Article

Wilfried Martens Centre for European Studies

European View
2021, Vol. 20(2) 140–149

DOI: 10.1177/17816858211059250
journals.sagepub.com/home/euv
SAGE

Cybersecurity post-COVID-19: Lessons learned and policy recommendations

Iva Tasheva

Abstract

This article looks at the impact of the novel coronavirus crisis and increased remote work on cybersecurity and the priorities for EU action. Actions should include improving the cybersecurity of businesses, critical infrastructure and users, and creating an EU cybersecurity industry. As more and more aspects of our lives happen online, we are becoming more vulnerable to malicious attacks. This was demonstrated in 2020 when cyber-attacks increasingly disrupted the work of hospitals, service providers, government services and businesses across the globe. The frequency and scale of the attacks created a sense of urgency to improve our cybersecurity resilience. This article argues that the EU should reap the benefits of cybersecurity by pursuing a more ambitious cybersecurity agenda and putting EU values at the core of its approach. It also calls for cybersecurity to be included in all EU pillars, including the EU industrial research and innovation policy, as well as in EU investment plans and diplomatic strategy.

Keywords

EU, Cyber, Security, Policy, Privacy, COVID-19, Democracy, Diplomacy

Introduction

The novel coronavirus (COVID-19) pandemic hit the world in March 2020, changing how we live, work and communicate. Social distancing and working from home became the norm. In Europe, as in most of the world, everything had to be digitalised to continue government, social and economic activities. Digitalisation was already a trend, but the arrival of COVID-19 caused it to happen overnight. Thus, the security of our

Corresponding author:
Iva Tasheva, CYEN, Avenue Paul Hymans 121, Brussels, 1200, Belgium.
Email: iva.tasheva@cyen.eu

government, businesses and citizens, which had been developed over the centuries, became a matter of cybersecurity in just a few months.

During 2020 the intensity and scale of cyber-attacks increased. Malicious actors exploited our fears linked to the health crisis, sending fake COVID-19 updates and alarming phishing messages to collect user information or install malware on users' devices. The many new Internet users were not prepared for this threat, and nor had they been instructed on how to face it. Estimated global losses from cybercrime in 2020 hit a record of just under $1 trillion (Malekos Smith and Lostri 2020). If measured as a GDP and compared with national economies, cybercrime turnover would rank thirteenth in the world right now (between Indonesia and Turkey). With everyone and everything now online, opportunities for attacks have increased. This and increased activity by malicious actors have made cybersecurity even more challenging to achieve. Naturally, therefore, integrating cybersecurity into all aspects of life, including remote work, has been an uphill battle.

This article, while presenting the current state of play, aims to define the opportunity that cybersecurity holds for Europe. It focuses on analysing the multiple facets of cybersecurity and the factors that play a role in achieving it, including the impact of the COVID-19 crisis and increased remote working. It argues that the EU should pursue a more ambitious cybersecurity agenda with the Union's values at the core of its approach, and calls upon policymakers to integrate cybersecurity into the EU's industrial innovation and research policy, as well as investment policies and diplomatic strategy. Finally, the article provides actionable policy recommendations for policymakers to help realise the opportunity that cybersecurity presents for the EU.

Cybersecurity during COVID-19

During the first three months of the pandemic, information and communication technology (ICT) teams everywhere worked around the clock to deliver digitalisation projects that, under normal circumstances, would have taken years to put in place. They had to implement the basics of remote work: creating large-scale remote connections, and ensuring sufficient portable devices and network capacity to make it all work. They also had to integrate collaborative solutions, such as virtual meeting rooms and information management solutions (i.e. the cloud and cloud-based applications), to ensure that the quality of services could be maintained. Despite the short time frame, all these solutions also needed to work securely (i.e. protecting the confidentiality, integrity and availability of data they processed). Integrating cybersecurity into processes, products and services is necessary to protect users, in a similar way to how security and safety are expected in the physical world, for instance, when using vehicles, roads, postal services, clothing and domestic appliances.

However, in an emergency digitalisation situation it is very difficult to ensure the security of systems. Ensuring security requires an analysis of the risks and mitigating measures, implementation planning, the integration of all processes, the use of expertise

and the education of users. All of these are continuous processes and adaptations, which could not happen overnight despite the sense of urgency. Cybersecurity, or the lack of it, became one of the key issues and fastest-growing concerns of this emergency digitalisation. Preserving the availability, confidentiality and integrity of the information and systems built so far became key for all business operations. Whether a company was able to stay in business or not began to depend on the security of their operations, people and technology. One cyber-attack could take a whole business offline. As well as businesses coming to depend on cyberspace, more data and more sensitive information have also become available online, including (national) security, business and private discussions.

