NEW TECH IN REVIEW

Computers on Wheels: Automated Vehicles and Cybersecurity Risks in Europe

Marjory S. Blumenthal and Raluca Csernatoni

EU CYBER DIRECT

March 2022

Contents

Disclaimer

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Introduction

As an emerging and disruptive technology, automated vehicles (AVs) are expected to fundamentally change transportation systems and sociomobility in the twenty-first century.[1] If adopted widely, AVs could affect both urban and rural spaces by altering transport dynamics, user behaviours, infrastructure, and logistics – not to mention create a new automotive ecosystem by shifting the makeup of business models, software and manufacturing industries, and skillsets (for example, of software engineers, data scientists, and AI experts). But is this expectation more hype than reality? More importantly, what are some of the concerns, risks, and security vulnerabilities associated with AVs and their uptake in the transportation systems of tomorrow?

AVs present a worthwhile case study for European and other policymakers seeking to understand the contexts of cybersecurity challenges.

The benefits of AVs are often painted in positive and techno-solutionist[2] terms, namely that the technological solution AVs represent could predominantly solve the complex problem of road safety and, for instance, help achieve the EU's "Vision Zero"[3] goal to dramatically reduce traffic injuries and deaths. Yet AVs illustrate how cyber-physical systems,[4] AI, and the Internet of Things will present new and complex multirisk profiles. In particular, like other technologies that use AI, AVs are vulnerable to cyber attacks that could compromise their proper functioning. AVs also present challenges for safe[5] mobility that arise from or aggravate cybersecurity vulnerabilities. As such, they present a worthwhile case study for European and other policymakers seeking to understand the contexts of cybersecurity challenges.

The cybersecurity, safety, and other risks associated with AVs pose important governance challenges for various stakeholders, including the EU. A recent regulation[6] by the United Nations Economic Commission for Europe – on "cyber security and cyber security management system" – highlights how stakeholders can coordinate their efforts in crafting governance mechanisms to manage AV cybersecurity risks. The regulation aims to set the future framework for vehicle cybersecurity in many parts of the world. The EU is planning to make the regulation's requirements mandatory for the approval of new vehicle types by July 2022[7] and to extend it to existing architectures by July 2024. This article examines the nature and evolution of AVs, options for steering AV development, and recent EU AV governance measures. It offers a guide to minimising cybersecurity and other risks to maximise eventual AV benefits in Europe and elsewhere.

---

[1] Kassens-Noor, Eva, *et al.* (2020) Sociomobility of the 21st century: Autonomous vehicles, planning, and the future city. *Transport Policy* 99: 329-335.

[2] Madrigal, Alexis C. (2013) Toward a Complex, Realistic, and Moral Tech Criticism. The Atlantic, 13 March. Available from: https://www.theatlantic.com/technology/archive/2013/03/toward-a-complex-realistic-and-moral-tech-criticism/273996/.

[3] European Parliament (2021b) Report on the EU Road Safety Policy Framework 2021-2030 – Recommendations on next steps towards 'Vision Zero'. Committee on Transport and Tourisms. Available from: https://www.europarl.europa.eu/doceo/document/A-9-2021-0211_EN.html.

[4] UC Berkley (2022) Cyber-Physical Systems. Available from: https://ptolemy.berkeley.edu/projects/cps/.

[5] Blumenthal, Marjory S., *et al.* (2020) Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA569-1.html.

[6] United Nations Economic Commission for Europe (UNECE) (2021b) UN Regulation No. 155 – Cyber security and cyber security management system, 4 March. Available from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[7] Lovells, Hogan, and Manuel Golling, Sebastian Polly (2022) New cyber security and software update rules in the automotive industry in 2022. JDSUPRA, 12 January. Available from: https://www.jdsupra.com/legalnews/new-cyber-security-and-software-update-1512229/.

Understanding AVs

But what are AVs? The SAE – formerly named the Society of Automotive Engineers and one of the industry's most-cited sources for defining and labelling the degrees of driving automation – currently describes six levels of driving automation,[8] ranging from Level 0 (no driving automation) to Level 5 (full driving automation). The SAE uses the term "automated" instead of "autonomous," in recognition that humans have a role in deciding where a vehicle is supposed to go and what it is supposed to do. The SAE's taxonomy references the specific roles played by three primary actors: the human user, the driving automation system, and other vehicle systems sharing the roadway. At Level 5, a fully automated car could make choices in performing the dynamic driving task, without human supervision. It would follow orders and then drive itself, using technology to perceive its environment and to plan and execute the driving. While an AV can drive itself in at least some situations, for the foreseeable future a human must always be ready to retake control (a challenge when even low levels of automation induce[9] complacency).

AV Risks Arise From Software and Other Defining Technology

The steady rise of computation in conventional cars through the latter part of the twentieth century made them vulnerable to cybersecurity attacks,[10] setting a baseline for today's concerns. No longer just one-purpose devices – providing transport from one place to another – vehicles are fast becoming functional assets and multipurpose platforms.[11] Accordingly, the share of value added to the vehicle by original equipment manufacturers (OEMs) is shifting in favor of software relative to hardware. And this shift is requiring more software competencies, agile development, and newer engineering approaches (perhaps epitomised by Tesla).

AVs' emerging hyper-dependence on software and on external communication – for example, for software updates and maintenance monitoring – feeds new concerns about cybersecurity for vehicles in general and AVs in particular. Compared to conventional cars, AVs are software-driven products. Cybersecurity risks are significant even at low, partial levels of automation, such as for automated parking.[12] Inadequate cybersecurity could allow malicious actors to take control of or shut down a vehicle, direct an AV to relocate itself, or target equipment connected with AVs by networks, such as cameras and traffic signals.

