0001-8074-8980 (L. Olivieri); 0000-0003-2973-0384 (F. Spoto)

and 4 report a detailed discussion of the collected data and observed trends. Finally, Section 5 concludes by underlying the importance of a cybersecurity culture focused on the Italian reality.

2. Digital Attacks Observatory

The *Digital Attacks Observatory* (OAD) [4] is the only independent online survey in Italy about intentional digital attacks on IT systems of companies and public bodies. It is implemented in collaboration with the Italian Postal and Telecommunication Police. The last OAD 2020 was the twelfth year of consecutive surveys on cyberattacks in Italy. The OAD survey is not directed at a predefined set of respondents, but allows potential interested parties to have full and free access to an online questionnaire, in a totally anonymous way. The survey has collected responses from 310 enterprises in 2020, in comparison to 296 and 2019 and 269 in 2018. Thanks to the number of responses collected and their balanced distribution between companies and public bodies of different size, belonging to different economic sectors, and different geographical areas, we can provide now a specific picture of the cyberattacks in Italy.

2.1. The Questionnaires

About half of the OAD questionnaires refer to the occurred cyberattack typologies and their main characteristics. The other half refers to the technical and organizational security measures implemented on the IT systems of the respondents. Therefore, OAD allows one to match the cyberattacks to the cyber-measures in each production IT system considered. In fact, OAD provides a qualitative macro-evaluation of the implemented measures (within the specific context of the company), in order to motivate the anonymous respondents to complete the questionnaires. In particular, the security measures considered in the 2020 questionnaire were subdivided in *technical*, *organizational*, *managerial* and *governamental*, as follow:

1. *Technical measures*
    - Overall architecture of the digital security measures, integrated with the entire IT system architecture
    - Physical countermeasures
    - Identification, Authentication, and Authorization (IAA) measures
    - Cybersecurity measures at local and geographical network level
    - Measures for logical protection of each single Information and Communication Technology (ICT) system
    - Application and software protection
    - Data protection
2. *Organizational measures*
    - Organizational structure, roles, skills, certifications
    - Organizational policies and procedures
    - Contracts, agreements and digital security clauses with third parties
    - Awareness and culture of digital security at all levels
    - Auditing
3. *Managerial and governmental measures*
    - Digital security control, monitoring and management systems
    - Disaster Recovery (DR) plan.

2.2. Overview from 2019 to 1Q-2020

The OAD 2020 survey [1] [5] took place during the Covid-19 pandemic and covered the entire 2019 and the first quarter of 2020, when the pandemic exploded in Italy. The comparison of data

[1]The report is written in Italian, only the Executive Summary is in English: 186 A4 pages, 148 images and graphics, 11 Chapters (147 A4 pages) and 9 Attachments (39 A4 pages).

from 2019 to that from the first quarter of 2020, provided by the same set of respondents, has statistical relevance and provides a clear indication of the Covid-19 pandemic on the intentional cyberattacks in Italy. This pandemic has triggered a wide range of cyberattacks, mainly caused by the sudden, and partly unexpected, passage to working from home and to a strong use of every type of IT service on the Internet, as a consequence of the mobility lockdowns imposed by the Italian authorities. The resulting respondents pool covers all the production sectors (Fig. 1), including public administration, even if the majority of the respondents companies belong to the ICT sector (30.8%). However, many of them are represented by low percentages. For this reason, missing sufficiently representative samples, we have not performed a particular data analysis and correlations by sectors. The 2020 pool is well balanced for the size of the organizations, in terms of employees, between those below 250 and the largest ones. It must be taken into account, as reported by ISTAT [6], that 99.91% of enterprises in Italy are SMEs, with up to 250 employees, and 95% have fewer than ten employees. The OAD 2020 survey is therefore able to consider small and tiny organizations, that are the vast majority in Italy, and that usually are not considered in other cybersecurity surveys: 57.5% of the OAD 2020 respondents belong to structures with less than 250 employees and, of these, 22.1% have fewer than ten employees. The distribution of annual respondents' turnover also reflects the turnover of SMEs, as shown in Fig. 2. Regarding geographical distribution (Fig. 3), the respondents' companies and organizations are mostly located in the Italian territory (77.9%), predominantly in northern Italy (43.3%).

