Emerging Technologies, Evolving Threats: Next-Generation Security Challenges

I. Introduction

SECURITY is a fundamental human requirement. We desire the security of our person against injury, security of our capability to provide for our families, security of income linked to needs (food, water, clothing, and shelter), and much more. Most also hope for security of a way of life that is fulfilling and pleasant and peaceful [1]. In 2003, Alkire [2] defined "human security" as: "[t]he objective ... to safeguard the vital core of all human lives from critical pervasive threats, in a way that is consistent with long-term human fulfillment." Today most of the world's population is highly dependent, even for basic needs, on large technological systems. According to the *Oxford Dictionary*, *dependence* can be defined as: "the state of relying on or being controlled by someone or something else." In the context of technological systems, dependence may imply an unwanted consequence of nonavailability. Dependence may also be deliberately misapplied to create some level of coercion toward some other action [3]. For instance, in drug abuse, we can say that there is an overreliance on a dependency that leads to addiction. In the realm of technology systems, as they are increasingly becoming a part of everyday life, dependencies can have major consequences. Thus, an emphasis on "security" seems highly relevant for a journal devoted to considering the effects of technology on society in all its facets.

Some distinctions in terminology are required before we proceed. *Technology* could imply a simple system that operates with clockwork (Boolean) clarity, constantly producing answers of unassailable probity from simple inputs. But *technology* could also imply an image recognition system that has been trained on a biassed dataset [4] and that will likely replicate the biases of those who curated the training material [5]. We also need to differentiate between a *technology* and a *technological system*; the latter often includes people within its scope, while the former is preoccupied with an object or artifact. And in this context, dependence relates to those who operate (wield) the technological system with the power to impact its availability. To illustrate the difference, a patient might think of a technology that displays whether they are in the infectious stage of COVID as harmless because "it is just another piece of code." But that very same patient might be skeptical of a human within a technology system that has the capability to override the software to change their patient status to "infectious/quarantined" and thereby prevent them from exercising their civil rights [6]. Technology and technology systems, both can accidentally or deliberately *lock out* individuals from accessing particular services [7], in addition to being *locked-in* to unwanted states.

II. Security Challenges

Consideration of *security* almost always challenges us to identify what we are securing. A list of fields in which security is relevant would be long indeed, but a review would likely suggest some degree of the hierarchical ordering of groupings. These might include: Environmental Security, Physical Security, Personal Security, Organizational Security, National Security, and Global Security [8]. This layered categorization of security should be a significant consideration when thinking through thought experiments and possible scenarios. For example, without underestimating the effects of a failure of organizational security, if personal security and global security are not compromised by the threats that affect an organization, then the organization can be rebuilt—but a failure of environmental security (catastrophic climate change) could potentially bring an end to all life on Earth [9]. At the local level, this might mean that a village does not have access to clean drinking water, or is subject to air that has been polluted by heavy industry. However difficult it might be to agree upon a basic hierarchy of needs, there would seem to be obvious benefit from preserving the security of more foundational needs and insulating these from the effects of security threats to layers up the stack.

A conception of layered security needs would then highlight the danger posed by either ubiquitous or highly integrated systems (communications and finance) that threaten cross-layer effects, and would draw attention to the possibility of cascading failures. At the macro level, recent world events have caused many to ask whether global supply chains and indeed global food supplies could be prone to cascading failure events, and at the micro and meso levels, devices such as implantable technologies could pose threats to both national, organizational, and personal safety [10]. Even considering the emergence of a *black ball* technology (as per Bostrom [11]), a society that has preserved foundational security needs and avoided pathways for cascading failures is more likely to retain functionalities that allow rebuilding. When we consider the social effects of a particular technology, consideration should include its flow-on effects as well as the scale of its effects. We cannot merely focus on organizational and national security in the hope that personal and global security will be attained. A holistic systems view is paramount to better understanding the complexity and

Digital Object Identifier 10.1109/TTS.2022.3202323

interdependent flows within and between subsystems at each layer. The interdependencies, in fact, often reveal the frailty of our modern technological systems: water (hydropower) powers electricity, electricity powers telecommunications, telecommunications powers banking, and banking enables retailing. If any one of these utility verticals is affected, the whole end-to-end system is unavoidably affected with major consequences to end users at various points of the service delivery.

An issue that emerges from the papers presented in this special issue, is the challenge of disentangling these multifaceted and multipart issues. Taken analogously, an employee may be providing for their family but contributing to injustices elsewhere if the fruits of their skills and labor meet their employer's direction. Alternatively, an employee may make a problematic decision that their personal well-being (or some perceived greater goal) is best served by actions whose effect is opposite to that for which an employer is striving [12]. How do we establish levels of security, to ensure that failures remain within a layer and do not become cascading? This issue is particularly challenging when considering emerging technologies and evolving threat vectors. As Gartner Research has stated, security technologies must continually evolve to match the transformations that are occurring across platforms, across sectors, and diverse landscapes [13].