At the same time, the security of the weakest link defines the overall level of cybersecurity, not the individual or average level of security. Data and activities have become more vulnerable than ever due to the low-security maturity of many of the new actors in the digital space, such as local small and medium-sized enterprises (SMEs), public services and employees working online for the first time. Arguably too many new users have come online without taking the time to develop proper cybersecurity awareness and hygiene (Fernandez et al. 2020), that is, the knowledge and habits of following basic cybersecurity rules. It has been particularly challenging to integrate security into the massive remote-working transition. There have been constraints due to the limited resources (experts, infrastructure and time) available to bring everyone online. In addition, users were often not prepared for dealing with the security risks during the new and overwhelming pandemic situation. Fear was also a bad adviser for many of them.

SMEs brought their operations and data online too quickly, without security processes, plans or tools in place. Numerous less publicised but still expensive attacks disrupt businesses every day. According to the *UK Cybersecurity Breaches Survey 2021* (UK, Department for Digital, Culture, Media and Sport 2021), 40% of all businesses and 65% of medium-sized businesses (those employing 50–200 persons) have experienced cybersecurity breaches in the last 12 months. Seven underlying cybersecurity issues amongst SMEs have been identified by the EU Agency for Cybersecurity (ENISA), including

- low cybersecurity awareness among staff,
- inadequate protection of critical and sensitive information,
- lack of budget,
- lack of cybersecurity specialists,
- lack of suitable cybersecurity guidelines specific to SMEs, and
- shadow ICT, that is, a shift of the work in the ICT environment out of the SME's control (ENISA 2021).

These are all substantial issues, and dealing with them is basic to achieving any level of security. The second half of the list includes issues that are beyond the power of an

individual SME to rectify, for example, the lack of cybersecurity talent and guidelines, and the shift to ever more complex digital solutions—these are more difficult to control or secure. The EU needs to step in and support member states and SMEs to address these issues.

Finally, critical infrastructure that is vital for society and the economy continues to lag behind in cybersecurity: healthcare facilities, energy grids, food and water supplies, public transport and more. There have been cyber-attacks on hospitals (Irish hospitals were shut down), government services (the Italian COVID-19 vaccination centres were taken down and the Bulgarian National Revenue Agency was the victim of a cyber-attack that resulted in the disclosure of the personal and financial data of the majority of the country's adult population), network management suppliers (SolarWinds) and US oil pipelines (Colonial Pipeline). These cybersecurity compromises have had major impacts on citizens, making cybersecurity everyone's problem. They were enabled by the poor security of the infrastructure and/or the failure of employees to contribute to the security of the systems.

Alongside the security weaknesses of the infrastructure, the low level of cybersecurity awareness and hygiene among users poses a severe risk to security and privacy. Human error is still the top reason for a cybersecurity incident. According to a CybSafe (2019) analysis of data from the UK Information Commissioner's Office, human error was the cause of approximately 90% of data breaches in 2019. This was up from 61% and 87% in the previous two years. Journalists even exploited poor cybersecurity hygiene (weak passwords) to introduce themselves at a secret EU Security Committee by guessing the password of one of the EU ministers present. These factors have created a massive opportunity for cybercriminals to exploit this knowledge and control critical infrastructure in a few clicks. COVID-19 has just made this a reality sooner than expected. Moreover, a hack is easier than we would like to admit. As evidenced by the highlighted attacks, cyber-attacks have the potential to paralyse critical sectors of the economy and society, and arguably, the whole economy.

As a result, the need to act on cybersecurity has arrived at the top of government agendas. In the EU, policymakers have approached the cybersecurity issue in a standard legislative way—that is, with recent agreements for a Cybersecurity Competence Centre and network of coordination centres, a proposal for a revamped EU Network and Information System Security Directive (NIS2), a series of awareness-raising initiatives for SMEs launched by ENISA and the announcement of the Cyber Resilience Act by Commission President von der Leyen in her State of the Union Speech (European Commission 2021b). We also finally saw the first-ever EU cyber sanctions in 2020.

