Istituto Affari Internazionali



ISSN 2532-6570

IAI COMMENTARIES 20 | 07 - MARCH 2020

# A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked

by Simona Autolitano

The start of a new political term offers good opportunities to formulate ambitious goals. The incoming European Commission President, Ursula von der Leyen, is no exception, having launched her team under the title "A Union that strives for more".[1]

Looking at the recently proposed digital agenda, numerous policy objectives have been put forward.[2] While ambitious, the programme does not introduce big surprises. Most of the envisioned actions have been strategically initiated in Europe over the past five years – for example, in the field of artificial intelligence and data economy, digital finance, online platforms and education.[3]

Cybersecurity represents the backbone for making "Europe fit for the digital age", as digitalisation and cyber are understood as "two sides of the same coin".[4] In this context, President von der Leyen has already understood the need to increase cooperation and information sharing within and between European

[1] In parallel to its audition before the European Parliament and its subsequent election on 14 July, Ursula von der Leyen put forward the document *A Union That Strives for More. My Agenda for Europe. Political Guidelines for the Next European Commission 2019-2024*, 16 July 2019, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

[2] European Commission, *Commission Work Programme 2020. A Union That Strives for More* (COM/2020/37), 29 January 2020, https://europa.eu/!mM99wr.

[3] For example, in the field of artificial intelligence, the High-Level Expert Group on Artificial Intelligence (AI HLEG) was initiated in 2019. Regarding digital finance, a first action plan on FinTech was adopted in March 2018, highlighting, among other things, the importance of increasing cybersecurity and resilience of the financial system. The "Digital Services Act", which aims to regulate platform companies, builds upon previous Commission initiatives, including, for instance, the public consultations launched in 2015 as part of the review of the e-Commerce Directive, as well as the Code of Practice on Disinformation, launched in 2018. Finally, on education, a first Action Plan was released in January 2018.

[4] Ursula von der Leyen, *A Union That Strives for More. My Agenda for Europe*, cit., p. 13.

*Simona Autolitano is a cyber security professional with experience in the private and public sector, in the field of information security, digitalisation and related issues.*

Commission Directorates, suggesting the development of a "Joint Cyber Unit" at the EU level to favour a more centralised cybersecurity approach. What this initiative actually entails, however, and whether it will help to make institutions more agile and flexible in responding to cyber threats remains to be seen.

Clearly, President von der Leyen still has a long way to go to secure our digital society. Nevertheless, the European Commission does boast some pretty solid pillars: resilience, deterrence and response.

Let us start with resilience.

The concept of resilience dates back to the cybersecurity baselines laid down in the EU's Network and Information Systems (NIS) Directive, adopted in 2016 with a view to boost the EU's overall level of cybersecurity. On this first piece of EU-wide cybersecurity legislation, the new Commission is expected to deliver a first review by 2020.[5]

While the Directive undoubtedly represents a vital step forward for the security of our digital society, it also presents important challenges. The fact that it only requires minimum harmonisation implies that implementation could differ significantly across member states. Secondly, both Annex I and II of the Directive, originally conceived back in 2013, no longer reflect the current threat landscape: which today includes incremental usage and consequent criticality of cloud services, the development of new technologies and more recent threats posed, for example, to our electoral systems.

Resilience also refers to secure products, processes and services. In this context, certifications have become important mechanisms to establish trust in cybersecurity. Certifications can demonstrate that a product or service meets or exceeds minimum standards and can offer significant benefits in efficiency and clarity of information.

With the 2019 Cybersecurity Act, the Juncker Commission aimed to centralise and harmonise the issuing of cybersecurity certificates at the EU level. Nevertheless, as argued by various industry associations, in order for the Cybersecurity Act to pave the way to a Digital Single Market for Europe, future certification schemes will need to be aligned with globally recognised, international standards.[6] Any duplication or contradiction of existing certification schemes could hamper innovation and growth in the Digital Single Market and the development of small and medium enterprises (SMEs) in Europe.

Europe should pay particular attention to SMEs and their role in ensuring resilience of our ecosystem. As part of the recently announced new SME Strategy, Commissioner Thierry Breton should prioritise cybersecurity as an

[5] As stated in the *Commission Work Programme 2020*, cit., p. 4.

[6] DigitalEurope, *Cybersecurity Act Gives Europe a New Framework to Increase Trust in a Digitising World*, 10 April 2019, https://www.digitaleurope.org/resources/cybersecurity-act-gives-europe-a-new-framework-to-increase-trust-in-a-digitising-world.

IAI COMMENTARIES 20 | 03 - MARCH 2020 ISSN 2532-6570

essential pillar given that enhancing Europe's digital leadership and strategic autonomy requires solid and secure foundations.

Resilience also relates to software vulnerability disclosure. As became clear with the WannaCry cyber-attacks back in 2017, governments are playing a central role in the stockpiling and consequent exploitation of software vulnerabilities. In this context, the EU has an important role to play and should provide stronger guidance on this issue to protect the "public core" of the Internet.[7]

One option could be to institutionalise processes at the European level on how software flows are managed and vulnerabilities reported to vendors, in order to increase transparency and accountability for both governments and industries.[8]

In a world that is rapidly being transformed by technology, digital skillsets are more important than ever to ensure resilient societies. A digitally skilled workforce is missing not only in Europe, but also globally. To address the widening digital skills gap and to strengthen Europe's digital strategic autonomy, training and skill investments are needed.[9]

The revision of the "Digital Education Action Plan", mentioned in the recently released Commission Work Programme 2020, should use public-private partnership mechanisms to identify cybersecurity skills that are particularly lacking.