New security risks continue to present themselves, and with the emergence of these threats must come commensurate responses posed by the new infrastructures, enabling technologies, and advanced security programs. All stakeholders, not just business, are needed to minimize the emergent risks [14]. The vectors of attack are now more diverse than ever, and this poses a great risk to society at large. While we seek greater efficiency, service, and profitability through transformations generated by the introduction of emerging technologies, such as AI office automation or the use of military drones, the question is whether we can absorb the potential cyber threats that come with the innovation, from the government office right through to the armed forces commensurately [15]. Emerging technologies must therefore undergo a technology assessment in order to evaluate their security robustness, and further anticipate the kinds of risk-related challenges that these new technologies may pose. This can be anything from Apps on mobile phones and network penetration, to unauthorized access and significant data leakage of sensitive information. One way to circumvent these risks is to assess them before they actually present as problems through strategic risk management [16], e.g., instituting agnostic adaptive data loss prevention solutions to reduce network breaches and data leakage [15]. Again, Gartner Research reminds us that it is not enough to demonstrate good security features to mitigate the threats, new security solutions must ensure "safety, availability, reliability, resilience, and privacy" [17].

III. Emerging Technologies and Evolving Threat Vectors

Many exemplar fields for emerging technologies exist, and each may align with an evolving threat vector. These threat vectors include: Wearables and Implantables, Internet of Things, 5G, Geospatial Technology, Biometrics, Data Analytics, Robotics, Biotechnology, 3-D Printing, Virtual and Augmented Reality, Advanced Materials, Artificial Intelligence and Machine Learning, Autonomous Systems, Genome Editing Technology, Cyber–Physical Advances, Quantum Computing and Convergence, among others [18]. Threat vectors also include major subcategories relating to government welfare systems, medical systems, and even defense-related autonomous vehicles. How then do we identify a vulnerability as a quality that is a potential threat-target? What framework do we use to assess a possible technological threat? And what unique contribution can we offer? Let us consider some basic categories.

Threats More Fundamental Than Intended: Of concern, we see cases where technologies are acquiring the capacity to threaten foundational layers of security. The acquisition of these capacities is perhaps not intentional but raises questions. How do we clearly identify technological issues that threaten such foundational layers? Conversely, if basic levels of personal security are preserved, then it is somewhat more acceptable that only more esoteric layers are exposed to debate. This issue might seem obvious, but it raises important questions of the extent to which foundational layers of security are actually insulated from the possibility of technological threat linked to higher layers of need.

Threats that are Magnified by Technological Capability (Insider Threats): Technology has always amplified the capability of individuals; this can be considered down to the most basic examples of a lever, fire control, or the application of wheels. Current technology advances extend to cases where technology enables an individual—not necessarily possessed of a refined ethical judgment—to wield power that is wildly outside the scope specifically assigned to them or outside the scope commensurate with their personal *mana* [19]. How shall a learned society respond to such magnifications of power?

Threats from Technological Hubris: Technological advances in many fields of science and engineering are cherished and embraced, often without much hesitation. Notably, AI technology, despite the concerns of many, e.g., T. Gebru, E. Bender, and others [20]. Large AI-based language and computer vision models have demonstrated unique capabilities, such as creating new sentences from a given context (Fig. 1) or creating images from a description (Fig. 2). The images in Fig. 2(b) are from things that do not occur naturally in our world but only in our imagination. The text and image models have been trained on large corpora and image datasets, and the outputs are the stochastic product of what the model assumes to be the next word in a sentence or the visual depiction of a phrase. And while we should certainly celebrate this and other technological achievements, we might also take a very high-level view of technologies we consider integrating into the society that are likely to reinforce dependencies.

As an example, with some humility, we can contrast the area of Artificial Intelligence with respect to the capabilities of natural things. Consider a listing of animal species organized in order of numbers of neurons/synapses, for example, the wandering spider (*Cupiennius salei*), that has an estimated 100 000 neurons. Each example of this humble and neuronally