3. Discussion

The data collected in the OAD 2020 show, in general, that the respondents have, for the most part, a good perception of the cybersecurity of their IT systems (Fig. 4). This information can be explained from the fact that:

- About 30% of respondents are in the ICT sector, therefore their IT systems are managed with some cybersecurity literacy and can properly react to cyberattacks, preventing them or minimizing their effects.
- In general, cybercriminals do not waste time and resources to attack small businesses, where they can only obtain a marginal profit and still take the risk of being caught by the police. As confirmed by the trends shown in Fig. 6 and Fig. 7, attackers target the larger companies most, because the illegal gain is more interesting in that case.

The chart in Fig. 5 analyzes the trend of cyberattacks. The figure shows that, from 2007 to 2015, in average, about 40% of the respondents reported cyberattacks (leftmost full red line). Since 2015, the trend increased to 45% of the respondents (rightmost full red line). In 2018, OAD reached the peak of reported attacks and, for the first time, the percent of reported attacks became larger than that percent of companies that did not report any attack. After the peak in 2018, year 2019 has a lower figure and the same occurs in the first quarter of 2020. The trend for full 2020 will be discovered with the currently ongoing OAD survey. This view, over several years, does not show significant changes, not even inside the pandemic period, but shows only a slight increase in cyberattacks in the recent years, not necessarily attributable to the pandemic

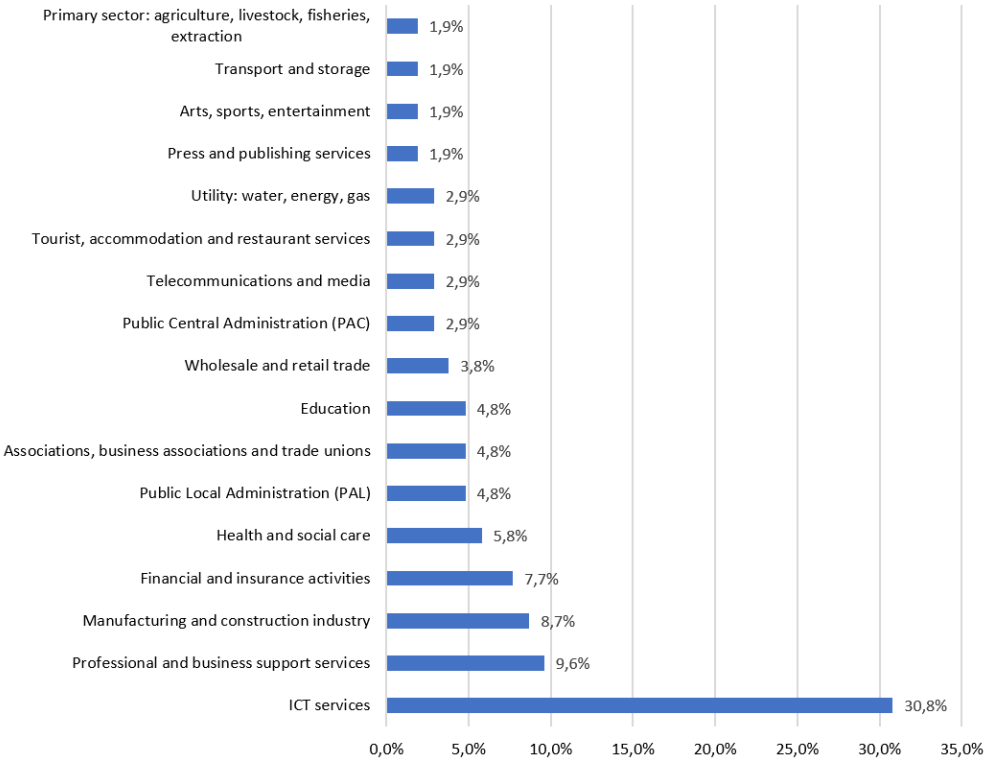

Figure 1: Product breakdown of the respondents' companies and organizations [5].

crisis. One could wonder why the percentages in Fig. 5 are lower than what the reader would have expected, given the numerous cyber attacks occurred in Italy. As already discussed at the beginning of this section, the main reason seems the size of the Italian companies.

The comparison between the whole 2019 and the first quarter of 2020 in Fig. 6 maintains the same logical trend. The only meaningful difference is in the number of attacks reported by the smallest organizations (up to ten employees): they were 0% in 2019 and grow up to 22,2% at the beginning of 2020 (see the red arrow in Fig. 6). Such a strong increase follows from the extensive use of e-banking and e-commerce services, with the related cyberattacks.

