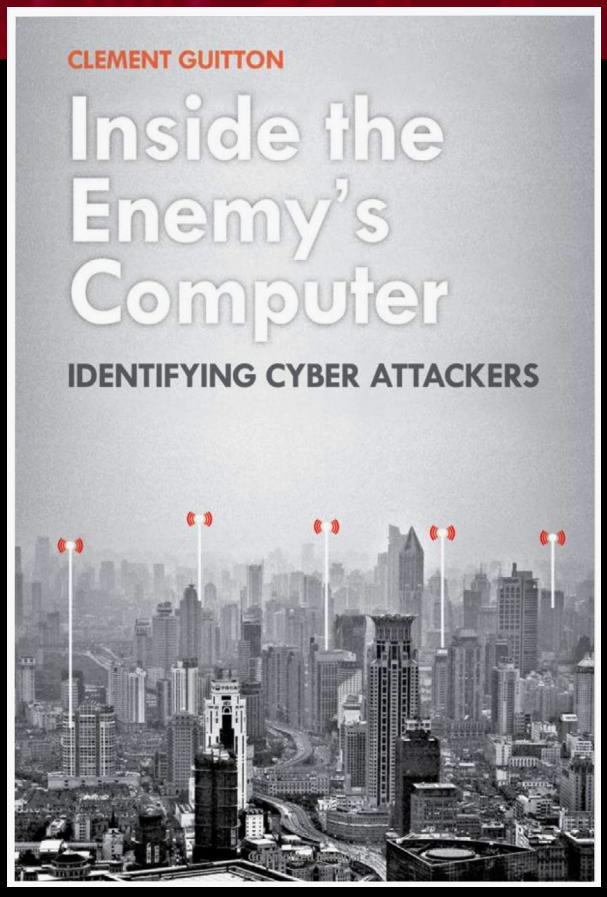
Book Review:
Inside the Enemy's Computer: Identifying Cyber-Attackers by Clement Guitton

Reviewed by Mark T. Peters II, USAF, Retired



Suggested Citation

Peters, Mark T. Review of *Inside the Enemy's Computer: Identifying Cyber-Attackers*, by Clement Guitton. Homeland Security Affairs 16, Article 2. www.hsaj.org/articles/15817

Expanding cyber-domain conflicts challenge modern strategists to create definitive attribution standards for who did what to whom, especially in developing national policy. Attribution's importance was illustrated during Russia's 2017 notPetya ransomware attack against the Ukraine, where Mondelez International's European retail services suffered over $100M in collateral information technology damages. Subsequently, Mondelez filed an insurance claim with their policy holder, Zurich International. However, U.S. and NATO public declarations attributed the NotPetya attack to the Russian state rather than the proxy group who launched the attack. Allowing Zurich to declare state sponsorship created a non-payable policy exclusion, leaving the issue yet to be legally settled.[1] Attribution's rising importance across the global cyber commons makes Clement Guitton's comprehensive analysis in *Inside the Enemy's Computer: Identifying Cyber-Attackers* vital to all readers and expertise areas. Beginning with an analysis of attribution constraints, the book moves rapidly to explore processes rather than individual, event-based problems. Guitton's attribution framework emphasizes differing criminal and national security approaches such as detailing, expert judgement, evidentiary standards, corporate privatization, timeliness, and plausible deniability.

The statement, "Attribution begets action " (186) proves core to Guitton's procedural exploration. If attribution is central to uncovering cyberattack origins, then overall attribution efforts drive intended results including criminal convictions, state sanctions, or retaliatory actions. Effective attribution theories favor legal and political investigations as quoted below:

> *The central argument of this book, and a short answer to the two research questions it investigates, is therefore that the attribution of cyber attacks is a two-pronged political process. The processes are never entirely 'solved', but evolve through different stages depending on the nature of the incident. In many such incidents, the process closely follows a legal path; in others, the incident and its attribution remain within the realm of the executive. However, in both processes the attribution of cyber attacks is not unique, and shares a wealth of common properties with the attribution of either criminal or national security incidents.(11)*

The book addresses common attribution misconceptions regarding technical complexity, hidden origins, and unique appearance while suggesting clear goals to generate effective responses following initial adversary actions. Each framework item fills a chapter and progressively builds through well-documented examples.

Guitton's first step examines assessing cyberattacks with expert judgement. Attribution's political imperatives first emerge from analytical aids such as known suspect lists and foreign IP address origins while using core concepts to frame practices with a predilection towards repeat offenders versus uncovering new actors. States select likely offenders from the previously guilty and blame them rather than conduct costly investigations. Tracking attacks to foreign-based IPs often remains sufficient to satisfy political attribution. Logical fallacies often occur but leave three main reasons supporting attribution: convincing the public, supporting retaliatory efforts, or building patterns for future events. The use of expert judgement leads directly to employed discovery standards.