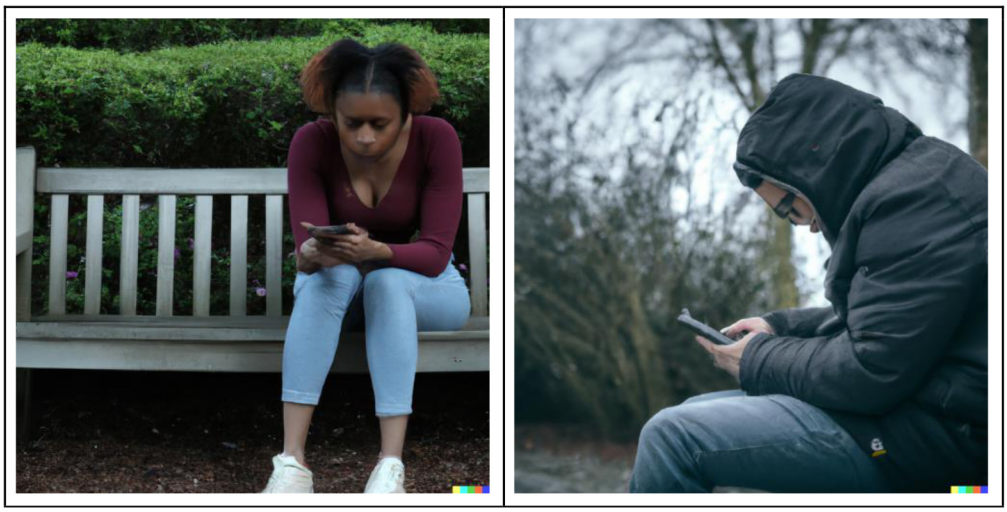

Fig. 1. Text generated with GPT-2 [21], where the text in italics is the context given to the model, and the rest is produced by the large language model. Note that a newer model, such as GPT-3, would produce even better, more "human-like" results; however, access to it is limited due to ethical concerns. Prompt: A photograph of a person sitting on a bench in the park on a dark day, worried about security and privacy while holding a smartphone. *Technological advances in many fields of science and engineering are cherished and embraced, often without much hesitation. Notably, AI technology, despite the concerns of many, large AI-based language and computer vision models have demonstrated unique capabilities such as*, of course, an accurate portrayal of humans and human emotions in real-time to improve human relations, more accurately predict the future behavior of society, and enhanced understanding by individuals; these advances have long been considered as a sign of progress and progress on all three fronts.

Fig. 2. Images generated with DALL-E [22], where the text in italics is the context given to the model, and the images are produced by the large text–image model. Similar to GPT-3, access to it is currently limited due to ethical concerns. None of the people in the images are real, nor is the entire image, but images are produced based on what is likely to correspond to the text. Prompt: A photograph of a person sitting on a bench on the surface of the moon, worried about security and privacy while holding a smartphone. *Technological advances in many fields of science and engineering are cherished and embraced, often without much hesitation. Notably, AI technology, despite the concerns of many, large AI-based language and computer vision models have demonstrated unique capabilities such as*, of course, an accurate portrayal of humans and human emotions in real-time to improve human relations, more accurately predict the future behavior of society, and enhanced understanding by individuals; these advances have long been considered as a sign of progress and progress on all three fronts.

challenged beastie is capable of completely autonomous navigation and locomotion, and fine control of legs, eyes, and mouthparts. It is capable of strategizing successfully to find and catch food (its food will run away or even fight back rather than be caught and eaten) to satisfy its energy needs, and it has demonstrated the ability to reproduce itself unaided and reliably over millennia. In contrast, the human-made Boston Dynamics' dog [23] has demonstrated impressive motor control and may be considered close to the leading edge of autonomous robotic devices but the Boston Dynamics dog requires detailed guidance from a human operator and a highly specialized and completely tame energy source provided by its creators. It also seems to lack either the equipment or the inclination to reproduce itself autonomously. IBM's "Deep Blue" has beaten human chess champions yet a more cynical view is that a chess game is a particular type of problem at which computers are extraordinarily adept, and which humans find particularly difficult [5], [24]. We can reflect on the shortcomings of Deep Blue, that the machine has never quite been able to be "commercialized" or "productized" for everyday end-user consumption by IBM. Deep Blue is unable to seek its own energy source, engage in a theological debate (despite

IBM's Project Debater [25]), run around on a football field or autonomously reproduce itself after a romance with another AI [26].

We may point to obvious incapabilities, but professional engineers' codes of ethics constantly exort us to operate within our scope of competence, and that ethics might lead us to ask whether the descriptor "artificial intelligence" is justified over less majestic descriptors like "advanced pattern-classification algorithms" or a "risk analysis depth-first search algorithm"? The comments are also perhaps unfair to technologies that only ever claimed "intelligence" rather than "alive-ness." Taking a more general view, it seems important to apply some consistent framework to the evaluation of an emerging technology: What fundamental levels of security needs does it intersect with? Does it interfere with the segregation of layers of security and hence contribute to the possibility of cascading failure?

IV. Responses to Security Challenges

Let us also consider how some specific issues are evolving. Recent claims that an AI system has reached sentience [27] evoke a level of scepticism. The details of the argument are fascinating, but the discussion of arcane points carries the risk of missing some very fundamental issues. Organic lives are finite and short. It is perhaps uncomfortable to contemplate how fundamental those two factoids are, but perhaps it is those foundational and pervasive awarenesses that underpin many human judicial approaches—for a person, a decade of incarceration cannot be recovered, but an AI system can power-up without loss, after being switched-off for a decade or a millennium. It would be sad if fear of punishment provided the only steerage for our moral compass but a total lack of fear of accountability is certainly not likely to help. We can observe that almost all persons have both a level of empathy, and a foundationally intuitive sense that their lifetime's doings will be somehow judged or at least assessed. Perhaps these are partially mediated by the functioning of the amygdala, but the basic concepts and connections seem to operate at a more fundamental level. Our self-judgments are measured carefully against concepts of consciousness—the capability to abstract/project—and the ability to evaluate ethical and moral responsibility that are common to most persons. We should consider ethical responsibilities if we (contributors to the *IEEE Transactions on Technology and Society*) allow a purveyor of technology to propose or imply a level of capability that is actually qualitatively beyond the actual [5], [28]. Let us not be too slow to "prick the bubbles of pretention." In the past, the approach has been (paraphrasing Elon Musk [29]) to wait till lots of bad things happen, then after much harm has been irreparably done, undertake agonizingly slow regulatory approaches to stop precisely the same things happening at some far-future date—and meanwhile slightly different, irreparably harmful things are already happening. Legal processes are indeed agonizingly slow and frequently appear to lack technological insight [30]. Does this perhaps emphasize the significance of comment from a body independent of commercial pressures, but with deep technological insight and a foundational regard for ethics… such as IEEE? And this with a nod to work contributed by Kate Crawford and her team that have provided an *Atlas of AI*, alongside the concept of "enchanted determinism" [31].