Regarding the geographical distribution of attacks, Table. 1 shows that occasional attacks were evenly distributed throughout the territory in 2019, with systematic attacks focused on northern Italy (where the companies with the highest turnover are present). While Table. 2 shows that, already in the first months of 2020, there were several attacks.

The impact of the pandemic on the cybersecurity in Italy is also highlighted by the data provided by the Italian Postal and Telecommunication Police, that shows the situation for the critical infrastructures (Table 3), for the financial cyber-crimes (Table 4) and for the cyber-terrorism (Table 5). Fraudulent transactions were blocked in all Italy in 2019 for a total value of €21.3 million and €18 million were recovered; in the first quarter of 2020, fraudulent transactions for €20.2 million were blocked, practically reaching in four months the amount blocked in the full twelve months of 2019, and €8 million have been recovered. This is an indication

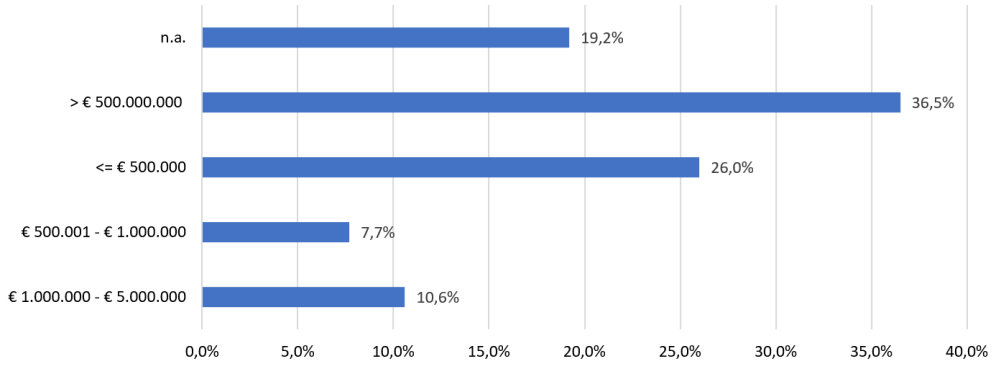

Figure 2: Last annual available turnover of respondents' companies and organizations [5]. It should be noted that almost 20% of the respondents cannot or do not want to provide the turnover class to which they fall, asserting that the confidentiality policies prevent them from indicating a turnover class, even in an completely anonymous investigation.

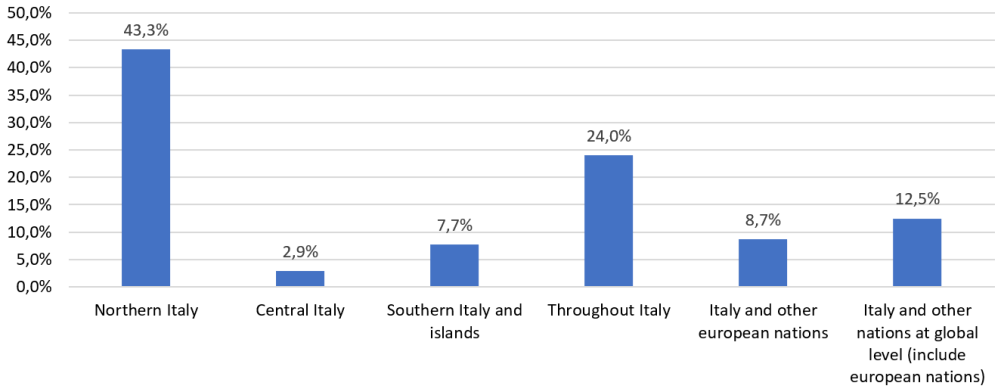

Figure 3: Geographical coverage of the companies/organizations of respondents [5].

of the increase in attacks on financial transactions and services due to the very large use of these online services, caused by the mobility reduction measures consequent of the Covid-19 pandemic.

4. Nature of Cyberattacks

In the pandemic period, between 2019 and the first quarter of 2020, the nature of the attacks and their vectors were quite diversified. The attacks on IAA that aimed at access control systems are widespread, since they amount to 28.2% of the total attacks of 2019 and to 34% of the total attacks in the first quarter of 2020 (Fig. 8).