In the US, cyber attribution and sanctions are not a novelty, and the Executive Order on Improving the Nation's Cybersecurity was swiftly signed in response to the abovementioned incidents. A massive plan for increased investment in the cybersecurity of government services followed to support the Executive Order. In addition, the US president called upon the key US digital services companies, including Google, Microsoft,

Amazon and Apple, and the financial services industry, to raise the cybersecurity bar and help create a much-needed cybersecurity workforce.

Lessons learned

For many years, cybersecurity was treated as a niche ICT problem. This is not the case anymore. The COVID-19 pandemic has brought about accelerated digitalisation and helped government leaders, businesses and end-users understand the importance of cybersecurity in building a sustainable digital future. If we are to live up to the high standard of security in our developed society and participate in a growing cyber economy, we need to address cybersecurity as a top priority and act upon it in various policy areas.

In this regard, cybersecurity creates an economic opportunity. Integrating cybersecurity into all aspects of life will provide opportunities for economic growth. The defence of cyberspace is a lucrative business. Cybersecurity expenditure has dramatically increased since the arrival of COVID-19: from $40.8 billion in 2019 to an expected $54.5 billion in 2020. The trend will continue post-COVID, with cybersecurity expenditure forecast at just under $60 billion for 2021 (*Statista* 2021a).

To bring these benefits to Europe, we first need to fix the cybersecurity talent issue. The existence of talent is crucial for the development of value-added sectors, including cybersecurity. With a zero-unemployment rate in the sector, talent is the number one barrier to growth. According to the Cybersecurity Ventures projects, we will end 2021 with an astonishing 3.5 million unfilled cybersecurity jobs globally, with 400,000 of those in Europe alone (Morgan 2019). There is a rapidly growing global skills gap, which has increased threefold since 2014. Statista provides an insight into the skills shortage through a survey, showing that the major gaps are in cloud computing security, security analysis and investigation, application security, and risk and compliance administration (*Statista* 2021b). Collaborative professional education, provided online by a network of EU universities and the private sector (e.g. the Ubiquity University), could help address the need for affordable, cutting-edge, large-scale training schemes for cybersecurity experts and practitioners (Tasheva 2017).

In parallel, we need more cybersecurity solutions to be developed in Europe—eventually supporting the uptake of new European global cybersecurity service providers. To quote Commission President Ursula von der Leyen (European Commission 2021b): ‘It should be here in Europe where cyber defence tools are developed. This is why we need a European Cyber Defence Policy’.

Cybersecurity is part of diplomacy. Cybercrime is by its nature a transborder crime, but we lack the robust rules, institutions and operational cooperation to counter cybercrime at scale. Progress in building common cybersecurity institutions has been made since 2013, with ENISA receiving a stronger mandate to support cybersecurity capacity building and awareness, and the EU Agency for Law Enforcement bringing its Joint

Cybercrime Centre into operation to support member states' law enforcement agencies' operations against cybercrime. These institutions have already helped improve cybersecurity. However, they could be further developed (Tasheva 2017).

We need to expand the circle and engage more member states and third-country partners in fighting cybercrime together. Building EU cybersecurity resilience capacity will not only help us to protect but also support global cybersecurity development. We can leverage the EU's experience in setting globally recognised standards, such as the EU General Data Protection Regulation. An opportunity for this could be the design of the announced EU Cyber Resilience Act, which aims to set a common standard for cybersecurity (European Commission 2021b). Setting the standard for cybersecurity cooperation and defining cyber norms could benefit the global community and sustain the EU's soft power in the post-COVID world. A recent EU Institute of Security Studies report, *International Cyber Capacity Building: Global Trends and Scenarios*, concludes that there is growth in the field of cyber capacity in terms of investment, which is attracting more investment and new donors and depth: initially focused on cybercrime, cyber capacity has gradually expanded to include further areas of expertise, such as critical infrastructure, incident response, public awareness and diplomacy, amongst others. The report sees this growth as a sign that a new field of international cooperation is slowly being formed (Collett et al. 2021).