We Offer Three Types of Responses: Our contributors should continue to analyze specific technologies in depth, considering their effect on specific aspects of society and taking the broadest view of their significance. Commercial pressures have strongly incentivized "vertical integration" of services, which inherently enable cascading failure scenarios and comprise the single largest category of "threat" [32].

We (potential contributors to these Transactions) should continue to explore, in both theoretical and practical realms, approaches to improving the generic robustness of a technologically dependent society [33]. Robustness within any field is valuable, but generic approaches to avoiding fragility and possibilities for cascading failure, have a greater breadth of effectiveness [34].

We would like to suggest that our Society (the Society on the Social Implications of Technology) is uniquely placed to aggregate and analyze the plethora of specific security issues, not limited to those included in this special issue, and to generate both clarifications, criteria, and also metrics for these security issues. This is definitely a nontrivial task: word-smithing a lowest-common-denominator definition that is acceptable to a varied group could even generate outcomes that actually have a negative value by being uselessly vague. But in contrast, really adequate functional clarifications could avoid the "whack-a-mole" conundrum and potentially provide a long-term basis for regulating improved security.

V. In This Issue

This guest editorial team accepted six papers for the special issue, ranging in diversity and unit of analysis. The resulting collection of articles examines potential threats, ranging from the issues of cybersecurity and individual rights, through broader medical cyber–physical systems threats, to privacy and security issues related to mobile IoT, and finally, cyber weapons assessment incorporating technical features of malicious software.

The first paper is written by Schwartz *et al.* [A1] who are with the Science and Technology for Peace and Security, Technical University of Darmstadt, Germany. Schwartz *et al.* attempted to learn more about people's awareness of dual-use technologies with respect to autonomous vehicles between the commercial and military domains by conducting in-depth interviews with a variety of actors engaged in autonomous vehicle development. The findings indicate that while most developers were aware of dual-use debates, few had reflected on the possible transfer of their own development processes in the context of autonomous driving to military applications. Mainly this lack of reflection was found to be related to the issue of complexity, enabling engineers to alienate themselves from responsibility for the use of the artifacts they had helped create. Additionally, actors had spent little time considering the potential misuse of such emerging technologies, with no standardized policy guidelines existing to provide information about possible risks.

Insider threats have always been a significant cybersecurity matter. In 2016, IBM found that over 60% of cybersecurity attacks were conducted by insiders [35]. These commonly take the form of sabotage, fraud, intellectual property theft, and espionage, among other attacks, and can be motivated by a variety of influences. The second paper [A2] written by Canadian psychologist Schoenherr with the Department of Psychology, Concordia University and with the Institute for Data Science, Carleton University, is focused on extending a cybersecurity questionnaire (CSEC) by including items that differentiate cyber hygiene behavior, self-disclosure vulnerability, intrusion vulnerability, and persuasion vulnerability. Using individual difference measures that are related to performance in experimental tasks, the study provided evidence that individuals high in emotionality (i.e., fear and anxiety) and low in moral motivations (i.e., fairness and morality) are more likely to report engaging in behaviors related to unintentional insider threats. Coupled with these findings is what we know about the commensurate acceleration of convergence among emerging technologies. Is it any wonder that reports continue to find that insider threats have increased 40%–50% in the last two years with estimates that this number is set to increase even more [36]? The question is, as company security perimeters continue to be vague, and remote work opportunities due to COVID-19 extend attack vectors, whether this statistic will also grow. While malicious intent is rampant industry-wide either through employees or associated personnel, unintentional errors are also on the rise according to Panda Security.

The third paper [A3] was submitted by transdisciplinary scholar Wigan, Emeritus Professor of Edinburgh Napier University, who contributes his lived experience and qualified perspectives on medical applications from a quality of life end-user perspective, advocating for a greater treatment of subjective patient quality engagements to work toward a better understanding of AI methods, and individual medical and associated life data cyber risks. The paper provides a future roadmap for research with five pertinent areas of concern, among which are: the security of ever more sensitive data streams; and vulnerability to unauthorized third-party use of machine learning/artificial intelligence-deduced characterizations of the patient.