The other 14 types of attacks follow, decreasing by a few percent points between them, whose characteristics and impacts are detailed in the related paragraphs of the OAD 2020 report. Regarding attack vectors and techniques, all the seven attack families considered in the 2020

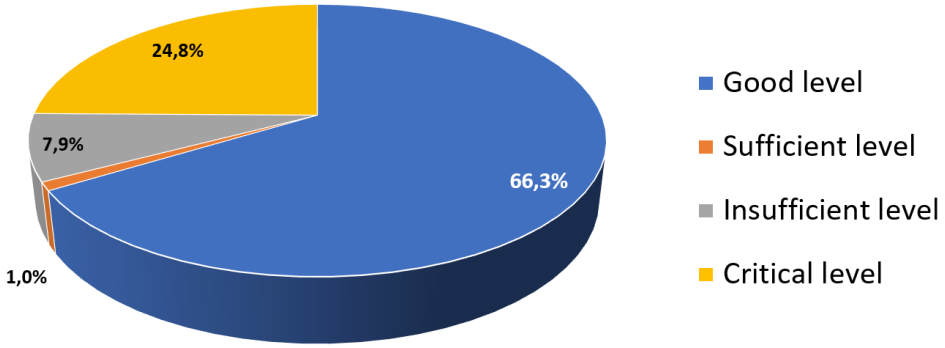

Figure 4: Extract of the OAD 2020 [5] on the macro-evaluation of the security level in the IT systems in Italy. The chart shows that more than two thirds of the respondents judge the level of cybersecurity of their IT systems as good.

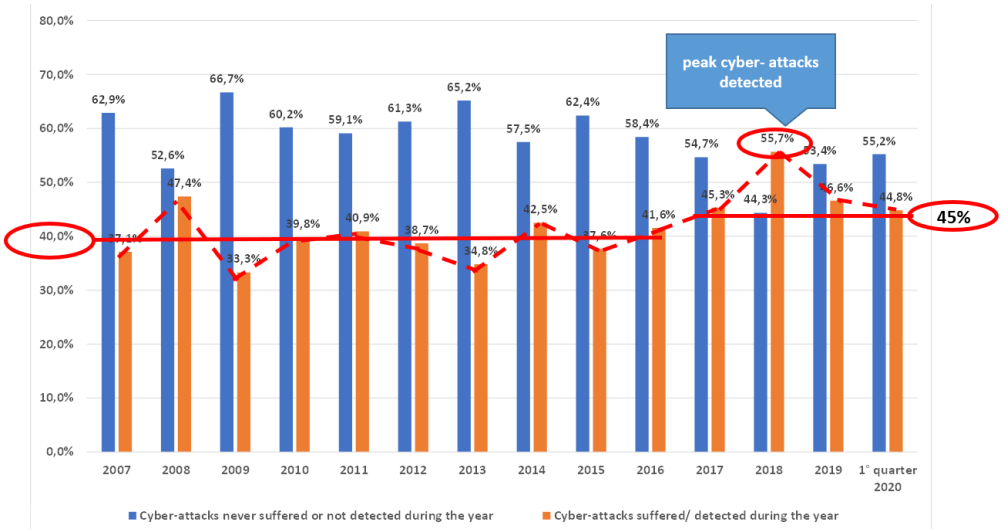

Figure 5: Trend of the reported attacks from the beginning of the OAD survey in 2008 [5]. This comparison is only valid as a trend and not as a statistical measure, since the respondents are different from year to year. The dotted red line shows successive waves: after a relative peak of attacks, companies react and strengthen their cybersecurity measures, so that, the following year, the trend decreases.

questionnaire are widely used in the various types of attacks, sometime even simultaneously, as shown in Fig. 9. The trend in Fig. 9 is also in line with most European reports, such as that of the European Network and Information Security Agency (ENISA) [7]. The most widespread one, in the average of the various attacks detected by the respondents, is the use of toolkits (rootkits, meta-exploits, etc.) for the identification and exploitation of vulnerabilities on the target system, with 38.8%, followed by the well-known malicious and unauthorized collection of information (social engineering, phishing, etc.), with 34.6%, and the use of malicious code and scripts, with 34.3%. The other considered techniques decrease, with a few percent points

