Predicting Technology and Its Impact on Humanity

Dejan Milojicic(iD), Hewlett Packard Labs, IEEE Fellow

Phil Laplante(iD), IEEE Fellow

This special issue of Computer reflects an intertwining of technology and sociopolitical factors. Articles range from medicine to war, from unmanned aircraft to software supply chains, and to the interconnection of technologies in an increasingly complex world.

The early 2020s will be remembered for COVID-19 and the war in Ukraine. Both events are examples of technology influencing human events—in defending humanity from pandemics and providing strategic advantages in conducting military operations. The opposite is also true—technological advancement and technology investments were shaped by medical and

[
THIS SPECIAL ISSUE OF *COMPUTER* INHERENTLY REFLECTS AN INTERTWINING OF TECHNOLOGY AND SOCIOPOLITICAL FACTORS.
]

military needs. This special issue of *Computer* inherently reflects an intertwining of technology and sociopolitical factors. Articles in this issue range from medicine to war, from unmanned aircraft to software supply chains, and to the interconnection of technologies in an increasingly complex world.

While predictions always attracted the interest of broad audiences, in the past few years, they became essential to humankind's survival. Whether pandemics or conflict, the ability to

predict the future became essential. Unfortunately, the prognosticators usually have few or fuzzy data to make these predictions—predicting critical decisions with scarce or uncertain information is now the norm rather than the exception.

We also continue to see the continued interest that these predictions have among authors and readers of *Computer*. For example, among the top 13 most accessed articles in *Computer*,[1] there are three articles from our past special issues.[2,3,4] Similarly, our first "Predictions" column in *Computer*[5] was the most downloaded IEEE column in all of 2021 even though it only appeared in October. In the span of the four years that we hosted special issues, we have observed a broadening of the scope of articles from very technology-focused articles to increasingly more humanity-focused ones. This is especially true in this issue.

In "Biometric Surveillance and the

Future of War," by Katina Michael,[A1] military "use cases" describe future applications of biometric surveillance and the corresponding social implications. Contributors to this study, presented as a Virtual Roundtable, present observations on the application of technology on citizens in both public and private contexts and applied to business and governmental regulations. The war in Ukraine is used as a testbed for technology exploration. Use cases are described, including identifying individuals in reported deaths, erroneous entry into enemy territory, deflection, and many others. All of these have both intended and unintended uses, and all of them have deep ethical implications.

"Ethics for Digital Medicine: A Path for Ethical Emerging Medical IoT Design," by Sudeep Pasricha,[A2] explores an interplay of ethical, regulatory, and societal issues introduced by digital medicine. Oversights in the design, implementation, and deployment of medical devices can have a detrimental impact on patients. To prevent these failures, Pasricha advocates innovations in medical devices based on education, programmable ethical behavior, and frameworks for ethical analysis. He argues that this approach is essential to prevent costly failures of future ever-complex smart devices while embedding ethical implications from their inception.

In "The Roles of Autonomy and Assurance in the Future of Uncrewed

Aircraft Systems in Low-Altitude Airspace Operations," Lanier Watkins, Denzel Hamilton, Tyler A. Young, Sebastian Zanlongo, Louis L. Whitcomb, Andrew R. Spielvogel, and Barbara Kobzik-Juul[A3]

The article "Software Supply Chain Security: Issues and Countermeasures," by Badis Hammi and Sherali Zeadally,[A4]

the whole solution can be compromised and used to stage attacks on high-profile end users. The authors provide a holistic solution to this problem, retaining all the benefits and eliminating the risks of the software supply chains.

In "Data Center Ethernet and Remote Direct Memory Access: Issues at Hyperscale," by Torsten Hoefler, Duncan Roweth, Keith Underwood, Robert Alverson, Mark Griswold, Vahid Tabatabaee, Mohan Kalkunte, Surendra Anubolu, Siyuan Shen, Moray McLaren, Abdul Kabbani, and Steve Scott,[A5] the future of data center Ethernet and remote direct memory access (RDMA) is discussed. The authors observe that with the convergence of high-performance computing, artificial intelligence, and traditional hyperscale data center applications, both Ethernet and RDMA over Converged Ethernet (RoCE) are

[**WHILE PREDICTIONS ALWAYS ATTRACTED THE INTEREST OF BROAD AUDIENCES, IN THE PAST FEW YEARS, THEY BECAME ESSENTIAL TO HUMANKIND'S SURVIVAL.**]

discuss advances in drone technology and their application. Drones are used in military operations around the world, but they are also being used for the delivery of consumer products. The authors focus on autonomy and

presents security challenges in a chain of software development by several organizations. Such a supply chain brings many benefits, such as maximizing profit, but it also exposes risks in terms of the weakest link in the chain. Thus,

APPENDIX: RELATED ARTICLES

A1. K. Michael, "Biometric surveillance and the future of war [Virtual Roundtable]," *Computer*, vol. 56, no. 7, pp. 21–30, Jul. 2023, doi: 10.1109/MC.2023.3249416.

A2. S. Pasricha, "Ethics for digital medicine: A path for ethical emerging medical IoT design," *Computer*, vol. 56, no. 7, pp. 32–40, Jul. 2023, doi: 10.1109/MC.2022.3216984.