In juxtaposing Wigan's paper about the importance of individual user feedback to organizations, we return to cyber–physical systems in the medical domain, toward Society 5.0 aspirations, in the fourth paper [A4] of the special issue. Patil, Ambritta, Mahalle, and Dey reflect on whether or not we are ready for this next big leap in our medical infrastructure. Patil and Mahalle are from Vishwakarma Institute of Information Technology, Ambritta is from Glareal Software Solutions in Singapore, and Dey is with JIS University. In many ways, this paper makes some inroads into Wigan's questions of "how to, next." Apart from putting forward an emergent framework, the authors subsequently identify a variety of attack vectors in emerging medical cyber–physical systems, and security-centric design issues focused on the introduction of a "data protection layer" in Society 5.0, demonstrating the importance of dealing with data in this context to maintain patient privacy. At the end of their paper, the authors postulate whether or not people are ready for Society 5.0 and the impact of Internet of Things devices, as the emphasis shifts from one of pure data collection to one of deriving meaning from that data. A discussion on ethical aspects of medical cyber-physical systems is presented, making strong links between emerging technologies that may be autonomous, and ethical approaches in the design of cyber–physical systems.

The fifth paper [A5] written by Sodagari is a substantial contribution to the literature. The paper is focused on the theme of crowdsourcing data from smart city infrastructure, in particular from Internet of Things devices used for pandemic monitoring, environmental monitoring, healthcare, Industrial IoT (IIoT), smart homes, wearable devices, smart furniture, and Internet of Vehicles (IoV), among other emerging technologies and applications. Sodagari from California State University develops a privacy and security taxonomy for mobile crowdsourcing systems (MCS), among which can be found MCS topics dedicated to: blockchain, machine learning, edge, vehicular, Android smartphone, Industrial IoT, 6G, recommendation systems, cloaking, fake news, truth discovery, and more. The author not only identifies the problems but also provides ways forward through probable solutions, all the while identifying some of the pertinent challenges that may emerge.

The final paper [A6] is by Reinhold and Reuter who are with the Science and Technology for Peace and Security, Technische Universität Darmstadt in Germany. The article provides a unique indicator assessment model based on parameters that can be measured prior to the application of malicious software, enabling the categorization of malicious tools as cyber weapons. Previous assessment models have identified cyber weapons based on assumptions about adversarial actors, or have done so only after the usage of a malicious tool. This paper, and also this special issue as a whole, represent various units of analysis in security, from personal to organizational, from smart cities that contain mobile crowdsourcing systems to military applications with respect to cyber weapons.

TAMARA BONACI
Khoury College of Computer Sciences
Northeastern University
Seattle, WA 98109 USA

KATINA MICHAEL
School for the Future of Innovation in Society
Arizona State University
Tempe, AZ 85281 USA

PABLO RIVAS
School of Engineering and Computer Science
Baylor University
Waco, TX 76798 USA

LINDSAY J. ROBERTSON
Tech-Vantage
New Plymouth, New Zealand

MICHAEL ZIMMER
School of Computer Science
Marquette University
Milwaukee, WI 53233 USA

APPENDIX: RELATED ARTICLES

[A1] S. Schwartz, L. G. Guntrum, and C. Reuter, "Vision or threat -awareness for dual-use in the development of autonomous driving," *IEEE Trans. Technol. Soc.*, early access, Jun. 13, 2022, doi: 10.1109/TTS.2022.3182310.

[A2] J. R. Schoenherr, "Insider threats and individual differences: Intention and unintentional motivations," *IEEE Trans. Technol. Soc.*, early access, Jul. 25, 2022, doi: 10.1109/TTS.2022.3192767.

[A3] M. Wigan, "Cyber security and securing subjective patient quality engagements in medical applications: AI and vulnerabilities," *IEEE Trans. Technol. Soc.*, early access, Jul. 14, 2022, doi: 10.1109/TTS.2022.3190766.

[A4] R. V. Patil, N. P. Ambritta, P. N. Mahalle, and N. Dey, "Medical cyber-physical system s in society 5.0: Are we ready?" *IEEE Trans. Technol. Soc.*, early access, Jun. 23, 2022, doi: 10.1109/TTS.2022.3185396.

[A5] S. Sodagari, "Trends for mobile IoT crowdsourcing privacy and security in the big data era," *IEEE Trans. Technol. Soc.*, early access, Jul. 15, 2022, doi: 10.1109/TTS.2022.3191515.

[A6] T. Reinhold and C. Reuter, "Towards a cyber weapons assessment model-assessment of the technical features of malicious software," *IEEE Trans. Technol. Soc.*, early access, Dec. 1, 2021, doi: 10.1109/TTS.2021.3131817.

ACKNOWLEDGMENT

The authors would like to acknowledge the editorial support of Terri Bookman LLC in preparing this manuscript for publication.

REFERENCES

[1] *United Nations Development Programme, Human Development Report*. New York, NY, USA: Oxford Univ. Press, 1994, p. 22.

[2] S. Alkire, "A conceptual framework for human security," CRISE, Dept. Int. Develop. London, U.K., Univ. Oxford, Oxford, U.K., Working Papers, 2016. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:d2907237-2a9f-4ce5-a403-a6254020052d

[3] R. Abbas, K. Michael, M. G. Michael, C. Perakslis, and J. Pitt, "Machine learning, convergence digitalization, and the concentration of power: Enslavement by design using techno-biological behaviors," *IEEE Trans. Technol. Soc.*, vol. 3, no. 2, pp. 76–88, Jun. 2022, doi: 10.1109/TTS.2022.3179756.

