# On the Problem of (Cyber) Attribution

**Hal Berghel,** University of Nevada, Las Vegas

*Is the recent report from the three-letter agencies on the alleged Russian hack of the Democratic National Committee evidence-based attribution or attributibabble?*

Attribution is one of those topics that few understand well, but everyone ought to study. It gets at the heart of human cognition—or, perhaps more accurately, what goes wrong with human cognitive processes. Fritz Heider, the father of attribution theory, used it to account for the way humans reconcile perceptions and observations in their quest for understanding.[1] A characteristic of human attribution is fundamental attribution error, whereby perceivers read more into a context than they take from it. Put another way, humans tend to be cognitive misers in that they search for the simplest explanation of events consistent with their disposition, biases, and world view. Nowhere has this been more evident than in the political Rumspringa of the current US president.

Attribution theory has been a staple of modern social psychology since Heider's seminal book. To be sure, there are refinements on the work.[2] But, so far as I know, the refinements don't detract from the theoretical foundation. That said, the public and media have yet to fully appreciate attribution theory and sibling psychological phenomena—a critical flaw in this era of "fake news." Is a feature of human nature to bring cognitive biases to a description of, and inferences from, perceptions? Attitudes and judgments have these biases baked into them. Failing to appreciate this simple fact allows all sundry forms of popular nonsense to remain unchallenged. Such is the case with cyberattribution.

## TECHNICAL CHALLENGES

Any forensics examiner worthy of the name would begin an investigation with the assumption that any adversary is every bit the examiner's equal in terms of proficiency. While this assumption might not hold true, it guides the examiner to first look for hardest evidence, rather than the easiest conclusion to reach. If the adversary lacks the examiner's skills, perhaps the investigation takes a bit longer. However, the most troublesome and fruitless investigations spring from a trail of missed clues. Such is the case with much of the cyberattribution proffered by government agencies and reported in the commercial media in response to the alleged recent hack of the Democratic National Committee (DNC) by Russia. We'll return to this topic below.

By way of background, let's profile a typical state-sponsored cyberadversary. State sponsors have the most resources, and in all likelihood hire those with the strongest skillsets. We might include military cyberwarfare


0018-9162/17/$33.00 © 2017 IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

units like North Korea's Unit 110, China's People's Liberation Army Unit 61398, Israel's Unit 8200, the UK's Government Communications Headquarters (GCHQ), the US National Security Agency, and so forth. It goes without saying that the Russians have similar agencies. In fact, all developed countries have operational cyberwarfare programs, under different auspices and of varying capabilities and budgets. In addition, we must include a coterie of government-financed private security companies (aka "pure plays") for each of these agencies, not to mention a network of individual freelance hackers who also hire out their services.

Such cybermercenaries are well known and their activities well documented, thanks to whistleblowers like Edward Snowden and investigative journalists like James Bamford[3,4] and Tim Shorrock.[5] Corporate players include Stratfor, HBGary/ManTech International, Gamma Group, the Equation Group, Cellebrite, and HackingTeam, to name but a few. The point to bear in mind is that in addition to their own internal apparatuses, state sponsors of cybercrimes, cyberterrorism, and cybersurveillance have a wide variety of private cybermercenary support at their disposal as well. In addition, there's a multimillion-dollar grayware market for malware.[6,7] US intelligence agencies even have a secret procedure to oversee the acquisition and retention of such malware called the Vulnerability Equities Process.[8] But whether the source of the attack is a government agency, corporate cybermercenaries, or independent agents, the source is likely to be highly skilled.

For example, in the case of the FBI decryption of the San Bernardino terrorists' iPhone, the technical expertise needed to circumvent the device's encryption has been attributed to both Cellebrite[9] and freelancers.[10] It's worth noting that state sponsors have nearly endless cyberweapon resources, especially those intelligence agencies connected with the STONEGHOST network made up of the English-speaking Five Eyes countries (the US, the UK, Canada, Australia, and New Zealand).