Automated vehicles' use of AI,[13] especially machine learning (ML) techniques, adds to these cybersecurity challenges. AVs use AI for interpreting large amounts of data generated by their cameras and sensors, recognising traffic signs and road markings, detecting other vehicles in traffic and other environmental features, planning the path ahead, and so on. But while AI is used to help improve safety and fuel efficiency, it introduces new risks for system error, such as mistakes in perceiving what is in the environment. And some of these errors could be induced by malice – for instance, by slightly modifying street sign graphics or using so-called

---

[8] Society of Automotive Engineers (SAE) (2021) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. J3016_2-2104, 30 April. Available from: https://www.sae.org/standards/content/j3016_202104/.

[9] Gross, Andrew (2019) Long-Term Use od Advanced Driver Assistance Technologies Can Result in Disengaged Drivers. NEWSROOM, 17 December. Available from: https://newsroom.aaa.com/2019/12/long-term-use-of-advanced-driver-assistance-technologies-can-result-in-disengaged-drivers/.

[10] Koscher, Karl *et al.*, (2010) Experimental Security Analysis of a Modern Automobile. *IEEE Symposium on Security and Privacy*, 2010, pp. 447-462, doi: 10.1109/SP.2010.34.

[11] Deloitte (2019) Autonomous Driving: Hype or Reality? Available from: https://www2.deloitte.com/be/en/pages/consumer-industrial-products/articles/autonomous-driving.html.

[12] Wimerskirch, André, and Derrick Dominic (2018) Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles. University of Michigan, 1 January. Available from: https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf.

[13] ENISA (2021) Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. ENISA and JRC, 11 February. Available from: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/.

adversarial images,[14] which are crafted to mislead ML systems, compromising their use of machine vision and leading to dangerous situations.

Addressing AI's vulnerability to spoofing – deceptive representation through adversarial images and other mischief – and other attacks will therefore be fundamental to AV cybersecurity. And because AI depends on large amounts of data, fears about privacy, as well as data retention and ownership and its potential contribution to surveillance, may feed distrust of AVs.

The Commercial Dimensions: AVs and Their Risks Reflect Market Dynamics

Europe presents a competitive landscape for AVs. Some analysts anticipate steep growth of the European fully automated (Level 5) vehicle market, which does not yet exist but is expected to garner $191.6 billion by 2030.[15] Vehicles with mid- to high-level automation (Levels 3 and 4) are currently being tested and are expected to be on the market in the 2030s.[16] Technical challenges, regulatory hurdles, and the current semiconductor crisis[17] might make at least the Level 5 forecast highly optimistic.

The European AV market has been dominated by three major OEMs: the Volkswagen Group, the PSA Group (legally known as Peugeot S.A.), and the Renault Group – which together accounted for over 50 percent of the market share in 2018.[18] Other European players active in AV development include BMW Group, Daimler, Mercedes-Benz Group, Volvo, and Fiat Chrysler Automobiles N.V. According to a 2021 study[19] requested by the European Parliament on "The Future of the EU Automotive Sector," European carmakers are jointly pursuing vehicle electrification and automation, with Volkswagen leading the way.

For example, Volkswagen's CARIAD automotive software subsidiary and the multinational engineering and technology company Bosch announced[20] that they will be teaming up to develop software for Level 2 vehicles, enabling hands-free driving in cities and rural areas and on highways. The software is to be implemented in Volkswagen vehicles starting in 2023. In addition, the two companies plan to develop software for Level 3 systems that will, under human supervision, take over driving on highways. Volkswagen has also invested $2.6 billion[21] in AV start-up Argo AI, which has also been working with Ford and both U.S. and European universities[22] to develop Level 4 AVs. Volkswagen's move is indicative of a change in strategy and in the long-term goals of

---

[14] Papernot, Nicolas, *et al.* (2017) Practical Black-Box Attacks against Machine Learning. Cornell University. Available from: https://arxiv.org/abs/1602.02697.

[15] Research and Markets (2019) Europe Autonomous Car Market Research Report: By Vehicle Autonomy, Vehicle Type, Application, Regional Insight – Industry Trend, Competition Analysis and Forecast to 2030. Available from: https://www.researchandmarkets.com/reports/4804026/.

[16] European Parliament (2019) Self-driving cars in the EU: from science fictions to reality. Available from: https://www.europarl.europa.eu/news/en/headlines/economy/20190110STO23102/self-driving-cars-in-the-eu-from-science-fiction-to-reality.

[17] Csernatoni, Raluca (2021) Chips geopolitics and EU's new semiconductors sovereignty agenda. EURACTIV, 29 October. Available from: https://www.euractiv.com/section/digital/opinion/chips-geopolitics-and-eus-new-semiconductors-sovereignty-agenda/.

[18] P&S Intelligence (2019) Europe Autonomous Car Market Overview Report. Available from: https://www.psmarketresearch.com/market-analysis/europe-autonomous-car-market.

[19] Brown, David, *et al.* (2021) The Future of the EU Automotive Sector. Study requested by the ITRE Committee, European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695457/IPOL_STU(2021)695457_EN.pdf.

[20] Waldersee, Victoria (2022) Volkswagen and Bosch team up on automated driving software. Reuters, 25 January. Available from: https://www.reuters.com/technology/volkswagen-bosch-collaborate-automated-driving-software-2022-01-25/.