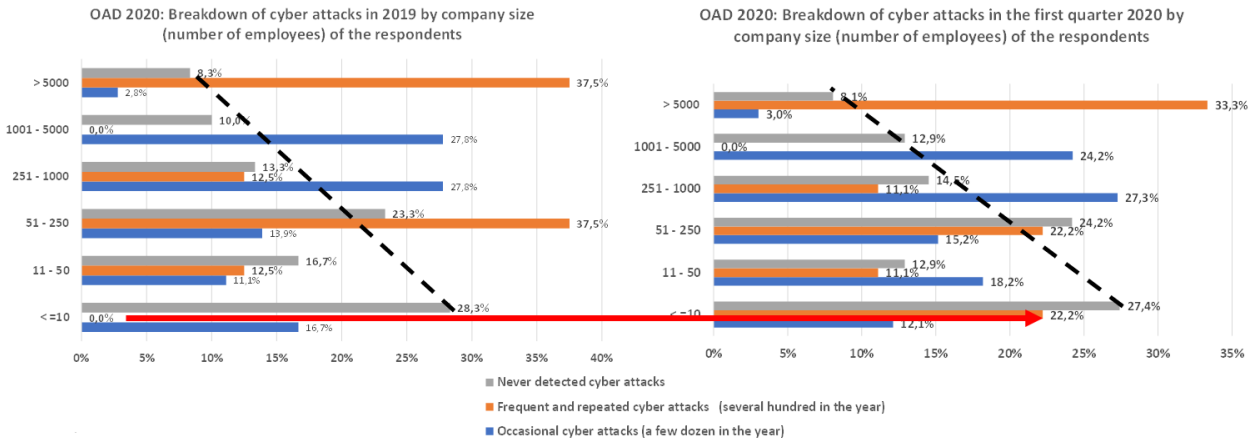

Figure 6: Comparison between cyberattacks occurred in 2019 and in the first quarter of 2020, wrt. the organization dimension [5]. The dotted line links the unreported attacks and shows that they decrease while moving from tiny to big organizations, in terms of employees.

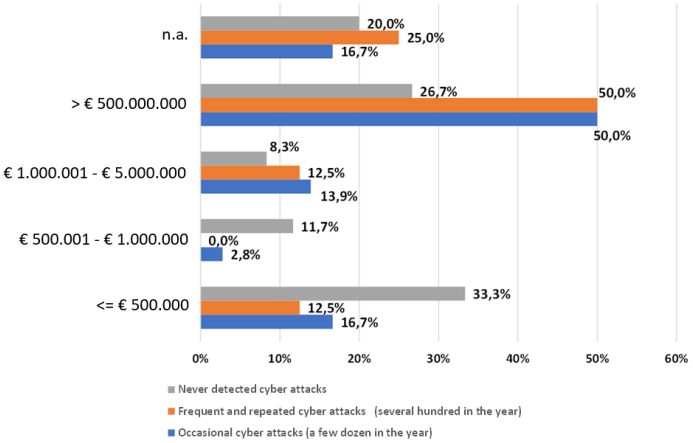

Figure 7: Trend of the reported attacks wrt. the organizations' turnover in 2019.

between them. The impacts of the most critical attacks are analyzed, for each attack type, as well as their possible motivations and the recovery time required by the most critical ones. In the 2020 OAD survey, all these attack characteristics vary for each type of attack, and the emerged results are described in the specific paragraphs dedicated to each attack type. In the overall, it emerges that:

- the impacts declared by the respondents are balanced between those irrelevant and/or easily resolvable with a quick recovery and at limited costs, and those very critical, that require expensive and long recovery actions and that, in some cases, can cause business and customer losses. These two very different impact cases depend mainly on the security

Geographic area	Occasional cyber attacks (few dozen in the year)	Frequent and repeated cyber attacks (hundreds or more in the year)	Never detected cyber attacks
Northern Italy	76,3%	18,0%	5,7%
Central Italy	46,5%	0,0%	53,5%
Southern Italy and islands	80,8%	0,0%	19,2%
Throughout Italy	100,0%	0,0%	0,0%
Throughout Italy and Europe	58,8%	0,0%	41,2%
Throughout Italy and abroad (also outside Europe)	100,0%	0,0%	0,0%

Table 1
Distribution of digital attacks (detected by the respondents) wrt. geographical area, in 2019. The percentages of central Italy are very different from the others because the organizations responding from that geographical area were much fewer than the rest of the survey participant (Fig.3).