[4] K. Michael, R. Abbas, P. Jayashree, R. J. Bandara, and A. Aloudat, "Biometrics and AI bias," *IEEE Trans. Technol. Soc.*, vol. 3, no. 1, pp. 2–8, Mar. 2022, doi: 10.1109/TTS.2022.3156405.

[5] K. Michael, R. Abbas, G. Roussos, E. Scornavacca, and S. Fosso-Wamba, "Ethics in AI and autonomous system applications design," *IEEE Trans. Technol. Soc.*, vol. 1, no. 3, pp. 114–127, Sep. 2020, doi: 10.1109/TTS.2020.3019595.

[6] N. Gan. "China's bank run victims planned to protest. Then their Covid health codes turned red." Jun. 2022. Accessed: Aug. 16, 2022. [Online]. Available: https://edition.cnn.com/2022/06/15/china/china-zhengzhou-bank-fraud-health-code-protest-intl-hnk/index.html

[7] S. Akter *et al.*, "Algorithmic bias in data-driven innovation in the age of AI," *Int. J. Inf. Manag.*, vol. 60, Oct. 2021, Art. no. 102387. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2021.102387

[8] R. Paris, "Human security: Paradigm shift or hot air?" *Int. Security*, vol. 26, no. 2, pp. 87–102, 2001.

[9] J. T. Mathews, "Redefining security," *Foreign Affairs*, vol. 68, no. 2, pp. 162–177, 1989. [Online]. Available: https://doi.org/10.2307/20043906

[10] M. N. Gasson and B. J. Koops, "Attacking human implants: A new generation of cybercrime," *Law Innov. Technol.*, vol. 5, no. 2, pp. 248–277, 2013.

[11] N. Bostrom, "The vulnerable world hypothesis," *Global Policy*, vol. 10, no. 4, pp. 455–476, Nov. 2019. [Online]. Available: https://nickbostrom.com/papers/vulnerable.pdf

[12] K. Michael, "Social and organizational aspects of information security management," in *Proc. IADIS e-Society*, Algarve, Portugal, Apr. 2008, pp. 1–9.

[13] R. Contu *et al.* "Emerging technologies and trends impact radar: Security." Gartner Research. Sep. 2020. Accessed: Aug. 24, 2022. [Online]. Available: https://www.gartner.com/en/documents/3991219

[14] C. Brooks. "Emerging tech impacting the security industry." Forbes. Aug. 2018. Accessed: Aug. 24, 2022. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2018/08/22/emerging-tech-impacting-the-security-industry/?sh=4e802da85429

[15] H. Lye. "Mitigating security risks from emerging technologies." Army Technology. Sep. 2019. Accessed: Aug. 8, 2022. [Online]. Available: https://www.army-technology.com/analysis/mitigating-security-risks-from-emerging-technologies/

[16] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy," *Ann. Oper. Res.*, to be published. [Online]. Available: https://doi.org/10.1007/s10479-022-04844-8

[17] B. Pace. "Emerging technologies: Securing manufacturing and critical infrastructure." Gartner: Blog Post. Nov. 2020. [Online]. Available: https://blogs.gartner.com/barika-pace/emerging-technologies-securing-manufacturing-and-critical-infrastructure/

[18] "Innovation: Global issues." WeForum: Strategic intelligence. Mar. 2014. [Online]. Available: https://intelligence.weforum.org/topics/a1Gb0000000LrSOEA0?tab=publications

[19] "Mana' is '(verb) to be legal, effectual, binding, authoritative, valid"' Maori Dictionary. Accessed: Aug. 20, 2022. [Online]. Available: https://maoridictionary.co.nz/word/3424

[20] C. Weber, "Engineering bias in AI," *IEEE Pulse*, vol. 10, no. 1, pp. 15–17, Jan./Feb. 2019, doi: 10.1109/MPULS.2018.2885857.

[21] A. Radford, J. Wu, R. Child, D. Luan, D. Amodei, and I. Sutskever, "Language models are unsupervised multitask learners," *OpenAI Blog*, vol. 1, no. 8, p. 9, Feb. 2019.

[22] A. Ramesh *et al.*, "Zero-shot text-to-image generation," in *Proc. Int. Conf. Mach. Learn.*, Jul. 2021, pp. 8821–8831.