[21] Reuters Staff (2020) Volkswagen closes $2.6 billion investment in self-driving startup ARGO AI. Available from: https://www.reuters.com/article/us-volkswagen-argo/volkswagen-closes-2-6-billion-investment-in-self-driving-startup-argo-ai-idUSKBN2390E6.

[22] Argo AI (2022) About. Available from: https://www.argo.ai/about/.

the car manufacturing industry toward intensifying use of software, increasing automation, and leveraging partnerships. Another example of Europe's progress in vehicle automation is the announcement that Mercedes-Benz is partnering with self-driving sensor maker Luminar Technologies[23] to enable its next-generation vehicles to carry out fully automated driving on highways.

The European Parliament study highlighted the importance of collaboration among European automotive firms – not only to achieve technical progress but also to effectively adapt to digitisation and mitigate the associated costs. But it is not only automotive firms that seek to collaborate and lead the way. Some European collaboration is being born from individual countries' recognition of its value. France, for example, issued an automated mobility strategy[24] that recognises the importance of advancing on a pan-European scale while calling for French leadership within Europe. Germany also conditioned its strategy[25] on AV leadership in Europe. Meanwhile, European companies are working with others on key aspects of AV development, such as testing,[26] where common approaches support the global marketplace. Taking a collaborative approach to AV risks like cybersecurity – building on existing industry attention[27] to it – could facilitate the development of better solutions.

Taking a collaborative approach to AV risks like cybersecurity – building on existing industry attention to it – could facilitate the development of better solutions.

What Is to Be Done?

The traditional automotive industry's approach to software development activities is not sufficient for lowering the risks associated with high levels of automation. Important business culture, technical, and governance changes are needed to assure attention to the full set of risks and their interactions.

All stakeholders now understand that an optimal technical solution includes the development of capabilities not only for automating driving but also for managing and limiting a variety of risks. Developers, vehicle users, civic leaders, policymakers, and consumer protection and safety advocates all seek confidence in the safety and security of AVs. But they bring different perspectives to policymaking processes, and three circumstances in particular make the political situation more difficult and awkward to navigate:

1. As with conventional vehicles, there will never be zero risk.[28]

[23] Edwards, David (2022) Mercedes-Benz partners with Luminar to develop automated driving systems. Robotics and Automation News, 24 January. Available from: https://roboticsandautomationnews.com/2022/01/24/mercedes-benz-partners-with-luminar-to-develop-automated-driving-systems/48532/.

[24] United Nations Economic Commission for Europe (UNECE) (2021a) *The French strategy* for *development of automated roads mobility 2020-2022, 22 January. Available from:* https://unece.org/sites/default/files/2021-01/GRVA-09-03e.pdf.

[25] German Federal Ministry for Digital and Transport (BMVI) (2015) Strategy for Automated and Connected Driving. Available from: https://www.bmvi.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.pdf?__blob=publicationFile.

[26] International Alliance for Mobility Testing and Standardization (IAMTS) (2022) About. Available from: https://iamts.sae-itc.com/about.

[27] European Automobile Manufacturers Association (2017) ACEA Principles Automobile Cybersecurity. Available from: https://www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf.

[28] Koopman, Philip, and Michael Wagner (2020) Positive Trust Balance for Self-Driving Car Development. Available from: https://arxiv.org/abs/2009.05801.

2. There is currently an asymmetry in access to information;[29] outsiders who seek to evaluate AVs do not have the same level of understanding and access to information that AV developers do.
3. Malicious actors will adapt to whatever technology they confront, and vulnerability will also continue to be caused by cyber threats and unintentional technical errors emerging from increasingly automated and complex software systems.

These realities have led industry, government, and other stakeholders to recognise that several indicators should be combined to assess safety and acceptable risk.[30] In particular, if how an AV perceives its environment and makes driving decisions is inscrutable, it should be possible to look more closely at how the developer is designing, testing, and producing the vehicle. However, stakeholders have yet to agree on who gets to take those looks.

Cybersecurity, safety, and other risks arising from AVs can be addressed ex ante, ex post, or both. In all cases, risk management is the goal. With ex post risk management, legal liability[31] is the dominant tool – it is intended to deter as well as remediate problems by providing a legal mechanism for people harmed by AVs to be compensated. Policymakers and safety advocates prefer the greater deterrence suggested by regulation and technical standards, which often arise separately but might be invoked by regulation. Available indicators that can reveal how AV developers are approaching AV safety and cybersecurity include (1) compliance with relevant international technical standards developed with European participation; and (2) evidence of safety culture, such as the extent to which company leaders convey the importance of safety and the extent to which workers can halt what they are doing if they detect a safety problem. Yet only AV development personnel can best monitor safety culture and compliance with standards.

Regulation for AVs combines conventional vehicle regulation (for example, for occupant protection and crashworthiness) with new features associated with software-based safety and cybersecurity risks. Here, the global marketplace shows a divide: the United States prefers self-certification by vehicle producers, while European and Asian countries prefer more oversight through "type approval"[32] processes. New EU type-approval rules[33] for safer and cleaner cars entered into force across the EU in September 2020.

