

ranges from 0.4 to 6.1 per 1000 patients.<sup>6</sup> How would methadone safety be defined in this context? At what incidence of naloxone administration would methadone be considered unsafe, or safe, compared to other opioids? Using Dr Weingarten's posit of 1 naloxone administration per 1000 anesthetics, one would need a trial of 78,789 patients to show a 30% difference in naloxone use. We agree that a comparative effectiveness trial would be ideal and encourage Patient-Centered Outcomes Research Institute or other entities to sponsor such an important and clinically meaningful outcome trial.

Weingarten et al also argue that provider inexperience with methadone could lead to adverse events. This is true of all opioids and all drugs. Practitioners should educate themselves, and trainees, about pharmacology, therapeutics, and appropriate drug use.

**Sarah Lumsden, MD**

Department of Anesthesiology  
Michael E DeBakey VA Medical Center  
Houston, Texas  
Anesthesiology and Surgical Oncology Research Group  
Houston, Texas

**Evan D. Kharasch, MD, PhD**

Department of Anesthesiology  
Duke University School of Medicine, Bernaride LLC  
Durham, North Carolina

**Juan Cata, MD**

Department of Anesthesiology & Perioperative Medicine  
MD Anderson Cancer Center  
Houston, Texas  
Anesthesiology and Surgical Oncology Research Group  
Houston, Texas  
jcata@mdanderson.org

## REFERENCES

1. Weingarten TN, Sprung SJ. Intraoperative methadone: safe for widespread use? *Anesth Analg*. 2024;139:e43–e44.
2. Dunn LK, Yerra S, Fang S, et al. Safety profile of intraoperative methadone for analgesia after major spine surgery: an observational study of 1,478 patients. *J Opioid Manag*. 2018;14:83–87.
3. Ramaiah VK, Kharasch ED. Methadone and enhanced recovery after surgery: concepts and protocols. *Anesth Analg*. 2024;139:670–674.
4. Kharasch ED. Intraoperative methadone and postoperative anesthesia care unit outcomes: a retrospective cohort analysis. *Anesthesiology*. 2024;141:408–410.
5. Shafi S, Collinsworth AW, Copeland LA, et al. Association of opioid-related adverse drug events with clinical and cost outcomes among surgical patients in a large integrated health care delivery system. *JAMA Surg*. 2018;153:757–763.
6. Weingarten TN, Sprung J. An update on postoperative respiratory depression. *Int Anesthesiol Clin*. 2022;60:8–19.

DOI: 10.1213/ANE.0000000000007159

## Remote Monitoring and Artificial Intelligence: Novel Technologies and New Threats

### To the Editor

We read with great interest the article by Feinstein et al,<sup>1</sup> discussing how new technologies, such as artificial intelligence (AI), remote monitoring, machine learning, and augmented reality, can radically change the future of anesthesiology. As the authors state, these concepts, together with advancing medical knowledge, have evolved rapidly, creating the potential for new therapeutics and synergistic applications. The enormous speed of technological development in anesthesia and intensive care has been evident in recent years, and the coronavirus disease-2019 (COVID-19) pandemic, along with, rising health care costs, has accelerated the progress of remote monitoring.

While the article delves into the potential benefits for patients, anesthesia providers, and health care systems, we have also seen serious risks with the developments described and would like to broaden the discussion for future analysis and research.

We recognize that it is very difficult to cover all the important aspects in a short article, but we feel that it is important to highlight some conspicuous patient safety risks as well as system risks related to widely implementing these services and technologies. There are clear threats associated with cyber breaches, cybercrime, cyberterrorism, and the growing danger of hybrid warfare. Whilst there is no internationally accepted definition of hybrid warfare, it is usually described as a combination of conventional, irregular, and asymmetric strategies deployed in civilian settings. Using a combination of disruptive attack modalities, including cyberterrorism and disinformation, is usually the norm. This concept has been increasingly driven by globalization, technological advancements, shifting demographics, and the “Great Power Competition,” a rivalry between the United States, China, and Russia aimed at influencing global security, trade, and development.<sup>2</sup>

Recent global events have also shown that health care facilities and medical providers are not immune to aggression and threats from terrorists, criminals, or rogue states. In fact, the current war in Ukraine clearly shows that hospitals, outpatient centers, and ambulances are targets.<sup>3</sup>

With our increasing dependence on computer systems and technology in operating rooms, intensive care units, and critical care transport, most health care systems are becoming extremely vulnerable to cyberattacks.<sup>4</sup> Many health care IT systems, communication systems, ventilators, radiotherapy, monitoring

systems, and infusion pumps are already extremely soft targets because of their inadequate or often outdated security controls.