Geographic area	Occasional cyber attacks (few dozen)	Frequent and repeated cyber attacks (hundreds or more)	Never detected cyber attacks
Northern Italy	5,8%	6,3%	87,9%
Central Italy	0,0%	0,0%	100,0%
Southern Italy and islands	0,0%	0,0%	100,0%
Throughout Italy	30,3%	0,0%	69,7%
Throughout Italy and Europe	0,0%	0,0%	100,0%
Throughout Italy and abroad (also outside Europe)	28,8%	0,0%	71,2%

Table 2
Distribution of digital attacks (detected by the respondents) wrt. geographical area, in 1Q-2020.

Critical structure protection	1 Jan - 30 Apr 2020	1 Jan - 31 Dec 2019	1 Jan - 31 Dec 2018	1 Jan - 31 Dec 2017	1 Jan - 31 Dec 2016
Relevant attacks	282	1.181	459	1.032	844
Issued alerts	24.824	82.484	80.777	31.524	6.721
Initiated investigations	34	155	74	72	70
People arrested	0	3	1	3	3
People reported	0	117	14	1.316	1.226
Perquisitions	n.a.	n.a.	n.a.	73	58
Initiated investigations	12,05%	13,12%	16,12%	6,98%	8,29%
People arrested out of reported	0%	2,5%	7,14%	0,23%	0,24%

Table 3
Data of critical structure protection collected by Italian Postal and Telecommunication Police [5].

measures in place;

- the motivations of the cyberattacks are mainly economic, such as fraud and blackmailing: the widespread diffusion of ransomware in Italy is a clear confirmation of these motivations.

As pointed out in Fig. 4, the IT systems considered in the 2020 survey and their cybersecurity are in the medium to high range and the collected information shows a relevant improvement in both technical and organizational measures, in comparison to the previous surveys. Few of the considered Italian IT systems are based on data centers in Italy: most of the respondents' companies have medium to small IT systems partly on premise and partly outsourced, with an increasing use of cloud services. The high number of attacks detected in 2018, and the privacy obligations related to the European General Data Protection Regulation (GDPR), have

Financial Cyber Crime	1 Jan - 30 Apr 2020	1 Jan - 31 Dec 2019	1 Jan - 31 Dec 2018	1 Jan - 31 Dec 2017	1 Jan - 31 Dec 2016
Blocked fraudulent transactions	**€20.200.000,00**	**€21.333.990,00**	€38.400.000,00	€20.839.576,00	€16.050.812,50
Recovered amounts	€8.700.000,00	€18.000.000,00	€9.000.000,00	€862.000,00	n.a.
People arrested	n.a.	n.a.	n.a.	25	25
People reported	n.a.	n.a.	n.a.	2.851	3.772
Recovered amounts out of fraud	12,05%	13,12%	16,12%	6,98%	8,29%

Table 4
Data of critical structure protection collected by Italian Postal and Telecommunication Police [5].

Cyber-terrorism	1 Jan - 30 Apr 2020	1 Jan - 31 Dec 2019	1 Jan - 31 Dec 2018
Monitored web space	€11.962	€36.377	€36.000
Removed contents	n.a.	n.a.	250

Table 5
Data of cyber terrorism collected by Italian Postal and Telecommunication Police [5].

certainly contributed to strengthening cybersecurity measures, and a further improvement comes from the growing use of cloud services, where high standard security measures are in place, usually. Organizational measures for cybersecurity, historically missing and neglected in Italy, have improved in terms of definition of roles and separation of duties, of organizational policies and procedures, and of incident management. These measures often are missing in small organizations, and in general the cybersecurity awareness and competence are low, and mainly concentrated at the top level of the public and private organizations. In Italy, there is still a long way to go in terms of cybersecurity continued training and awareness. A formal and bureaucratic approach to the organizational procedures is still prevalent. Once defined, such procedures often do not find concrete application and misses periodic updates and operational tests. A significant example is the disaster recovery plans, for which, typically, the required alternative IT resources are neither forecast nor allocated. Periodic exercises and simulations of the possible disasters are not implemented. Cybersecurity management tools have limited diffusion yet, among the 2020 OAD respondents. This is particularly true for the most advanced ones, based on artificial intelligence. Although the use of IoT [8], industrial automation, robotics systems [9] and systems based on blockchain technology [10] are expanding and can contribute to fight the Covid-19 pandemic. In the OAD 2020 report, one finds only a few respondents involved in such technologies, which also derives from the limited portion of their economic sector, interested in such systems: the manufacturing sectors, the logistics, the research and development centers and labs, the local public administration for territorial control, and so on.