A3. L. Watkins et al., "The roles of autonomy and assurance in the future of uncrewed aircraft systems in low–altitude airspace operations," *Computer*, vol. 56, no. 7, pp. 41–53, Jul. 2023, doi: 10.1109/MC.2023.3242579.

A4. B. Hammi and S. Zeadally, "Software supply chain security: Issues and countermeasures," *Computer*, vol. 56, no. 7, pp. 54–66, Jul. 2023, doi: 10.1109/MC.2023.3273491.

A5. T. Hoefler et al., "Data center Ethernet and remote direct memory access: Issues at hyperscale," *Computer*, vol. 56, no. 7, pp. 67–77, Jul. 2023, doi: 10.1109/MC.2023.3261184.

A6. C. Bash, P. Faraboschi, E. Frachtenberg, P. Laplante, D. Milojicic, and R. Saracco, "Megatrends," *Computer*, vol. 56, no. 7, pp. 93–100, Jul. 2023, doi: 10.1109/MC.2023.3271428.

exposed and require fresh solutions. The authors further predict that this new and improved Ethernet will replace RoCE and TCP protocols in less than a decade.

This is our fourth special issue of *Computer* on technology predictions. It follows three increasingly successful special issues.[6,7,8] These special issues complement our annual technology predictions[10] as well as two extensive "Future of" reports.[11,12] We would also like to refer you to the quarterly "Predictions" column in *Computer*, including in this special issue.[A6] You can find more about our approach to predictions in our two articles.[9,13]

We hope you will enjoy this special issue, and we would very much like to hear from you about it, particularly recommendations for improvements. It takes the effort, foresight, and wisdom of many to prepare a special issue. We offer our thanks to those who have already approached us with comments and suggestions from previous special issues and to all of the authors and reviewers of all the submitted articles of the present one. Finally, thanks to Jeff Voas, the editor in chief of *Computer*, for trusting us to organize these special issues. ▣

REFERENCES

1. "Computer," IEEE Xplore. Accessed: Apr. 15, 2023. [Online]. Available: https://ieeexplore.ieee.org/xpl/topAccessedArticles.jsp?punumber=2

2. E. Frachtenberg, "Practical drone delivery," *Computer*, vol. 52, no. 12, pp. 53–57, Dec. 2019, doi: 10.1109/MC.2019.2942290.

3. D. Patterson et al., "The carbon footprint of machine learning training will plateau, then shrink," *Computer*, vol. 55, no. 7, pp. 18–28, Jul. 2022, doi: 10.1109/MC.2022.3148714.

4. K. Bresniker et al., "Grand challenge: Applying artificial intelligence and machine learning to cybersecurity," *Computer*, vol. 52, no. 12, pp. 45–52, Dec. 2019, doi: 10.1109/MC.2019.2942584.

5. A. Vahdat and D. Milojicic, "The next wave in cloud systems architecture," *Computer*, vol. 54, no. 10, pp. 116–120, Oct. 2021, doi: 10.1109/MC.2021.3099955.

6. D. Milojicic, "Technology predictions," *Computer*, vol. 52, no. 12, pp. 31–33, Dec. 2019, doi: 10.1109/MC.2019.2944708.

7. P. Laplante and D. Milojicic, "Technology predictions," *Computer*, vol. 54, no. 7, pp. 14–16, Jul. 2021, doi: 10.1109/MC.2021.3074265.

8. P. Laplante and D. Milojicic, "Predicting technologies that advance humanity," *Computer*, vol. 55, no. 7, pp. 15–17, Jul. 2022, doi: 10.1109/MC.2022.3170600.

9. P. Faraboschi et al., "Technology predictions: Art, science, and fashion," *Computer*, vol. 52, no. 12, pp. 34–38, Dec. 2019, doi: 10.1109/MC.2019.2942286.

10. "CS tech trends and predictions," IEEE Computer Society, Washington, DC, USA. Accessed: May 4, 2023. [Online]. Available: https://www.computer.org/press-room/news-archive?tag=cs-tech-trends-and-predictions

11. H. Alkhatib et al., "What will 2022 look like? The IEEE CS 2022 report," *Computer*, vol. 48, no. 3, pp. 68–76, Mar. 2015, doi: 10.1109/MC.2015.92.

12. M. Arlitt et al., "Future of the workforce," *Computer*, vol. 56, no. 1, pp. 52–63, Jan. 2023, doi: 10.1109/MC.2022.3203505.

13. D. Milojicic, "The art of predictions," in *Proc. IEEE Carl K. Chang Symp. Softw. Services Eng.*, to be published.

ABOUT THE AUTHORS

DEJAN MILOJICIC is a distinguished technologist at Hewlett Packard Labs, Milpitas, CA 95035 USA. His research interests include high-performance computing, operating systems, distributed systems, and systems management. Milojicic received a Ph.D. in distributed systems from the University of Kaiserslautern, Germany. He is a Fellow of IEEE. Contact him at dejan.milojicic@hpe.com.

PHIL LAPLANTE is a computer scientist and software engineer. His research interests include computer security, safety critical software systems, artificial intelligence and software quality. Laplante received a Ph.D. in computer science from Stevens Institute of Technology. He is a Fellow of IEEE. Contact him at plaplante@psu.edu.