Guitton then turns to the analysis of discovery standards. Discovery standards illustrate criminal and national security requirements for distinct attribution. In the absence of such standards, each case appears isolated rather than linked to processes. The highlighted criminal case features Data Stream Cowboy's USAF server attack while the highlighted national security case explores Operation Ababil's Stuxnet retaliation on U.S. banking. The U.S. judiciary uses binary guilt and "beyond a reasonable doubt" standards while national security attribution evinces a more nuanced perspective. A six-item national security attribution list appears with items including attack scale, associated technical or geopolitical data, and attack beneficiary. The checklist demonstrates a process to convince national audiences to support retaliatory action without waiting for criminal proof.

Next, the author questions which players possess the technical and political knowledge to identify attacks accurately. Private companies conducting attribution analysis face multiple credibility challenges from factors like past associations, technical expertise, and result quality. This chapter's cases are Mandiant's Chinese Advanced Persistent Threat-1 (APT1) work and Kaspersky Lab's initial Stuxnet reports. Private firms conducting attribution analysis face three political questions: how many former intelligence officials they employ; who benefits from release timing; and why some refuse to name suspected offenders. The author explores how private corporate ownership shifts responsibility from national actors through government contracts.

Timeliness follows knowledge to generate process speed through delivery differences between criminal and national practices. Criminal cases tend towards quick actions, justifying arrest with mere suspicion, and gathering most evidence after arrests. Analysis of the case studies suggests that national attribution favors gathering information during cyberattack events and waiting to formulate retaliatory actions before publicizing theories. These models support the theory of all attribution being political at its core. Public attribution debates sometimes favor instant results. However, this work clearly suggests that context matters more than immediate answers. Citing the discovery of ten new malware items daily with minimal attribution as cybersecurity elements focus on fixes rather than causes, market reports still find that cybersecurity protects the average corporation from $11M in losses yearly even without attribution.[2]

Closing with a contrary approach, Guitton describes how attribution efforts can be countered with plausible deniability. States deferring expert judgement to private companies mitigate incorrect attribution risks just as hacker group proxies reduce state culpability. The book

evaluates cases involving Iranian, Russian, and Syrian proxy groups with techniques including denying sponsorship, staying below attributable thresholds, and technical masking practices. Most deniable practices appear to follow the informal CIA covert operations motto, "admit nothing, deny everything, and counter-accuse" rather than implement complex, technical, and potentially costly, solutions.[3]

An excellent attribution analysis, *Inside the Enemy's Computer* explores a well-defined thesis and key cases. The book is admittedly focused primarily on U.S.-based events and Guitton emphasizes attribution's political nature over technical solutions. Overall, the author adequately sums up his theoretical shortfalls. However, the book could be improved by expanding attribution's historical context, providing comparative charts, and adding a single, baseline case study. The discussion of historical context was limited to the introduction and lacked any comparison for past practices to the new model. Consolidated tables as comparative charts for criminal and national security models would have been helpful also. Finally, detailing one cyber-attack case and following it throughout the work may have increased multidimensional viability.

Overall, *Inside the Enemy's Computer* offers an exceptional strategic attribution analysis and well-developed alternative model. This work should be of interest to anyone who deals regularly with cyber challenges to homeland security. It is highly enjoyable and a quick read, even for those not intimately familiar with cyberspace operational practices. The biggest take away for government policy expert, or intelligence analyst remains Guitton's central comment: "Attribution begets action" (187). Cybersecurity's dynamic nature means technical factors change on a weekly, daily, and hourly basis making excellent attribution processes critical. Guitton describes the necessity to discount purely technical limitations and explore strategic options. Successful analytic models will create standards and study areas without technical restraints. I recommend this text to everyone, but especially those working with cybersecurity, intelligence analysis, or policy issues surrounding the global cyber commons.

About the Author

Dr. Mark Peters retired from the Air Force after 22+ years as an intelligence professional and now works for Technica Corporation as a Security Engineer on a US Air Force Defensive Cyber Weapon System Program Office in San Antonio, TX. During his Air Force career, he deployed five times, worked with a variety of tactical and operational systems, and commanded a space intelligence squadron. Graduated as a Strategic Security specialist, he authored, "Cashing in on Cyberpower" analyzing system-level- economic impacts of over 10 years of cyber-attacks. While originally specializing in military applications, the integration of cybersecurity, threat intelligence, and homeland defense is one of his passions. He may be reached at mpetersii@yahoo.com .

Copyright

Endnotes

1. Brian Corcoran, "What Mondelez v. Zurich May Reveal about Cyber Insurance in the Age of Digital Conflict", Lawfare, (8 Mar 2019), https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

2. Gaurav Pendse, "Cybersecurity: Industry Report & Investment Case", Nasdaq, (25 Jun 2018), https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html

3. N.Y. Times, "Washington Talk: Briefing; Tribute to C.I.A.," (12 Jun 1987). https://www.nytimes.com/1987/06/12/us/washington-talk-briefing-tribute-to-cia.html