Different types of cybercrime and cyberterrorism are constantly increasing, posing a serious threat to all parts of the health care system from prehospital care and patient transport to in-hospital and outpatient care. Most attacks are perpetrated by criminal hackers, but there are also attacks by state-sponsored groups, such as the cyber attacks against Boston Children's Hospital, Boston, MA, in 2021<sup>5</sup> and against Singapore Health in Singapore during 2018.<sup>6</sup> Recent examples of state-sponsored attacks include those from Russian hackers who have actively targeted US hospitals in response to the support of Ukraine in the current conflict. Cyberattacks have been shown to cause disruptions in care as well as complications from medical procedures and increased mortality.

A paradigm shift in the implementation of advanced technologies, such as AI and automated systems for assessment and intervention in the operating room, as well as advanced monitoring at home, necessitates a comprehensive analysis of individual patient safety and its impact on society's preparedness and resilience. For instance, data from power outages indicate that there is a clear increase in Emergency Department visits by patients with chronic diseases. Consequently, a cyberattack targeting patients receiving remote monitoring at home could pose a significant threat to patient safety and put substantial pressure on emergency medical services (EMS), emergency departments, and hospitals.

It is also evident that intraoperative and postoperative workflows, and patient safety, could be seriously affected if they are dependent on automated processes for anesthesia, monitoring, and predicting the patients' clinical needs.

We agree with the conclusion of the article that "The only certainty is change, and the pace certainly seems to be accelerating." However, we suggest that the substantial risks of implementing these technologies must be addressed in guideline writing, research, and preparedness planning to mitigate the looming threat of cyberattacks and hybrid warfare.

**Fredrik Granholm, MD**

Sundsvall County Hospital  
Sundsvall, Sweden  
fredrik.granholm@rvn.se

**Derrick Tin, MBBS**

Department of Emergency Medicine  
Beth Israel Deaconess Medical Center  
Harvard Medical School

**Richard Staynings, BA**

University of Denver-University College

**Gregory R. Ciottone, MD**

Department of Emergency Medicine  
Beth Israel Deaconess Medical Center  
Harvard Medical School

## REFERENCES

1. Feinstein M, Katz D, Demaria S, Hofer IS. Remote monitoring and artificial intelligence: outlook for 2050. *Anesth Analg*. 2024;138:350–357.
2. Granholm F, Tin D, Doyle L, Ciottone G. A gray future: the role of the anesthesiologist in hybrid warfare. *Anesthesiology*. 2023;139:563–567.
3. Barten DG, Tin D, Granholm F, Rusnak D, van Osch F, Ciottone G. Attacks on Ukrainian healthcare facilities during the first year of the full-scale Russian invasion of Ukraine. *Confl Health*. 2023;17:57.
4. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. *J Clin Monit Comput*. 2023;37:1123–1132.
5. Raymond N. Iranian-backed hackers targeted Boston Children's Hospital, FBI chief says. Reuters. Accessed May 3, 2024. <https://www.reuters.com/world/us/iranian-backed-hackers-targeted-boston-childrens-hospital-fbi-chief-says-2022-06-01/>.
6. Singapore Ministry of Communications and Information. Public report of the COI into the cyber attack on Singapore Health Patient Database. Accessed May 4, 2024. <https://www.mci.gov.sg/media-centre/press-releases/public-report-of-the-coi/>.

DOI: 10.1213/ANE.0000000000000716

## In Response

We agree with the response of Dr Granholm et al<sup>1</sup> that cybersecurity considerations are warranted when discussing the future of technology in anesthesiology. The authors delineate a range of technology-related threats and identify examples of cyberattacks on health care systems that have already occurred. We agree with their suggestion that technological advancements in health care must be coupled with ongoing analyses of individual patient safety as well as societal preparedness for cyberattacks.

To this end, recent developments in health care sector cybersecurity in the United States indicate that the federal government recognizes the increasing significance of cybersecurity threats and importance of proactively protecting against them.<sup>2</sup> Strategic goals include creating financial incentives for health care systems to invest in advanced cybersecurity practices. Many other countries, including those in the European Union, for example, have adopted strategic

**Funding:** This work was funded by NIH grant 1K01HL150318.

**Conflicts of Interest:** Dr I. S. Hofer is the founder and President of Extrico Health a company that helps hospitals leverage data from their electronic health record for decision making purposes. Dr I. S. Hofer receives research support and serves as a consultant for Merck.