[23] K. Michael. "Meet Boston Dynamics' LS3—The latest robotic war machine." Oct. 2012. The Conversation. Accessed: Aug. 24, 2022. [Online]. Available: https://theconversation.com/meet-boston-dynamics-ls3-the-latest-robotic-war-machine-9754

[24] J. Vincent. "Former go champion beaten by DeepMind retires after declaring AI invincible." 2019. Accessed: Aug. 20, 2022. [Online]. Available: https://www.theverge.com/2019/11/27/20985260/ai-go-alphago-lee-se-dol-retired-deepmind-defeat

[25] N. Slonim *et al.*, "An autonomous debating system," *Nature*, vol. 591, pp. 379–384, Mar. 2021. [Online]. Available: https://doi.org/10.1038/s41586-021-03215-w

[26] M. Aparks, "No sign of a machine mind yet," *NewScientist*, vol. 254, no. 3391, p. 9, Jun. 2022. [Online]. Available: https://doi.org/10.1016/S0262-4079(22)01039-9

[27] M. Sparkes. "Has Google's LaMDA artificial intelligence really achieved sentience?" NewScientist. Jun. 2022. Accessed: Aug. 2, 2022. [Online]. Available: https://www.newscientist.com/article/2323905-has-googles-lamda-artificial-intelligence-really-achieved-sentience

[28] A. F. Winfield, K. Michael, J. Pitt, and V. Evers, "Machine ethics: The design and governance of ethical AI and autonomous systems [scanning the issue]," *Proc. IEEE*, vol. 107, no. 3, pp. 509–517, Mar. 2019, doi: 10.1109/JPROC.2019.2900622.

[29] E. Musk. "Elon Musk warns Governors: Artificial intelligence poses 'existential risk"' Nov. 2017. [Online]. Available: NPR.org

[30] C. I. Gutierrez, G. E. Marchant, and K. Michael, "Effective and trustworthy implementation of AI soft law governance," *IEEE Trans. Technol. Soc.*, vol. 2, no. 4, pp. 168–170, Dec. 2021, doi: 10.1109/TTS.2021.3121959.

[31] K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT, USA: Yale Univ. Press, 2021.

[32] L. Robertson, A. M. Aneiros, and K. Michael, "A theory of exposure: Measuring technology system end user vulnerabilities," in *Proc. IEEE Int. Symp. Technol. Soc. (ISTAS)*, 2017, pp. 1–10, doi: 10.1109/ISTAS.2017.8319089.

[33] L. J. Robertson, "The technological 'exposure' of populations; characterisation and future reduction," *Futures*, vol. 121, Aug. 2020, Art. no. 102584, doi: 10.1016/j.futures.2020.102584.

[34] R. Abbas and A. Munoz, "Designing antifragile social-technical information systems in an era of big data," *Inf. Technol. People*, vol. 34, no. 6, pp. 1639–1663, 2021. [Online]. Available: https://doi.org/10.1108/ITP-09-2020-0673

[35] M. van Zadelhoff. "The biggest cybersecurity threats are inside your company." Harvard Business Review. Sep. 2016. Accessed: Aug. 2, 2022. [Online]. Available: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[36] D. Georgiev. "22 insider threat statistics to look out for in 2022." TechJury. 2022. Accessed: Aug. 2, 2022. [Online]. Available: https://techjury.net/blog/insider-threat-statistics

Tamara Bonaci received the B.Sc. degree from the University of Zagreb, Zagreb, Croatia, in 2008, and the M.Sc. and Ph.D. degrees from the University of Washington, Seattle, WA, USA, in 2011 and 2015, respectively.

She is an Assistant Teaching Professor with the Khoury College of Computer Sciences, Northeastern University Seattle, Seattle, and an Affiliate Assistant Professor with the Department of Electrical and Computer Engineering, University of Washington. Her research interests focus on security and privacy of biomedical technologies, with an emphasis on emerging technologies. Some technologies she has been focusing on in recent years include teleoperated robots, brain–computer interfaces, deep-brain stimulators, bionic eyes, AR/VR devices, and femtech. She is actively involved in computer science education and curriculum development, with a special focus on education and mentoring in the areas of privacy engineering, cyber security, and societal impact of technology. She feels very strongly about diversity in engineering, and about bringing and retaining underrepresented minorities in STEM.

Katina Michael (Senior Member, IEEE) received the Bachelor of Information Technology degree from the School of Mathematical and Computing Science, University of Technology, Sydney, NSW, Australia, in 1996, the Doctor of Philosophy degree in information and communication technology from the Faculty of Informatics, University of Wollongong, Wollongong, NSW, Australia, in 2003, and the Master of Transnational Crime Prevention degree from the Faculty of Law, University of Wollongong in 2009.

Since 2018, she has been a Tenured Professor with the School for the Future of Innovation in Society and the School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ, USA. She is also the Director for the Society Policy Engineering Collective, and a Senior Global Futures Scientist with the College of Global Futures. She is the Founding Chair of the Master of Science in Public Interest Technology with ASU and has hosted the PIT Colloquium since 2020. She was a Professor with the School of Computing and Information Technology, University of Wollongong from 2002 to 2020 and the Associate Dean (International) of the Faculty of Engineering and Information Sciences, University of Wollongong from 2013 to 2017 overseeing eight partner and twinning arrangements throughout Asia and the Middle East. She has previously been employed as a Senior Network Engineer with Nortel Networks, Wollongong, from 1996 to 2001. She has also worked as a Systems Analyst with Andersen Consulting, North Sydney, NSW, Australia, and OTIS Elevator Company, Minto, NSW, Australia. She has published hundreds of peer-reviewed papers, over 20 special issues, and authored and edited several books. She researches predominantly in the area of emerging technologies and their ethical, legal, and social implications.

