Practicing a Science of Security

A Philosophy of Science Perspective

Jonathan M. Spring
University College London
London
jspring@cs.ucl.ac.uk

Tyler Moore
The University of Tulsa
Tulsa, OK
tyler-moore@utulsa.edu

David Pym
University College London
London
Alan Turing Institute
d.pym@ucl.ac.uk

ABSTRACT

Our goal is to refocus the question about cybersecurity research from ‘is this process scientific’ to ‘why is this scientific process producing unsatisfactory results’. We focus on five common complaints that claim cybersecurity is not or cannot be scientific. Many of these complaints presume views associated with the philosophical school known as Logical Empiricism that more recent scholarship has largely modified or rejected. Modern philosophy of science, supported by mathematical modeling methods, provides constructive resources to mitigate all purported challenges to a science of security. Therefore, we argue the community currently practices a science of cybersecurity. A philosophy of science perspective suggests the following form of practice: *structured observation to seek intelligible explanations of phenomena, evaluating explanations in many ways, with specialized fields (including engineering and forensics) constraining explanations within their own expertise, inter-translating where necessary.* A natural question to pursue in future work is how collecting, evaluating, and analyzing evidence for such explanations is different in security than other sciences.

KEYWORDS

security research; science of security; cybersecurity; history of science; philosophy of science; ethics of security

ACM Reference Format:
Jonathan M. Spring, Tyler Moore, and David Pym. 2017. Practicing a Science of Security: A Philosophy of Science Perspective. In *Proceedings of 2017 New Security Paradigms Workshop (NSPW 2017).* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3171533.3171540

Note. The DOI may not yet be live. The paper is available at http://www.cs.ucl.ac.uk/staff/D.Pym/NSPW2017.pdf in the mean time.

NSPW 2017, October 1–4, 2017, Santa Cruz, CA, USA

ACM ISBN 978-1-4503-6384-6/17/10.
https://doi.org/10.1145/3171533.3171540

PRACTICING A SCIENCE OF SECURITY: A PHILOSOPHY OF SCIENCE PERSPECTIVE

Jonathan M. Spring,[1] Tyler Moore[2], David Pym[1,3]

1: University College London   2: University of Tulsa   3: Alan Turing Institute

Published and presented at NSPW 2017

Proceedings of 2017 New Security Paradigms Workshop, Santa Cruz, CA, USA, October 1–4, 2017 DOI: 10.1145/3171533.3171540

Abstract

Our goal is to refocus the question about cybersecurity research from 'is this process scientific' to 'why is this scientific process producing unsatisfactory results'. We focus on five common complaints that claim cybersecurity is not or cannot be scientific. Many of these complaints presume views associated with the philosophical school known as Logical Empiricism that more recent scholarship has largely modified or rejected. Modern philosophy of science, supported by mathematical modeling methods, provides constructive resources to mitigate all purported challenges to a science of security. Therefore, we argue the community currently practices a science of cybersecurity. A philosophy of science perspective suggests the following form of practice: *structured observation to seek intelligible explanations of phenomena, evaluating explanations in many ways, with specialized fields (including engineering and forensics) constraining explanations within their own expertise, inter-translating where necessary.* A natural question to pursue in future work is how collecting, evaluating, and analyzing evidence for such explanations is different in security than other sciences.

Definitions

Scientific "a very prestigious label that we apply to those bodies of knowledge reckoned to be most solidly grounded in evidence, critical experimentation and observation, and rigorous reasoning" [6, p. 1].

Security "measures taken to protect a system" [18].

Contact Info

jonathan.spring.15@ucl.ac.uk

Supposed reasons Science of Security does not work, and counterarguments

Complaint	Modern counter-perspective
Untenable experiments	Structured observations more broadly, not just experiments, are necessary for science. Qualitative research methods [11] such as case studies [22], and natural experiments [16], provide usable intellectual structure. Privacy and ethical concerns have been adequately addressed by the Menlo report [7]. Rapid technological change makes generalization of results a genuine challenge, but generalization tactics should help [17, 21].
Reproducibility is impossible	Reproduction comes in many forms (corroboration, statistical power, repetition, etc.) and usually several, though rarely all, work [8, 23]. The misconception is requiring all forms simultaneously, which is overkill. For a historical touch point, see [3]. Traditional scientific work sometimes covers non-replicable events, e.g., the extinction of the dinosaurs [12].
No laws of nature	'Law' interprets how scientists explain or generalize knowledge, but is too rigid even to describe physics [2]. Causal explanation as intervention is well-developed [25, 13, 14]. Philosophy of science provides access to a rich set of mechanism discovery heuristics used in other sciences [1, 4, 5] that can be productively ported to security [20]. These heuristics for designing and interpreting observations are not available with 'laws' as our goal.
No single ontology	A single language does not define a field. Within physics, the subfields communicate via trading zones in which specialized languages enable exchanges between the jargons of two subfields [9]. Trading zones apply in security as well [10]. Neuroscience provides a better metaphor for demarcating a science of security: the mosaic unity coheres from multiple subfields providing constraints on multi-level mechanistic explanations [4].
'Just' engineering	Subsuming engineering under science [19] or science under engineering [15] is not satisfying. Engineering as usually practiced depends on science [24], while at the same time science as usually practiced depends on engineering [6]. Our tentative working definition differentiates based on the goals: engineering is forward-looking, but science tries to generalize models from structured observations. By this definition, a science of cybersecurity clearly exists.