Increasingly, AV developers are allying to create technical standards and best practices[34] that combine cybersecurity and traditional safety measures. This welcome trend recognises that the two kinds of risks interrelate. Relevant technical standards have been proliferating, a sign of greater understanding of the issues and of international collaboration in support of a global marketplace. Standards-setting organisations – the SAE, the International Organization for Standardization (ISO), the International Electrotechnical Commission, the European Union Agency for Cybersecurity (ENISA), the Institute for Electrical and Electronics Engineers, the UN International Telecommunication Union, the UN Economic Commission for Europe, and others – are all promoting AV safety and cybersecurity standards (both separately and together). For example, a joint ISO-SAE standard addresses cybersecurity engineering for road vehicles,[35] and another ISO standard speaks to assuring

[29] Fraade-Blanar, Laura, *et. al.* (2018) Measuring Automated Vehicle Safety: Forging a Framework. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2662.html.

[30] Blumenthal, Marjory S., *et al.* (2020) Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA569-1.html.

[31] Winkelman, Zev, *et al.* (2019) When Autonomous Vehicles Are Hacked, Who Is Liable?. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2654.html.

[32] European Commission (2022c) FAQ Type approval for vehicles. Available from: https://ec.europa.eu/growth/sectors/automotive-industry/technical-harmonisation/faq-type-approval-vehicles_en.

[33] European Commission (2020d) Questions and answers: New EU type-approval rules for safer and cleaner cars. Available from: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1534.

[34] Blumenthal, Marjory S., *et al.* (2020) Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA569-1.html.

[35] International Organization for Standardization (ISO) (2021) Road vehicles – Cybersecurity engineering, ISO.SAE 2143:2021. Available from: https://www.iso.org/standard/70918.html.

safety and cybersecurity by design.[36] Compliance with such standards is considered necessary by safety experts but not sufficient for achieving either safety or cybersecurity.

The EU's Approach

EU member states, the European Commission, and European tech and industry players have started to collaborate to achieve an ambitious vision for automated mobility across Europe. Particularly noteworthy is the creation in 2016 of the European Automotive and Telecoms Alliance (EATA[37]) to promote the development of connected and automated driving. Also notable is the European Commission's 2018 strategy,"On the road to automated mobility: An EU strategy for mobility of the future,"[38] which aims to make Europe a leader in the research, development, and deployment of AVs. This has been an arena where European companies have been active, leveraging historical strengths in motor vehicle design and production and targeted research initiatives[39].

The European Commission has been supporting the introduction and deployment of what it terms Cooperative, Connected and Automated Mobility (CCAM[40]). Although focused on AVs, CCAM recognises the growing use of communication between vehicles and between a vehicle and other things, such as traffic control devices. The commission, in collaboration with stakeholders, has put forward policy initiatives, supported standards at the EU level, and co-funded research projects. (For a cursory overview of recent EU cybersecurity-related initiatives, see table 1.) Horizon 2020, a large EU research funding program, featured joint funding with industry to support cybersecurity for AVs.[41] Some examples of research projects include the Knowledge Base on Connected and Automated Driving (CAD), a platform for data, knowledge, and experiences on CAD. The project is part of the Horizon 2020 Action ARCADE[42], an acronym that stands for Aligning Research and Innovation for Connected and Automated Driving in Europe. Under the new Horizon Europe program[43] (2021–2027), research and innovation related to CCAM will remain an important priority area. Another funding initiative, the Connecting Europe Facility (CEF[44]) (2021–2027), aims to promote the development of high-performing, sustainable, and efficiently interconnected trans-European networks in the fields of transport, energy, and digital services.

---

[36] International Organization for Standardization (ISO) (2020) Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation, ISO/TR 4804: 2020. Available from: https://www.iso.org/standard/80363.html.

[37] European Automotive and Telecoms Alliance (EATA) (2016) About. Available from: https://eata.be/news/.

[38] European Commission (2018a) On the road to automated mobility: An EU strategy for mobility of the future. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283.

[39] Aligning Research & Innovation for Connected and Automated Driving in Europe (ARCADE) (2022) Funded by the European Commission's Horizon 2020 programme. Available from: https://www.connectedautomateddriving.eu/about/arcade/.

[40] European Commission (2018c) Cooperative connected and automated mobility (CCAM). Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1957-Cooperative-connected-and-automated-mobility-CCAM-_en.

[41] *European Road Transport Research Advisory Council (ERTRAC) (2019) Connected Automated Driving Roadmap. Available from:* https://www.ertrac.org/uploads/documentsearch/id57/ERTRAC-CAD-Roadmap-2019.pdf.

[42] Knowledge Base on Connected and Automated Driving (CAD) (2022) Developed as part of the Horizon 2020 Action ARCADE. Available from: https://www.connectedautomateddriving.eu/about/.

[43] European Commission (2022a) Horizon Europe. Available from: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

[44] European Commission (2022b) Connecting Europe Facility. Available from: https://ec.europa.eu/inea/en/connecting-europe-facility#:~:text=The%20Connecting%20Europe%20Facility%20(CEF,infrastructure%20investment%20at%20European%20level.

Table 1: EU Initiatives Connecting Cybersecurity to AV Development[45]