Prof. Michael has received U.S. $7.5 million in national funding from the National Science Foundation, the Canadian Social Sciences Research Council, and the Australian Research Council. The grants have related to the design and manufacture of biomedical devices and implants with the goal to develop use-inspired and human-centered devices; adaptive AI training systems in manufacturing; citizen-centered smart cities and smart living; fostering responsible innovation through critical by design methods, and location-based services regulation. She is the Founding Editor-in-Chief of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, and was formerly the Editor-in-Chief of the *IEEE Technology and Society Magazine*. She was also a Senior Editor of the *IEEE Consumer Technology Magazine* from 2015 to 2022, an Editor of the *Computer & Security* from 2012 to 2013, and the Technical Editor of the *Journal of Theoretical and Applied Electronic Commerce Research* from 2005 to 2011. She was the Chair of the IEEE International Symposium on Technology and Society from the University of Wollongong in 2010, the University of Toronto in 2013, and Arizona State University in 2020. Most recently, she was the Executive Chair of the IEEE International Symposium on Digital Privacy and Social Media, San Jose, CA, USA, in 2022. She has also ran an international workshop on the Social Implications of National Security (SINS) since 2006 focused on human factors of emerging technologies.

Pablo Rivas (Senior Member, IEEE) received the B.S. degree in computer systems engineering from the Nogales Institute of Technology, Nogales, Mexico, in 2003, the M.S. degree in electrical engineering from the Chihuahua Institute of Technology, Chihuahua, Mexico, in 2007, and the Ph.D. degree in electrical and computer engineering from The University of Texas at El Paso, El Paso, TX, USA, in 2011.

He has been an Assistant Professor of Computer Science with the School of Engineering and Computer Science, Baylor University, Waco, TX, USA, since 2020. Before that, he was with the School of Computer Science and Mathematics, Marist College, Poughkeepsie, NY, USA, from 2015 to 2020. He has more than eight years of industry experience as a Software Engineer and has been recognized for his creativity and academic excellence. He has published several peer-reviewed papers and authored a book on deep learning in 2020. He predominantly researches artificial intelligence and its ethical and social implications, focusing on computer vision, natural language processing, and quantum machine learning.

Dr. Rivas is a member of the IEEE Standards Association and is involved in the working groups developing the P70XX series standards for AI ethics. In 2011, he was inducted into the international honor society for IEEE Eta Kappa Nu; in 2021, he was inducted into Upsilon Pi Epsilon, the international honor society for the computing and information disciplines; and in 2022, he was elevated to Senior Member of ACM. He is currently in the planning phase of the Center for Standards and Ethics in Artificial Intelligence (http://cseai.center/) with funding from the National Science Foundation.

Lindsay J. Robertson received the B.E. degree from Canterbury University, Christchurch, New Zealand, in 1976, the M.Tech. degree from Massey University, Palmerston North, New Zealand, in 1990, and the Ph.D. degree from the University of Wollongong, Wollongong, NSW, Australia, in 2017 on the theme of technological risk, exposure, and resilience.

From 1976 to 1987, he held positions with the New Zealand Government, from 1990 to 2007, he worked with Fonterra (and NZ Dairy) Research Centre, Palmerston North, and he was a Principal Engineer with Parsons Brinckerhoff from 2007 and 2016. He is currently a Principal Engineer with WSP, Montreal, QC, Canada.

Dr. Robertson was the Editor-in-Chief of *IPENZ Transactions* from 2002 to 2016. He has been a Fellow of the Institution of Professional Engineers in New Zealand (IPENZ) since 1999 and the Institution of Mechanical Engineers, U.K., since 2013.

Michael Zimmer received the B.B.A. degree from the University of Notre Dame, Notre Dame, IN, USA, in 1994, and the M.A. and Ph.D. degrees in media, culture, and communication from New York University, New York, NY, USA, in 2002 and 2007, respectively.

He has been an Associate Professor of Computer Science with Marquette University, Milwaukee, WI, USA, since 2019, and was previously on the faculty of the School of Information Studies, University of Wilsconsin–Milwaukee, Milwaukee, WI, USA, from 2008 to 2019. He is the Director of Marquette's Center for Data, Ethics, and Society, and is an Affiliated Fellow with the Information Society Project, Yale Law School, New Haven, CT, USA, as well as Northwestern Mutual Data Science Institute, Milwaukee. With a background in communication and Internet studies, science and technology studies, and information policy and ethics, he uses mixed methods to help reveal the social and ethical dimensions of our contemporary digital ecosystem. Recent projects have focused on both quantitative and qualitative investigations into the privacy and ethical dimensions of big data and computational social science research, wearable fitness trackers, intelligent personal assistants, the application of artificial intelligence in various healthcare settings, and surveillance practices during the COVID-19 pandemic.

Dr. Zimmer currently serves on the SIGCHI Research Ethics Committee and the AoIR Ethics Working Group, and sits on numerous other advisory and editorial boards.