Secondly, collaboration with private actors in delivering executive training could also be considered. In the medium term, governments could develop dedicated university programmes to form and train new personnel on digital issues needed for improved public administration. In this context, Germany has this year launched a new study programme focused on cybersecurity and digital administration, a first step towards developing the future cybersecurity force for the German public administration.[10]

Secondly, deterrence from and responses to cyber-attacks.

Since the launch of the European Cyber Security Strategy in 2013, the External Action Service had started and then gradually expanded a series of "Cyber Dialogues" with a number of countries, including China and the US. Nevertheless, the increasing number of state-sponsored attacks – whether carried out by hacktivists or directly by

[7] One of the new tasks of ENISA, as included in the Cybersecurity Act.

[8] Lorenzo Pupillo, Afonso Ferreira and Gianluca Varisco, "Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenges", in *CEPS Task Force Reports*, June 2018, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges.

[9] European Commission, *Commission Work Programme 2020*, cit., p. 4.

[10] The Federal University of Applied Administrative Sciences, a university for public service at the federal level in Germany, launched a new study programme to develop IT professionals to be employed by the public sector. Details available online: *Studiengang "Digital Administration and Cyber Security" (DACS)*, https://www.hsbund.de/DE/02_Studium/10_Duale_Studiengaenge/53_DACS/DACS-node.html.

IAI COMMENTARIES 20 | 03 - MARCH 2020 ISSN 2532-6570

governments – as well as the fact that countries are increasingly investing in defensive as well as offensive cyber-capabilities, continues to put our society and economy at risk.[11]

Strategic cyber espionage campaigns or militarily motivated cyber-attacks are leading us towards a new era in international relations. Cyberspace is increasingly developing into a war zone, where people are not fighting with weapons, soldiers and bombs, but with bits, malware and botnets. Such realities present new challenges and demands; in particular, on what can be considered responsible state behaviour in cyberspace.

Both the United Nations Group of Governmental Experts (GGE) on Advancing Responsible State behaviour in cyberspace and the 2018 Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), represent ideal fora to advance such discussions. The EU should cooperate with like-minded partners and lead the debate, avoiding that more aggressive states dictate the rules of the game. To achieve a stronger Europe in the world, the EU should certainly play a more active role in such crucial discussions.[12]

Norms alone, however, are not enough to deter cyber-attacks against civilian infrastructures by criminals or nation-states. Back in June 2017, the Council agreed to develop a framework for a joint EU diplomatic response to malicious cyber activities. The "Cyber Diplomacy Toolbox", thus aims to increase the cost of carrying out cyber-attacks and ultimately deter potential aggressors in the long term.[13]

With some delay, a new regulation was finally adopted to implement the 2017 Council decision. Since May 2019, the EU is now able to impose sanctions in relation to cyber-attacks, which constitute an external threat to the EU or its member states. As part of its Common Foreign and Security Policy, the EU is theoretically also able to address and react to cyber-attacks targeting third states or international organisations.[14]

In this context, the EU should focus more attention on third states, supporting the development of necessary capabilities to strengthen their resilience against potential cyber-attacks. To make "a stronger Europe in the world", the forthcoming "EU Security Union Strategy" should consider these aspects closely.[15]

The objectives revealed in the new Commission's programme to make

[11] An overview on recorded cyber capabilities per country is available in the GIP Digital Watch website: *UN GGE and OEWG*, https://dig.watch/processes/un-gge.

[12] Patryk Pawlak et al., "Pathways to Change: Resilience, Rights and Rules in Cyberspace", in *EU Cyber Direct Research in Focus*, June 2019, https://eucyberdirect.eu/content_research/pathways-to-change.

[13] Council of the European Union, *Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions*, 19 June 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox.

[14] Council of the European Union, *Cyber-attacks: Council Is Now Able to Impose Sanctions*, 17 May 2019, https://europa.eu/!yp76kW.

[15] European Commission, *Commission Work Programme 2020*, cit., p. 6-7.

IAI COMMENTARIES 20 | 03 - MARCH 2020 ISSN 2532-6570

"Europe fit for the digital age" are ambitious. Their feasibility will largely depend on how close the cooperation within and between directorates in the European Commission will be. Over the next five years, two Commissioners will primarily be responsible for the digital agenda in Europe.

Commissioner Thierry Breton and Marghrete Vestager will need to work together to ensure the strengthening of the European cybersecurity ecosystem and the creation of a secure digital society. Whether a EU-wide "Joint Cyber Unit" can respond to these needs remains unclear. Certainly, President Ursula von der Leyen will need to speed up information sharing within the Commission itself to move towards implementation of her new and ambitious cybersecurity agenda.

*12 March 2020*



ISSN 2532-6570

ISSN 2532-6570

IAI COMMENTARIES 20 | 03 - MARCH 2020

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*Affarinternazionali*), three book series (*Global Politics and Security*, *Quaderni IAI* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

# Latest IAI COMMENTARIES

Director: Andrea Dessì (a.dessi@iai.it)