Year	EU Initiatives
2014	The European Commission's Directorate-General for Mobility and Transport sets up a Cooperative Intelligent Transport Systems (C-ITS) deployment platform.
2016	The European Commission adopts a European Strategy on Cooperative Intelligent Transport Systems, a milestone initiative toward cooperative, connected, and automated mobility.
2016	Member states and the European Commission launch the C-Roads Platform to link C-ITS deployment activities, jointly develop and share technical specifications, and verify interoperability through cross-site testing.
2016	The Directive on Security of Network and Information Systems provides legal measures to boost the overall level of cybersecurity in the EU. It is the first piece of EU-wide legislation on cybersecurity. Currently, there is a proposed revision called the Network and Information Systems Directive (NIS2). It is a key focus of the current French Presidency of the Council of the EU, which aims to push forward the negotiations on NIS2.
2017	The European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship, and Small and Medium-Sized Enterprises launches an initiative on safety regulations. The aim is to further decrease the number of road fatalities and injuries by considering amendments to the General Safety Regulation and the Pedestrian Safety Regulation.
2018	The European Commission publishes the EU Strategy for Mobility of the Future. This strategy sets out a specific action to implement a pilot project on common EU-wide cybersecurity infrastructures and processes that are needed for secure and trustworthy communication between vehicles and infrastructure for road safety and traffic management.
2019	The European Commission sets up an Expert Group on Cooperative, Connected, and Automated Mobility, named CCAM, to provide advice and support to the commission in the field of testing and pre-deployment activities for CCAM.
2020	In 2020, to successfully implement the pilot project on common EU-wide cybersecurity infrastructures and processes, a subgroup on C-ITS under the commission's Expert Group on Cooperative Intelligent Transport Systems is set up. The European Commission publishes a report[46] by an independent Expert Group on Ethics of Connected and Automated Vehicles. The report includes twenty recommendations covering dilemma situations, the creation of a culture of

[45] Source: Georgia Dede, Rossen Naydenov, Apostolos Malatras, Ronan Hamon, Henrik Junklewitz, and Ignacio Sanchez, "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving," ENISA and JRC, European Union, 2021, https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/.

[46] European Commission (2020a) New recommendations for a safe and ethical transition towards driverless mobility. News, 18 September. Available from: https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en.

	responsibility, and the promotion of data, algorithm, and AI literacy through public participation.
2021	Drafted jointly by ENISA and the EU's Joint Research Centre (JRC), the report "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving" aims to provide insights on the cybersecurity challenges specifically connected to the uptake of AI techniques in autonomous vehicles.

Notwithstanding the above activities, the absence of clear, defined technical requirements or standards for autonomous driving – especially related to the security assessments of AI components – constrains what policy can accomplish in addressing AV cybersecurity and other risks. This challenge was highlighted in a joint 2021 report[47] by ENISA and the JRC, titled "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving." It warns that AVs carry serious cybersecurity risks. The report covers both the European and international policy contexts and includes an in-depth overview of technical aspects of AI in the automotive sector. Its threat model combines unintentional and intentional software and hardware vulnerabilities. Intentional threats involve the malevolent exploitation of AI and ML vulnerabilities. Threat actors might also introduce new vulnerabilities, given AV susceptibility to adversarial ML techniques[48] such as evasion or poisoning attacks. Unintentional harms mainly stem from limitations, malfunctions, or the poor design of AI models.

The European approach to AV regulation, unsurprisingly, extends to privacy and other data protection concerns, including the protection of know-how and potential data ownership, which are also at risk from AV cybersecurity threats. AVs produce data[49] of enormous value, ranging from how components and systems work to patterns of use by human riders. Using and monetising this data could, for example, improve old business models or create new ones. Under EU law, controllers of personal data, such as car manufacturers or application providers, have to implement appropriate technical and organisational measures *"to ensure a level of security appropriate to the risk"* posed by processing personal data according to Article 32 of the General Data Protection Regulation[50]. These concerns can be addressed in part by protecting against cybersecurity threats such as industrial espionage, as guided by the standards for IT (and AV) security.

The European approach to AV regulation, unsurprisingly, extends to privacy and other data protection concerns, including the protection of know-how and potential data ownership, which are also at risk from AV cybersecurity threats.

There is increasing demand for legal clarity at the EU level to facilitate predicted AV market growth and regulatory interventions. Some of the chief factors driving market growth are governmental subsidies for AV research and development; the rising demand for efficient, environmentally friendly, and safe travel; and the evolution of connected, automated, and electric car technologies. EU laws related to competition policy,

[47] ENISA (2021) Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. ENISA and JRC, 11 February. Available from: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/.

[48] Taddeo, Mariarosaria, *et al.* (2019) Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence* 1:557–560.

[49] Götz, Florian (2021) The Data Deluge: What do we do with the data generated by AVs? Siemens Blogs, 22 January. Available from: https://blogs.sw.siemens.com/polarion/the-data-deluge-what-do-we-do-with-the-data-generated-by-avs/.

[50] European Commission (2018b) General Data Protection Regulation. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

intellectual property rights, cybersecurity policies,[51] and product liability[52] also shape the regulatory ecosystem for European AV market growth.

Yet, are existing EU and national frameworks sufficient to provide the necessary protections, given the fast-evolving technological landscape in this sector? In principle, there are many civil, criminal, and administrative legal issues to be sorted out in relation to AVS that affect criminal liability for individuals and companies. Criminal law issues,[53] such as the prevention of cyber crime targeting vehicles, fall within the jurisdiction of each EU member state and are dealt with at the national level. But the EU does recognise that product liability frameworks need adjusting[54] to accommodate AVs. While the EU already has a robust safety and product liability regulatory framework, complemented by national and nonharmonised liability legislation, it recently acknowledged the need to assess the implications of emerging digital technologies – and AI systems in particular – and whether these technologies integrate safety and security-by-design.

The European Commission has since taken important steps toward making the needed adjustments. In February 2020, it published a "Report on safety and liability implications of AI, the Internet of Things and Robotics."[55] In April 2021, it proposed an AI regulation on "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)[56] and Amending Certain Union Legislative Acts," which recommends a risk-based approach to legal framework. The EU's ambition as stated in this regulation is to become a "global leader in the development of secure, trustworthy and ethical" AI. A coherent legal framework is indeed crucial for accelerating safe AI deployment in motor vehicles. Overall, although safety has been the primary liability factor for cars – and software flaws in driver-assistance systems have motivated recalls – the extreme dependence of AVs on software and other information technologies shifts liability away from drivers to developers (or fleet operators) and increasingly requires cybersecurity risks to be addressed through liability frameworks and other mechanisms.