Cybersecurity is key to preserving human rights and democracy. Personal data were the number one attack target in 2020, with such breaches forming 58% of all data breaches (Verizon 2020). In 2021 personal data moved down to second place, after credential disclosure (Verizon 2021). Therefore, cybersecurity, that is, preserving data confidentiality, is vital for privacy. Furthermore, since COVID-19, most communication, including private conversations and relationships, has moved online. This has made the protection of communication channels and the confidentiality of data more important than ever in order to preserve users' privacy. We have observed, however, that multiple security weaknesses in online communication channels have been exploited, for example hacking Zoom passwords has allowed malicious actors to reveal the details of private meetings and even to take part in such gatherings. Moreover, autocratic government leaders have taken advantage of cybersecurity weaknesses. As revealed by the Pegasus scandal, a malicious code (spyware) developed by a private company was deployed by several autocratic governments, including European member states (Hungary), to intensively surveil the digital communications of their opponents, civil society leaders and even their own families. The spyware was very powerful, with the ability to activate the camera and microphone on demand. All content of messages, calls and agendas, and the GPS coordinates of those targeted by the spyware, were accessible to the attacker. This circumvented all privacy and democracy protection mechanisms, and the information obtained created a major risk for the targets.

Cybersecurity is necessary to ensure the success of democratic processes, such as evidence-based public debate and fair elections. Disinformation is still a major issue when it comes to the COVID-19 public debate. As a result, many have chosen not to

believe in the scientific data, acknowledge COVID-related health risks and/or be vaccinated against the disease (European Commission 2021a).

As for fair elections, we have seen several clear examples of attempts to hack the election process since 2016. Both the EU and the US have been affected by unprecedented election scandals triggered by security incidents—email leaks, spying, and website and infrastructure take-downs (distributed denial-of-service attacks) (NIS Cooperation Group 2018, Annex 1). In addition, there has been mass disinformation during elections (ENISA 2019; Benkler et al. 2020; Council of Europe 2020). However, while intensive cyber-attacks continue to target election processes, we seem to have learned a lesson. In subsequent elections —for instance, those for the European Parliament (2019), and the US (2020) and German (2021) national elections—the national security services have been better prepared and have countered cyber-attacks in time to avoid significant disruptions. Nevertheless, we must evolve and ensure continuous improvement to keep up with the ever-growing threats.

Finally, the way in which we implement cybersecurity also matters for human rights. While having the good intention of protecting data and infrastructure, we should not forget that security needs to work for people and not against them. We should avoid security tools that are too restrictive, abusive or involve mass surveillance. Diversity in the development processes (in terms of gender, race and language) can help us to develop better solutions with fewer discriminatory biases. We should also aim to make cybersecurity more inclusive—it should be affordable and accessible for everyone, not a luxury item available only to the young and the rich. More transparency and solutions are needed to ensure we achieve the above goals.

Conclusions

The massive digital transition has posed cybersecurity challenges on three fronts: there are too many new users online, the digitalisation of SMEs and public services has been too rapid, and the level of cybersecurity resilience in critical infrastructure has been too low. There is significant room for improvement, and the EU has three instruments to achieve this —legislation, research and investment —and the mandate to act. The EU could lead the way in introducing a minimum level of cybersecurity, providing cybersecurity solutions and investment, and supporting and leveraging the capacity of the 27 member states to build true EU cyber resilience.

Europe should act swiftly to capitalise on the growing opportunity to boost the development of its modern cybersecurity industry. Efforts should focus on creating an environment for EU cybersecurity champions by upskilling and re-skilling cybersecurity talent, removing trade barriers and creating local cybersecurity demand.

With European cybersecurity solutions, we can export our values. The ability to protect the human right to privacy, sustain democracy and carry out effective diplomacy all depend on the security solutions we deploy at home and export globally. Setting the

standard for diversity in the development processes (in terms of gender, race and language) could help us to develop better solutions with no discriminatory biases. We should also aim to make cybersecurity more inclusive—it should be affordable and accessible for everyone, not only for the young or the rich.

As well as economic interest, the EU has the chance to deliver the high levels of security expected from its citizens and businesses. For instance, it could invest in increasing the minimum level of cybersecurity for government services, provide SMEs with cybersecurity tools and tax breaks, and fund cybersecurity education and awareness-raising for citizens.

