H-Net Reviews
in the Humanities & Social Sciences

Clement Guitton. *Inside the Enemy's Computer: Identifying Cyber-Attackers.* Oxford: Oxford University Press, 2017. 320 pp. $34.95 (cloth), ISBN 978-0-19-069999-4.

Reviewed by Nicholas Sambaluk (Air University)

Published on H-War (May, 2019)

Commissioned by Margaret Sankey (Air University)

Widespread opinion holds that attribution is one of the thorniest challenges with regard to cybersecurity, because the aspects of anonymity to the internet pose such a formidable technical problem. This book confronts these assumptions and argues that attribution has been commonly misunderstood and mischaracterized. The central and most intriguing point in the book is that attribution is not fundamentally a technical problem and that it should instead be viewed as a process that involves some inherently political dimensions.

There are important merits to this argument, starting with the point that nuance should be added to understandings of deriving attribution. As the author forcefully notes, problems exist in either a solved or unsolved state. However, real-world sleuthing much more commonly involves probable understanding and weight of evidence and analysis rather than a proverbial smoking gun or slam dunk outcome. The pursuit of valid and useful information is, as Clement Guitton observes, much more accurately conceptualized as a process. It might be added, although this does not appear within the book's own argumentation, that this conceptualization of processes rather than solved or unsolved binary cases is valuable beyond simply a more accurate understanding of affairs in cybersecurity, and the topic has been treated in some works about technological and other innovation more broadly. Guitton's conclusions dovetail with some of those findings in a larger context.

Guitton also asserts that attribution is inherently about policy and politics, both for domestic cases and the enforcement of law and for international cases and foreign relations. The author engages with six characteristics often used to ascribe national security relevance to a cyber incident: severity of the attack, political character of the target, the apparent geographic origin of the attack, evident "sophistication" of the attack, and the larger political context. Repeatedly in his work, however, Guitton presents the prevalent viewpoints in order to question their applicability and veracity. For example, in each case for the above six criteria commonly used for deeming an attack to have national security relevance, he offers reasons why these may be insufficient or even misleading. Opportunities to spoof the location of an attack's origin throw the seemingly useful third criterion into serious question, for example.

The pursuit of nuance inserts a distinct element of ambiguity into much of the resulting book. Guitton aims to show the reader that attribution is not an insurmountable technical problem (and not fundamentally a problem of technology alone at all), but the reader is nonetheless pulled back and forth through a series of arguments. The reader is told that attribution is not possible, or valuable, to accomplish in real time—in contrast to figures who opine the apparent need for real-time attribution of attacks. Arguing against this common viewpoint, Guitton notes that "as with the claim by Mandiant towards China" in its report of the first identified Advanced Persistent Threat, "the attribution link remained pertinent despite being made two years after the discovery of the malware" (p. 153).

Thus the reader is to be persuaded that attribution well after the fact is a powerful tool. However, in a different context, Guitton observes that "less than two months after Mandiant's publication, China had resumed using

exactly the same modus operandi to conduct its cyber attacks" (p. 178). There is no concession anywhere that these two statements conflict with each other, despite the fact that their conflict is comparable to the shortcomings of some of the commonplace viewpoints regarding cyberattack attribution that the author works to challenge. Guitton closes his book with a pair of policy recommendations that center on the need for competent and cooperative international law enforcement entities and the importance of clear thinking and analytical methods that spurn bias.

Works of revision frequently strive to add nuance to narratives that might have lacked them earlier. Expressing and explaining this nuance, and pointing accurately and effectively to the topics that require further detail, is complex and challenging to accomplish in a meaningful way. Overall, Guitton's study advances this effort, if not because his work "solves" the problems of our contemporary understanding of cyberattack attribution, then because it adds to the process of developing a more useful framework through which to consider them.