> The involvement of European citizens in the early stages of AV initiatives and communication about AV safety and cybersecurity from trusted sources could be important steps toward building trust and shaping public perceptions about risks and opportunities.

Within Europe, the German government, for example, supported a multiyear project[57] to foster the collaborative development of approaches to simulation testing for AV safety and performance; follow-on projects are underway, and an international technical community participates in associated discussions. In 2021, Germany also passed the Autonomous Driving Act,[58] its first national law allowing automated driving in regular traffic at the SAE-defined Level 4 (as soon as 2022) – albeit only where designated by authorities and with the requirement that vehicles should be overseen

[51] European Commission (2022d) Cybersecurity Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

[52] Council of the European Communities (1985) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31985L0374.

[53] Punev, Anastas (2020) Autonomous Vehicles: The Need for a Separate European Legal Framework. *European View* 19(1):95-102.

[54] European Parliament (2018) A common EU approach to liability rules and insurance for connected and autonomous vehicles. EPRS Study. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf.

[55] European Commission (2020b) Commission Report on safety and liability implications of AI, the Internet of Things and Robotics, 19 February. Available from: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en.

[56] European Commission (2021) Proposal for an AI Regulation laying down harmonised rules for the EU (*Artificial Intelligence Act*). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[57] Pegasus (2019) Pegasus Symposium. Available from: https://www.pegasusprojekt.de/en/home.

[58] German Federal Government (2021) Autonomous Driving Act. Available from: https://perma.cc/LAW7-G4BU.

by a human. The law offers Germany some legal clarity and an edge[59] in designing AV technology. It stipulates three steps for the nationwide approval process of AVs; lists manufacturers' obligations and data processing requirements; and, because the autonomous driving function no longer requires a person to drive the vehicle during operation, it introduces a "technical supervisor" role to ensure compliance with current international regulations.

In the EU, a legislative framework specifically dedicated to the approval of AVs does not yet exist. However, existing EU legislation is to a large extent applicable to AVs, such as the Directive 2007/46/EC[60] framework updated in 2018[61] for use from 2020 for the approval of motor vehicles. And by submitting a draft EU implementing act[62] on the automated driving system in November 2021, the European Commission has taken an important first step toward shaping the future of AVs across the EU. The act proposes a harmonised European regulatory framework for Level 4 and 5 automated vehicles to be deployed on public roads across EU member states.

Finally, the commission formed an independent expert group[63] in 2019 to advise on ethical issues raised by driverless mobility and to address a number of technical, regulatory, and societal challenges before AVs can be safely deployed in the EU. Its 2020 report[64] features twenty recommendations covering (moral) dilemma situations, the creation of a culture of responsibility, and the promotion of data, algorithms, and AI literacy via public participation. Such attention to ethical perspectives can guide the evolution of regulation and other policy for AV cybersecurity and safety. The involvement of European citizens in the early stages of AV initiatives and communication about AV safety and cybersecurity from trusted sources[65] would be important steps toward building trust and shaping public perceptions about risks and opportunities.

Conclusion

Europe's leadership in AV development, testing, standards-setting, and regulation reinforces its place in the dynamic global AV arena. Thus, the EU has an opportunity to shine a brighter spotlight on cybersecurity – not to impede progress but to assure that this risk is not marginalised during the scramble to improve and demonstrate AV safety. Multi-stakeholder work on technical standards is one avenue for coupling safety and cybersecurity more consistently. From a broader perspective, the EU needs to unlock the potential of the AV disruption. The optimal strategy is to pursue safe, smart, environmentally sustainable, and inclusive mobility by aligning the design and implementation of vehicular automation technology with societal values and needs through a supportive policy environment.

---

[59] Ewing, Jack (2021) How Germany Hopes to Get the Edge in Driverless Technology. The New York Times, 14 July. Available from: https://www.nytimes.com/2021/07/14/business/germany-autonomous-driving-new-law.html.

[60] European Commission (2019b) Directive 2007/46/EC (Framework Directive). Consolidated version of 1 September 2019. Available from: https://ec.europa.eu/growth/sectors/automotive-industry/legislation/motor-vehicles-trailers/directive-200746ec-framework-directive_en.

[61] Association for Emissions Control by Catalyst (AECC) (2020) New Type-Approval framework Regulation (EU) 2018/858. Available from: https://www.aecc.eu/legislation/type-approval-framework/.

[62] European Commission, Directorate-General for Research and Innovation (2019a) Commission Implementing Regulation, laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of motor vehicles with regard to their emergency lane- keeping system (ELKS). Publications Office. Available from: https://op.europa.eu/en/publication-detail/-/publication/47d82bf0-564a-11eb-b59f-01aa75ed71a1/language-de.

[63] European Commission (2020a) New recommendations for a safe and ethical transition towards driverless mobility. News, 18 September. Available from: https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en.

[64] European Commission, Directorate-General for Research and Innovation (2020) Ethics of connected and automated vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility. Publications Office. Available from: https://data.europa.eu/doi/10.2777/966923.

[65] Blumenthal, Marjory S., *et al.* (2020) Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA569-1.html.