Attribution theory is relevant to cyberattribution. It's commonly politically motivated. Anup Ghosh, CEO of Invincea, refers to this activity as a blame game. "Nonetheless, many private firms and security researchers are quick to reach a conclusion on who is behind an attack based on code and infrastructure re-use, as well as the tactics, techniques, and protocols (TTPs) they have previously ascribed to bad actors with cute names. The methods typically would not pass a court of law's evidentiary standards, but are good enough for Twitter."[11] His point is well-taken. Politicians and the power elite find it very convenient to engage in this blame game as they seek to discredit adversaries, avoid responsibility for insecure practices and inept leadership, influence politics and elections, and exploit attribution biases in support of cherished big government programs. In the words of singer-songwriter Bruce Hornsby, "That's just the way it is."

So whenever a politician, pundit, or executive tries to attribute something to one group or another, our first inclination should always be to look for signs of attribution bias, cognitive bias, cultural bias, cognitive dissonance, and so forth. Our first principle should be cui bono: What agendas are hidden? Whose interests are being represented or defended? What's the motivation behind the statement? Where are the incentives behind the leak or reportage? How many of the claims have been substantiated by independent investigators? However, these are cerebral questions that require thorough study, unlike viewing footage of police shootings and surfing the web for cats that look like Hitler. That's the reason we see more of the latter from commercial media.

> Humans tend to be cognitive misers in that they search for the simplest explanation of events consistent with their disposition, biases, and world view.

## FAITH-BASED ATTRIBUTION

Faith-based attribution is a term used by security specialist Jeffrey Carr to denote nonscientific analysis that leads to untestable attribution to a security incident. Carr sums this up nicely in a recent article:[12]

> *It's important to know that the process of attributing an attack by a cybersecurity company has nothing to do with the scientific method. Claims of attribution aren't testable or repeatable because the hypothesis is never proven right or wrong. Neither are claims of attribution admissible in any criminal case, so those who make the claim don't have to abide by any rules of evidence (i.e., hearsay, relevance, admissibility).*

As Carr points out, no one holds the private security contractor who makes such claims accountable if they are subsequently proven false because the notion of evidentiary proof is

anathema in this domain. If it's possible, government accountability is even less likely because of secrecy claims and security policies. Further, governments have an effective bully pulpit from which to spawn memes.

Such was the case with the 2014 Sony hack when FBI Director James Comey leveraged familiar "trust me" and "if you only knew what I know" claims to advance a variety of accusational frameworks. This reaffirmed that truth is a moving target for government agencies when it comes to preferred narratives.[13] If this sounds like modern politics to you, it's not coincidental. The same sleight-of-hand tactics are used by political operatives. As we saw in the last election cycle, some politicians are quite comfortable making false claims knowing full well that they'll neither be critically examined nor held up to even a minimal evidentiary standard. We call this political deception. In cyberspace, the same phenomenon is called evidence-free accusation or faith-based attribution. The term faith-based may also be used to describe novice cybersecurity practices as well,[14] and should probably be extended to all political narratives.

But the general phenomena is far more generic than these examples suggest. Long before Comey took on the role of the FBI's chief misattributionist, the controlling elite perfected the art of placing blame for political, economic, or social advantage at the feet of their adversaries. That's how the names of Saddam Hussein, Fidel Castro, and Kim Jong-il entered the popular lexicon. Every empire needs bête noirs to keep the public's adrenaline running high.

## SENSITIVE SOURCES AND METHODS INDEED

The fanfare surrounding the 6 January 2017 report from the Office of the Director of National Intelligence (ODNI) on the recent hack of the DNC[15] seems to be inversely related to the reader's understanding of computing networks. To borrow a phrase from Columbia journalism professor Nicholas Lemann, this report was a "golden-brown wobbly soufflé of speculation." There was no evidence produced, no data revealed, no forensics mentioned—just 13 pages of undocumented opinion by the same folks who claimed that the Soviets were four years away from building an atomic bomb the eve before they detonated one, the USSR would never place missiles in Cuba, China wouldn't get involved in the Korean War, North Vietnam attacked US forces in the Gulf of Tonkin, and Saddam Hussein had weapons of mass destruction, and who failed to foresee both the Iranian revolution and the Soviet Union's collapse. I have no idea whether Vladimir Putin and his cyber hit squad was behind the DNC hack. And based on the report under review, it's an open question whether the security agencies do either. Intelligence services hide behind the mantra that they can't disclose sensitive sources and methods, real or imagined. For want of a better term, we'll call this fantasy intelligence.