5. Conclusion

The OAD 2020 survey highlights the presence of cyberattacks of various types in Italy, all technically of an high complexity and sophistication, with a slight increase compared to the trend that emerged in the twelve years of the previous OAD surveys, but still below the peak of 2018. Despite the proliferation of cyberattacks related to the Covid-19 pandemic, in the first

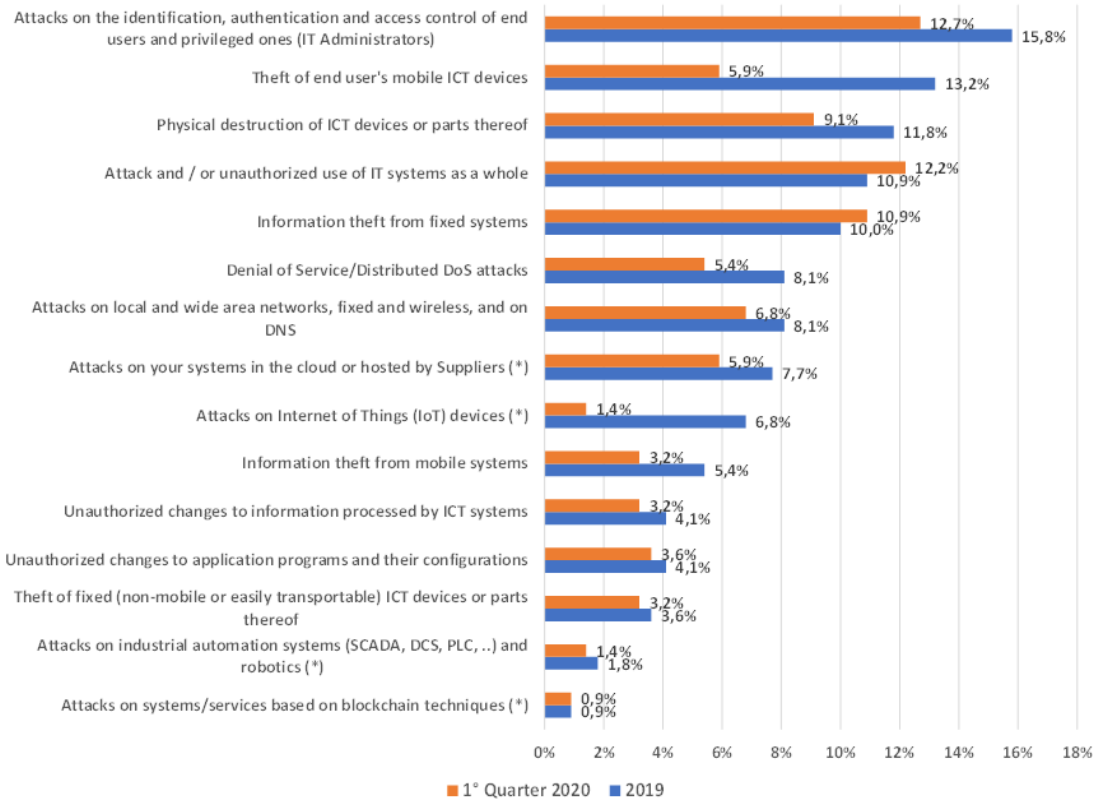

Figure 8: Widespread of the digital attacks on the respondents' computer systems, classified wrt. the type of attack, between 2019 and the first quarter of 2020 (multiple answers) [5]. Where marked with (*), we note that not all the IT systems of the respondents use these types of solutions/systems.

four months of 2020 the widespread of attacks is at a level similar to that of 2019. This will be better verified with the next OAD 2021. The Italian reality, made up of a very large number of small and tiny organizations, does not make our country very attractive to cybercriminals, but cyber-warfare and massive attacks represent a growing and serious risk, as has already occurred with the widespread of ransomware on computer systems with no or low measures of cybersecurity. The OAD 2020 shows a clear improvement and strengthening of digital security measures, both technical and organizational, even if the most modern prevention, protection and management systems that use artificial intelligence techniques are still in their infancy among the respondents. The defense measures and techniques in use fight the increasingly sophisticated and smart evolution of attacks, but often too late. The high density of vulnerabilities requires different approaches, aiming at making all IT systems interconnected to the Internet and safe, by default and by design. However, we are still a long way from this goal. In order to improve the actual fight against continuous attacks and cybercrime, it is currently necessary to increase awareness on cybersecurity and skills at all levels. It is also paramount to support an effective collaboration between police bodies at the international level.