References

Aligning Research & Innovation for Connected and Automated Driving in Europe (ARCADE) (2022) Funded by the European Commission's Horizon 2020 programme. Available from: https://www.connectedautomateddriving.eu/about/arcade/.

Association for Emissions Control by Catalyst (AECC) (2020) New Type-Approval framework Regulation (EU) 2018/858. Available from: https://www.aecc.eu/legislation/type-approval-framework/.

Argo AI (2022) About. Available from: https://www.argo.ai/about/.

Blumenthal, Marjory S., *et al.* (2020) Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA569-1.html.

Brown, David, *et al.* (2021) The Future of the EU Automotive Sector. Study requested by the ITRE Committee, European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695457/IPOL_STU(2021)695457_EN.pdf.

Council of the European Communities (1985) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31985L0374.

Csernatoni, Raluca (2021) Chips geopolitics and EU's new semiconductors sovereignty agenda. EURACTIV, 29 October. Available from: https://www.euractiv.com/section/digital/opinion/chips-geopolitics-and-eus-new-semiconductors-sovereignty-agenda/.

Deloitte (2019) Autonomous Driving: Hype or Reality? Available from: https://www2.deloitte.com/be/en/pages/consumer-industrial-products/articles/autonomous-driving.html.

European Automotive and Telecoms Alliance (EATA) (2016) About. Available from: https://eata.be/news/.

Edwards, David (2022) Mercedes-Benz partners with Luminar to develop automated driving systems. Robotics and Automation News, 24 January. Available from: https://roboticsandautomationnews.com/2022/01/24/mercedes-benz-partners-with-luminar-to-develop-automated-driving-systems/48532/.

ENISA (2021) Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. ENISA and JRC, 11 February. Available from: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/.

European Automobile Manufacturers Association (2017) ACEA Principles Automobile Cybersecurity. Available from: https://www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf.

European Commission (2022a) Horizon Europe. Available from: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

European Commission (2022b) Connecting Europe Facility. Available from: https://ec.europa.eu/inea/en/connecting-europe-facility#:~:text=The%20Connecting%20Europe%20Facility%20(CEF,infrastructure%20investment%20at%20European%20level.

European Commission (2022c) FAQ Type approval for vehicles. Available from: https://ec.europa.eu/growth/sectors/automotive-industry/technical-harmonisation/faq-type-approval-vehicles_en.

European Commission (2022d) Cybersecurity Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

European Commission (2021) Proposal for an AI Regulation laying down harmonised rules for the EU (*Artificial Intelligence Act*). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission (2020a) New recommendations for a safe and ethical transition towards driverless mobility. News, 18 September. Available from: https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en.

European Commission (2020b) Commission Report on safety and liability implications of AI, the Internet of Things and Robotics, 19 February. Available from: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en.

European Commission, Directorate-General for Research and Innovation (2020c) Ethics of connected and automated vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility. Publications Office. Available from: https://data.europa.eu/doi/10.2777/966923.

European Commission (2020d) Questions and answers: New EU type-approval rules for safer and cleaner cars. Available from: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1534.

European Commission, Directorate-General for Research and Innovation (2019a) Commission Implementing Regulation, laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of motor vehicles with regard to their emergency lane- keeping system (ELKS). Publications Office. Available from: https://op.europa.eu/en/publication-detail/-/publication/47d82bf0-564a-11eb-b59f-01aa75ed71a1/language-de.

European Commission (2019b) Directive 2007/46/EC (Framework Directive). Consolidated version of 1 September 2019. Available from: https://ec.europa.eu/growth/sectors/automotive-industry/legislation/motor-vehicles-trailers/directive-200746ec-framework-directive_en.

European Commission (2018a) On the road to automated mobility: An EU strategy for mobility of the future. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283.

European Commission (2018b) General Data Protection Regulation. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Commission (2018c) Cooperative connected and automated mobility (CCAM). Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1957-Cooperative-connected-and-automated-mobility-CCAM-_en.

European Road Transport Research Advisory Council (ERTRAC) (2019) Connected Automated Driving Roadmap. Available from: https://www.ertrac.org/uploads/documentsearch/id57/ERTRAC-CAD-Roadmap-2019.pdf.

European Parliament (2021a) NIS2 Directive: A high common level of cybersecurity in the EU. EPRS Briefing, 1 January. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

European Parliament (2021b) Report on the EU Road Safety Policy Framework 2021-2030 – Recommendations on next steps towards 'Vision Zero'. Committee on Transport and Tourisms. Available from: https://www.europarl.europa.eu/doceo/document/A-9-2021-0211_EN.html.

European Parliament (2019) Self-driving cars in the EU: from science fictions to reality. Available from: https://www.europarl.europa.eu/news/en/headlines/economy/20190110STO23102/self-driving-cars-in-the-eu-from-science-fiction-to-reality.

European Parliament (2018) A common EU approach to liability rules and insurance for connected and autonomous vehicles. EPRS Study. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf.

Ewing, Jack (2021) How Germany Hopes to Get the Edge in Driverless Technology. The New York Times, 14 July. Available from: https://www.nytimes.com/2021/07/14/business/germany-autonomous-driving-new-law.html.

German Federal Government (2021) Autonomous Driving Act. Available from: https://perma.cc/LAW7-G4BU.

German Federal Ministry for Digital and Transport (BMVI) (2015) Strategy for Automated and Connected Driving. Available from: https://www.bmvi.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.pdf?__blob=publicationFile.

Götz, Florian (2021) The Data Deluge: What do we do with the data generated by AVs? Siemens Blogs, 22 January. Available from: https://blogs.sw.siemens.com/polarion/the-data-deluge-what-do-we-do-with-the-data-generated-by-avs/.

