Prolog to the Section on Privacy and Cybersecurity

By Carl Landwehr, *Senior Member IEEE*

The ancient word "security" originated from the Latin *securitas*, meaning freedom from anxiety or care, according to the Oxford English Dictionary (OED) [1]. In September 2011, the OED added a new definition to its entry for security:

> 2. Freedom from danger or threat: e. with reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc.

"Cybersecurity" is a recent term for security in cyberspace. Cyberspace, according to one dictionary available there [2], is "the electronic medium of computer networks, in which online communication takes place." The OED tells us "cyberspace" was apparently coined by William Gibson in a 1982 science fiction short story. Earlier terms for security in computing and communications systems include "information assurance," "information security," and "computer security."

A hundred years ago, the closest ancestor to cyberspace may have been the telephone networks, since they provided person-to-person communication in real time, but the only "space" was the space of telephone numbers. The telegraph networks required intermediaries and wireless communications were nascent. The people behind the telephone numbers were a rich resource, but were not really part of the infrastructure, so perhaps it was a 1-D space.

This article introduces a paper that forecasts the future of privacy and cybersecurity in the next 10, 20, 50, and 100 years from the perspectives of theory and algorithms, technology, policy, and economics.

The advent of person-to-person e-mail communications via the Arpanet and Internet in the 1970s added a new dimension to the space of telephone networks, but only the advent of the World Wide Web in the early 1990s brought the feeling of a third dimension, a true "space," providing instant access to information that is continuously evolving and also connected to people as perhaps Gibson envisioned.

Privacy is:

> 1. the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.

According to the primary OED definition. Privacy has avoided being conjoined with "cyber" in the OED, but not in the U.S. Legislature, where a "Cyber Privacy" act was introduced in 2010 [3] (but not passed). This proposed legislation incorporated the now common idea of private information as being information over which the subject can exercise some control, in this case over its removal from an Internet website, rather than information which is entirely secluded.

An eloquent, and still relevant, discussion of the tension between needs of record keepers and the rights of individuals to know about, consent to, correct, and control the use of records that include their personal data was provided nearly 40 years ago in a report [4] advising the U.S. Secretary of Health, Education, and Welfare. More recently, philosopher Helen Nissenbaum has developed the idea that privacy violation comes when the subject of information intended to be used in one context (e.g., medical) escapes to a different context (e.g., commercial) without the subject's permission—thus privacy corresponds to what Nissenbaum terms "contextual integrity" [5].

In the following paper, "Privacy and cybersecurity: The next 100 years," five expert (and dauntless) authors forecast the future of privacy and cybersecurity in the next 10, 20, 50, and 100 years from the perspectives of theory and algorithms, technology, policy, and economics. They expect that on awakening, a future Rip van Winkle will find that some untoward event has triggered regulatory or economic pressures that have reduced the vulnerabilities of deployed systems and that we have developed a better understanding of how to design and build systems able to enforce specified policies. However, he will also find that those systems still have bugs and are subject to attack, and that the privacy policies to be enforced are surprising. ■

The author is with University of Maryland, College Park, MD 20742 USA (e-mail: Carl.Landwehr@gmail.com).

Digital Object Identifier: 10.1109/JPROC.2012.2189820

0018-9219/$31.00 ©2012 IEEE

REFERENCES

[1] Oxford English Dictionary, 3rd ed. Oxford, U.K.: Oxford Univ. Press, Nov. 2010, online version Dec. 2011. [Online]. Available: http://www.oed.com/

[2] Farlex, The Free Dictionary. [Online]. Available: http://www.thefreedictionary.com/cyberspace

[3] U.S. 111th Congress, H.R. 5108—Cyber Privacy Act. [Online]. Available: http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.5108

[4] U.S. Department of Health, Education, and WelfareRecords, computers, and the rights of citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Jul. 1973. [Online]. Available: http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[5] H. Nissenbaum, "A contextual approach to privacy online," *Daedelus*, vol. 140, no. 4, pp. 32–48, Fall 2011.

ABOUT THE AUTHOR

Carl Landwehr (Senior Member, IEEE) received the B.S. degree in engineering and applied science from Yale University, New Haven, CT, and the M.S. and Ph.D. degrees in computer and communication sciences from the University of Michigan, Ann Arbor.

He has conducted research in computer science for more than three decades, primarily in what is now referred to as cybersecurity and was earlier called computer security, information security, and information assurance. For the past decade he has assisted in creating, funding and managing cybersecurity research programs for the U.S. National Science Foundation, the Intelligence Advanced Research Projects Activity (IARPA), and the Defense Advanced Research Projects Agency (DARPA) while serving as a Senior Research Scientist at the University of Maryland, College Park, and a Senior Fellow at Mitretek Systems, Falls Church, VA. For more than two decades prior, he led a research group in computer security at the U.S. Naval Research Laboratory, Washington, DC. He is now employed as an independent consultant.

Dr. Landwehr has received awards from the IEEE Computer Society, the Association for Computing Machinery (ACM) Special Interest Group on Security, Audit and Control (SIGSAC), the International Federation for Information Processing (IFIP), and the National Science Foundation (NSF) for distinguished service.