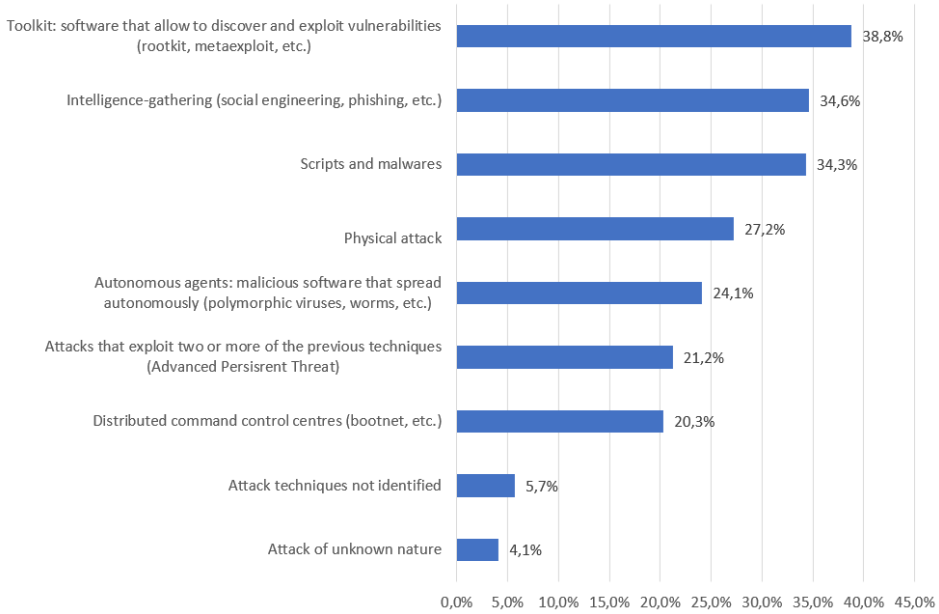

Figure 9: Average diffusion (in percent) of the attack techniques detected in the most serious attacks between 2019 and the first quarter of 2020 (multiple answers) [5].

References

[1] L. Goasduff, Covid-19 accelerates digital strategy initiatives, Gartner (2020).

[2] S. Hakak, W. Z. Khan, M. Imran, K. R. Choo, M. Shoaib, Have you been a victim of covid-19-related cyber incidents? survey, taxonomy, and mitigation strategies, IEEE Access 8 (2020).

[3] B. Pranggono, A. Arabo, Covid-19 pandemic cybersecurity issues, Internet Technology Letters 4:e247 (2021).

[4] O. Team, Digital Attacks Observatory Webpage, 2020. https://www.oadweb.it/en/.

[5] O. Team, Digital Attacks Observatory 2020 Survey, 2020. https://www.oadweb.it/en/oad-2020/to-download-the-oad-2020-report.html.

[6] I. Istat, Enterprises and persons employed, dataset DICA_ASIAUE1P, 2021. http://dati.istat.it/Index.aspx?DataSetCode=DICA_ASIAUE1P&Lang=en.

[7] E. Network, I. S. A. (ENISA), Threat Landscape 2020 - List of top 15 threats, 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats.

[8] M. Javaid, I. H. Khan, Internet of things (iot) enabled healthcare helps to take the challenges of covid-19 pandemic, Journal of Oral Biology and Craniofacial Research 11 (2021) 209–214.

[9] Y. Shen, D. Guo, F. Long, L. A. Mateos, H. Ding, Z. Xiu, R. B. Hellman, A. King, S. Chen, C. Zhang, H. Tan, Robots under covid-19 pandemic: A comprehensive survey, IEEE Access 9 (2021) 1590–1615.

[10] L. Riccia, D. D. F. Maesab, A. Favenzac, E. Ferro, Blockchains for covid-19 contact tracing and vaccine support: a systematic review, IEEE Access (2021).