References

[1] BECHTEL, W., AND RICHARDSON, R. C. *Discovering complexity: Decomposition and localization as strategies in scientific research*, 1st ed. Princeton University Press, Princeton, NJ, 1993.

[2] CARTWRIGHT, N. *How the Laws of Physics Lie.* Clarendon Press, Oxford, 1983.

[3] CARTWRIGHT, N. Replicability, reproducibility, and robustness: Comments on Harry Collins. *History of Political Economy 23*, 1 (1991), 143–155.

[4] CRAVER, C. F. *Explaining the brain: mechanisms and the mosaic of unity of neuroscience.* Oxford University Press, 2007.

[5] DARDEN, L. *Reasoning in Biological Discoveries: Essays on Mechanisms, Interfield Relations, and Anomaly Resolution.* Cambridge University Press, 2006.

[6] DEAR, P. *The intelligibility of nature: How science makes sense of the world.* University of Chicago Press, Chicago and London, 2006.

[7] DITTRICH, D., AND KENNEALLY, E. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Tech. rep., U.S. Department of Homeland Security, Aug 2012.

[8] FEITELSON, D. G. From repeatability to reproducibility and corroboration. *ACM SIGOPS Operating Systems Review 49*, 1 (2015), 3–11.

[9] GALISON, P. Trading zone: Coordinating action and belief. *The Science Studies Reader* (1999), 137–160.

[10] GALISON, P. Augustinian and Manichaean science. In *Symposium on the Science of Security* (National Harbor, MD, Nov 29, 2012).

[11] GIVEN, L. M., Ed. *The Sage encyclopedia of qualitative research methods.* Sage, Thousand Oaks, CA, 2008.

[12] GLENNAN, S. Ephemeral mechanisms and historical explanation. *Erkenntnis 72* (2010), 251–266.

[13] HALPERN, J. Y., AND PEARL, J. Causes and explanations: A structural-model approach. Part I: Causes. *The British Journal for the Philosophy of Science 56*, 4 (2005), 843–887.

[14] HALPERN, J. Y., AND PEARL, J. Causes and explanations: A structural-model approach. Part II: Explanations. *The British Journal for the Philosophy of Science 56*, 4 (2005), 889–911.

[15] KOEN, B. V. *Discussion of the method: Conducting the engineer's approach to problem solving.* Oxford University Press, New York, 2003.

[16] MORGAN, M. S. Nature's experiments and natural experiments in the social sciences. *Philosophy of the Social Sciences 43*, 3 (2013), 341–357.

[17] MORGAN, M. S. Resituating knowledge: Generic strategies and case studies. *Philosophy of Science 81*, 5 (2014), 1012–1024.

[18] SHIREY, R. Internet Security Glossary, Version 2. RFC 4949 (Informational), Aug. 2007.

[19] SIMON, H. A. *The sciences of the artificial*, 3rd ed. MIT press, Cambridge, MA, 1996.

[20] SPRING, J. M., AND HATLEBACK, E. Thinking about intrusion kill chains as mechanisms. *Journal of Cybersecurity 2*, 2 (2017).

[21] SPRING, J. M., AND ILLARI, P. Mechanisms and generality in information security. *Under review* (2017).

[22] STAKE, R. E. *The art of case study research.* Sage, Thousand Oaks, CA, 1995.

[23] STODDEN, V. Reproducing statistical results. *Annual Review of Statistics and Its Application 2* (2015), 1–19.

[24] VINCENTI, W. G. *What engineers know and how they know it: Analytical studies from aeronautical history.* Johns Hopkins Studies in the History of Technlogy. Johns Hopkins University Press, Baltimore and London, 1990.

[25] WOODWARD, J. *Making things happen: A theory of causal explanation.* Oxford University Press, Oxford, UK, 2003.

Ask me about our lit review of statements of challenges in Science of Security!

LATEX TikZposter