To sum up, these are the key recommendations for EU policymakers' immediate action:

1. Agree on and adopt the ambitious EU NIS2 Directive and the Cyber Resilience Act with no delay. After their adoption, coordinate the transposition of the NIS2 Directive and its enforcement among the member states to ensure timely and effective implementation. Results should be better than in the past (e.g. the transposition of the NIS Directive, which has been ongoing since 2016).
2. Develop democracy, diversity and inclusion standards for cybersecurity tools and services. Encourage the uptake of solutions that correspond with our values through public procurement and societal awareness-raising on the topic.
3. Continue the cybersecurity awareness-raising and hygiene campaigns and translating materials into all EU languages to enable their easy reuse and dissemination in all member states.
4. Engage with major government and private-sector actors on the topic of cybersecurity.

In the medium term, EU policymakers should

1. develop the European cybersecurity industry through providing tax incentives, facilitating the accumulation of public market data, creating cybersecurity demand through legislation and public investment, and supporting the upskilling and re-skilling of talent;
2. support the development of robust cybersecurity rules, institutions and cooperation to counter cybercrime; and
3. lead the debate on global cyber norms and develop globally accepted cybersecurity standards.

References

Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J., & Schmitt, C. (2020). *Mail-in voter fraud: Anatomy of a disinformation campaign*. Berkman Centre

Research Publication no. 2020-6. 2 October. https://ssrn.com/abstract=3703701. Accessed 29 September 2021.

Collett, R., Barmpalious, N., & Pawlak, P. (2021) *International cyber capacity building: Global trends and scenarios*. EU Institute of Security Studies. Luxembourg. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios. Accessed 26 September 2021.

Council of Europe. (2020). Democracy hacked? How to respond? Resolution 2326. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28598&lang=e. Accessed 29 September 2021.

CybSafe. (2020). Human error to blame for 9 in 10 UK cyber data breaches in 2019. 7 February. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/. Accessed 27 September 2021.

ENISA. (2019). *Election cybersecurity challenges and opportunities*. February. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities. Accessed 29 September 2021.

ENISA. (2021). *Cybersecurity for SMEs – Challenges and recommendations*. 28 June. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. Accessed 24 September 2021.

European Commission. (2021a). Fighting disinformation. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_en. Accessed 29 September 2021.

European Commission. (2021b). State of the Union address by President von der Leyen. 15 September. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701. Accessed 27 September 2021.

Eurostat. (2021). ICT specialists – Statistics on hard-to-fill vacancies in enterprises. June. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises. Accessed 26 September 2021.

Euractiv. (2021). Germany probes claims of pre-election MP hacking by Russia. 10 September. https://www.euractiv.com/section/global-europe/news/germany-probes-claims-of-pre-election-mp-hacking-by-russia/. Accessed 29 September 2021.

Fernandez, S., Jenkins, P., & Vieira, B. (2020). Europe's digital migration during COVID-19: Getting past the broad trends and averages. *McKinsey*, 24 July. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages. Accessed 28 September 2021.

Malekos Smith, Z., & Lostri, E. (2020). *The hidden cost of cybercrime*. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf. Accessed 13 September 2021.

Morgan, S. (2019). Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021. *Cybercrime Magazine*, 24 October. https://cybersecurityventures.com/jobs/. Accessed 14 September 2021.

NIS Cooperation Group. (2018). *Compendium on cyber security of election technology, Annex 1*. CG Publication 03/2018, July. https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf. Accessed 29 September 2021.

Statista. (2021a). Areas with biggest shortage of cybersecurity skills within organizations worldwide in 2021, by technology category. https://www.statista.com/statistics/1259502/cybersecurity-skills-shortage-tech-categories-worldwide/. Accessed 29 September 2021.

Statista. (2021b). Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted). https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending. Accessed 14 September 2021.

Tasheva, I. (2017). *European cybersecurity policy: Trends and prospects*. EPC Policy Brief, 8 June. https://www.epc.eu/content/PDF/2017/European_cybersecurity_policy.pdf. Accessed 26 September 2021.

UK, Department for Digital, Culture, Media and Sport. (2021). *Cyber security breaches survey 2021*. 24 March. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021. Accessed 26 September 2021.

Verizon. (2020). *2020 data breach investigations report*. https://enterprise.verizon.com/resources/reports/dbir/2020/dbir-report/. Accessed 27 September 2021.

Verizon. (2021). *2021 data breach investigations report. Results and analysis*. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/. Accessed 7 October 2021.

Author biography

Iva Tasheva *is the co-founder and cybersecurity lead at CYEN, a consultancy. She is a member of ENISA's Ad-Hoc Working Group on Enterprise Security and a board member of the DPO Circle.*