Gross, Andrew (2019) Long-Term Use od Advanced Driver Assistance Technologies Can Result in Disengaged Drivers. NEWSROOM, 17 December. Available from: https://newsroom.aaa.com/2019/12/long-term-use-of-advanced-driver-assistance-technologies-can-result-in-disengaged-drivers/.

International Alliance for Mobility Testing and Standardization (IAMTS) (2022) About. Available from: https://iamts.sae-itc.com/about.

International Organization for Standardization (ISO) (2021) Road vehicles – Cybersecurity engineering, ISO.SAE 2143:2021. Available from: https://www.iso.org/standard/70918.html.

International Organization for Standardization (ISO) (2020) Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation, ISO/TR 4804: 2020. Available from: https://www.iso.org/standard/80363.html.

Kassens-Noor, Eva, *et al.* (2020) Sociomobility of the 21st century: Autonomous vehicles, planning, and the future city. *Transport Policy* 99: 329-335.

Knowledge Base on Connected and Automated Driving (CAD) (2022) Developed as part of the Horizon 2020 Action ARCADE. Available from: https://www.connectedautomateddriving.eu/about/.

Koopman, Philip, and Michael Wagner (2020) Positive Trust Balance for Self-Driving Car Development. Available from: https://arxiv.org/abs/2009.05801.

Koscher, Karl *et al.*, (2010) Experimental Security Analysis of a Modern Automobile. *IEEE Symposium on Security and Privacy*, 2010, pp. 447-462, doi: 10.1109/SP.2010.34.

Lovells, Hogan, and Manuel Golling, Sebastian Polly (2022) New cyber security and software update rules in the automotive industry in 2022. JDSUPRA, 12 January. Available from: https://www.jdsupra.com/legalnews/new-cyber-security-and-software-update-1512229/.

Madrigal, Alexis C. (2013) Toward a Complex, Realistic, and Moral Tech Criticism. The Atlantic, 13 March. Available from: https://www.theatlantic.com/technology/archive/2013/03/toward-a-complex-realistic-and-moral-tech-criticism/273996/.

Papernot, Nicolas, *et al.* (2017) Practical Black-Box Attacks against Machine Learning. Cornell University. Available from: https://arxiv.org/abs/1602.02697.

Pegasus (2019) Pegasus Symposium. Available from: https://www.pegasusprojekt.de/en/home.

Punev, Anastas (2020) Autonomous Vehicles: The Need for a Separate European Legal Framework. *European View* 19(1):95-102.

P&S Intelligence (2019) Europe Autonomous Car Market Overview Report. Available from: https://www.psmarketresearch.com/market-analysis/europe-autonomous-car-market.

Research and Markets (2019) Europe Autonomous Car Market Research Report: By Vehicle Autonomy, Vehicle Type, Application, Regional Insight – Industry Trend, Competition Analysis and Forecast to 2030. Available from: https://www.researchandmarkets.com/reports/4804026/.

Fraade-Blanar, Laura, *et. al.* (2018) Measuring Automated Vehicle Safety: Forging a Framework. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2662.html.

Reuters Staff (2020) Volkswagen closes $2.6 billion investment in self-driving startup ARGO AI. Available from: https://www.reuters.com/article/us-volkswagen-argo/volkswagen-closes-2-6-billion-investment-in-self-driving-startup-argo-ai-idUSKBN2390E6.

Society of Automotive Engineers (SAE) (2021) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. J3016_2-2104, 30 April. Available from: https://www.sae.org/standards/content/j3016_202104/.

Taddeo, Mariarosaria, *et al.* (2019) Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence* 1:557–560.

UC Berkley (2022) Cyber-Physical Systems. Available from: https://ptolemy.berkeley.edu/projects/cps/.

United Nations Economic Commission for Europe (UNECE) (2021a) *The French strategy* for *development of automated roads mobility 2020-2022, 22 January. Available from:* https://unece.org/sites/default/files/2021-01/GRVA-09-03e.pdf.

United Nations Economic Commission for Europe (UNECE) (2021b) UN Regulation No. 155 – Cyber security and cyber security management system, 4 March. Available from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

Waldersee, Victoria (2022) Volkswagen and Bosch team up on automated driving software. Reuters, 25 January. Available from: https://www.reuters.com/technology/volkswagen-bosch-collaborate-automated-driving-software-2022-01-25/.

Wimerskirch, André, and Derrick Dominic (2018) Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles. University of Michigan, 1 January. Available from: https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf.

Winkelman, Zev, *et al.* (2019) When Autonomous Vehicles Are Hacked, Who Is Liable?. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2654.html.

About the authors

Marjory S. Blumenthal is a senior fellow and the director of the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Her career has focused on technology trends, impacts, and policy, with an emphasis on information and communications technologies and extending to biotechnology, health, and more.

Raluca Csernatoni is a visiting scholar at Carnegie Europe, where she works on European security and defense with a specific focus on disruptive technologies. She is also a guest professor at the Institute for European Studies at the Free University of Brussels (VUB).

About EU Cyber Direct – EU Cyber Diplomacy Initiative

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

New Tech in Review is a collection of commentaries, highlighting key issues at the intersection of emerging technologies, (cyber)security, defence, and norms.

IMPLEMENTING ORGANISATIONS

euiss European Union Institute for Security Studies

Universiteit Leiden Institute of Security and Global Affairs

CARNEGIE EUROPE

FUNDED BY THE EUROPEAN UNION