I'm delighted to be the new editor in chief of IEEE Security & Privacy; these are exciting times to be examining issues in security, privacy, and dependability. Nearly every day, a relevant news article or program points to cybersecurity issues that affect us: targeted advertising, information sharing, network breaches, cyberdefense policy, and more. Readers of this magazine are practitioners, researchers, and policymakers, and these daily reminders challenge our assumptions and talents in all realms addressed by S&P: security, privacy, reliability, trust, and policy.

Last year, we celebrated the magazine’s 10th anniversary by examining some of these challenges. In our first decade, S&P authors examined the ways in which we were building dependable, secure systems as well as how effective our approaches have been. These investigations were not done in isolation; in our columns, departments, articles, interviews, podcasts, and special features, we probed and prodded in the context of the wider world, including economics, human behavior, education and training, public policy, and national and international security.

In taking the reins of S&P as it begins its second decade, I want to build on the strong foundation I inherit from my predecessors, George Cybenko, Carl Landwehr, and John Viega. How can this magazine contribute to making security, privacy, and dependability more mature and more scientific? More generally, what is the trajectory of a discipline as it becomes more mature, and how do thought and action move toward a solid basis in understanding and principle?

The history of Western thought offers a useful example. In *Radical Enlightenment: Philosophy and the Making of Modernity 1650–1750* (Oxford University Press, 2001), Jonathan Israel notes that, until the Age of Enlightenment, Western civilization “was based on a largely shared core of faith, tradition and authority.” We can say the same about many aspects of security, privacy, and dependability: we’ve spent a decade describing the threats and risks, the actions taken to address them, and the results. We sometimes take action based on standards and best practices, tempered by our experience and often influenced by the technique du jour. In other words, in many cases, our actions rest on the shifting sands of faith, tradition, and authority.

In the 17th century, the move toward a scientific examination of the foundation of knowledge was prompted by philosophers such as Rene Descartes, whose call for enlightened thinking separate from church doctrine heralded an era in which assumptions were questioned and cause and effect explored. In *The Philosophy of the Enlightenment* (Princeton University Press, 1951), Ernst Cassirer calls enlightenment the path to achieving “clarity and depth in its understanding of its own nature and destiny, and of its own fundamental character and mission.” Perhaps “enlightened security” is our next stage in becoming a more mature and solid discipline. Accordingly, we at S&P plan to take a closer look at two essential elements that will move cybersecurity closer to being a science as well as a craft: why we do what we do, and what we know about cause and effect.

The English word *science* derives from the Latin *scientia*, meaning knowledge. In *The Character of Physical Law* (British Broadcasting Corporation, 1965), Richard Feynmann suggests that scientific knowledge relies on laws that can be used to predict some phenomena of interest; he points out that there is “a pattern between the phenomena of nature which is not apparent to the eye, but only to the eye of analysis.” In *Bad Science* (Harper Collins, 2009),
A Prestigious Honor

Two members of IEEE Security & Privacy’s editorial board were recently inducted into the National Cyber Security Hall of Fame (www.cybersecurityhallofame.com). Congratulations to Carl Landwehr and Peter Neumann!

Ben Goldacre confirms that good science makes us better researchers, practitioners, and citizens, but that bad science can mislead us, providing unwarranted confidence in a tool or technique. It’s important for us not only to enlighten security in a scientific way but to ensure that the science is appropriate and rigorous. So how will we move toward enlightened security? By documenting and testing our assumptions and “best practices” and exploring where, when, and why our techniques and tools work best, via research designs that are ethical and appropriate.

To those ends, we’re making some changes to the magazine:

- **Improving reader experience.** Our readers are a heterogeneous lot, an international set of practitioners, policymakers, and researchers interested in security, privacy, and reliability. The introduction to each article will point out what each type of reader will learn by reading it, and sidebars and related content in our Up to Speed department (sometimes still Basic Training) will provide background information for those seeking to understand or master a new topic.

- **Unveiling research findings.** Our magazine brings you accessible articles about mature research, accompanied by explorations of key issues that affect policy and practice. Our On the Horizon department will continue to focus on research findings that hold great promise for solving or mitigating current problems in the future. We’re also placing more emphasis on reports about industry experience from the trenches about what industry needs and how researchers can more directly address them. Our new Security by the Numbers department will report on how we’re doing this quantitatively—for example, what’s the real cost of cybercrime? Is the number of attacks going up or down? How is cybersecurity related to GDP?

- **Improving the author experience.** We’re updating our guidelines for authors, asking them to describe the audience they want to reach and the assumptions they have made about the technique, idea, or tool being described. We want our authors to explain the motivation for the question being addressed, the concepts needed to understand the research approach, the application of the research outcomes, and any limitations in conducting the study or applying the results. Importantly, if the research involves an experiment or survey, we’ll ask our authors to describe the number and kinds of people involved in the study, and how well they represent the population that will be using or affected by the tool, technique, or policy involved.

- **Expanding coverage to reflect our mission.** This magazine is supported jointly by the IEEE Computer Society and the IEEE Reliability Society. Because reliability and security are clearly intertwined, we’re expanding our coverage of reliability and dependability issues to paint a clearer picture of the state of software and systems. Our News Briefs department now has four sections: security, privacy, policy, and dependability, with three editors trawling the media to bring you interesting and relevant highlights of significant events. We’re also making sure that our special issues address reliability directly or as part of the topic being covered. Similarly, we’re highlighting areas in privacy and policy.

- **Learning from other disciplines.** We all know that people are important to security, privacy, and reliability as designers, builders, maintainers, and users. But sometimes our articles reflect only the technology, without providing the larger context. Consequently, we’re introducing In Our Orbit: a department describing principles and findings from other disciplines that can have bearing on security, reliability, and privacy. We’ll hear from anthropologists, lawyers, economists, legislative staff, and other professionals whose experience and expertise can help us enlighten the way we think about and practice security, privacy, and reliability.

- **Highlighting and exploring controversies.** Because many aspects of our field are quite controversial, S&P will present both sides in a point-counterpoint debate. Experts will examine conflicting sides of issues such as the effectiveness of profiling, the risks inherent in autonomous vehicles, and the costs and benefits of targeted advertising, so that you can make informed decisions at home and on the job.

We hope that these changes will enrich your S&P experience, and we welcome your feedback.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.