Intelligence services hide behind the mantra that they can't disclose sensitive sources and methods, real or imagined. For want of a better term, we'll call this fantasy intelligence.

Let's consider for a moment what these "sensitive sources and methods" might be. Here are a sampling of known knowns to digital forensics experts. First, suspected malware file hashes can be matched against any number of detection programs to identify usual suspects (www.virustotal.com is a good starting point). These programs for the most part use public databases. There's nothing sensitive about this information. Second, any malware can be statically reverse-engineered by de-compilation or disassembly and searched for string signatures that betray anomalies or exploits. Again, no news here. Further, runtime debuggers can be used to dynamically determine linkages and runtime dependencies associated with suspected malware. File headers might reveal compile dates, mnemonics used, file sizes, version numbers, and so forth that provide circumstantial clues to program authors and sources. Of course, state-sponsored cyberunits have the best tools known for these purposes—but even the best tools don't provide prosecutable evidence. The operative point is that there's nothing "sensitive" about any of these information-gathering tools and tactics. They're well known and used worldwide by computer forensicists. The likelihood is that if all of these methods were disclosed to the public, no "sensitive" information would be revealed if only personally identifiable information were redacted.

On the network side, state actors routinely sniff all network traffic they can get their hands on—including, as the disclosures concerning the NSA's bulk data collection programs revealed, information about private citizens not suspected of any crimes and without benefit of court order. So let's assume that the US intelligence agencies have captured all network traffic to and from their suspects and have analyzed them down to the packet level. What would that reveal? If the adversaries are worth their money, very little. It's likely that Russian cybercapability is in a league with our own. Such being the case, the IP addresses, MAC addresses, and ISPs involved in the traffic are very unlikely to be traceable back to Putin, Russia, or the hackers themselves. If the perpetrators are "A Team" hackers, the traffic is more likely to trace back to a daycare center in Milan.

Professional hackers don't leave digital fingerprints on the computer and network resources they use. Script kiddies might, but not professionals. Again, any such information released by the US government is unlikely to disclose anything "sensitive," because all security experts already know these agencies' capabilities, and the "perps" we must assume are every bit the equal of the cybersleuths seeking to out them. Of course, both sides occasionally make mistakes. But a mistake so large as to identify the president of a sovereign nation as involved in hacking another sovereign state is exceedingly improbable. Consider that no forensics traced Stuxnet back to the second Bush administration. Plausible deniability is the matron to every controversial or unpopular big government initiative. As Carr has pointed out, the tangible facts in the DNC breach were distorted by press reports into Disney-like caricatures.[16]

Security experts David Clark and Susan Landau[17] provide an overview of the attribution problem from a defensive perspective. They accurately sum up the problem: "Attribution is central to deterrence ... and the Internet was not designed with deterrence in mind." A more technical description is supplied by David Wheeler and Gregory Larsen.[18] Taken together, these papers are notable for the absence of detailed strategies to provide justiciable, evidence-based cyberattribution. There's a reason for that: there is none. The most we have is informed opinion. And the intelligence agencies that offered such opinions concerning the recent alleged "Russian Activities and Intentions in Recent US Elections" assesment[15] have an exceedingly spotty reputation when it comes to such reports' accuracy.[19,20]

The recent survey of attribution challenges by Earl Boebert[21] is to be recommended in this regard. As Boebert observes, the Internet infrastructure itself works against attribution. Network address translation, the Dynamic Host Configuration Protocol, the triviality of spoofing IP and MAC addresses, the lack of source authentication in DNS registration, proxy servers, encryption, anonymizing services, and the like all work against justiciable cyberforensic attribution

## THAT LEAVES US WITH HUMINT

This is where Fancy Bear and Cozy Bear meet Guccifer 2.0.[22,23] Are the claims about Russian hacking groups' involvement in the DNC breach by Guccifer 2.0, a Russian misinformation specialist, legitimate or meant to deflect criticism? Is he really Romanian? I have no idea, but that misses the central point. There's no way to build confidence in any of this reporting without the ability to follow the incentives—and that's the data that the three-letter agencies are guarding so zealously. I would be remiss if I failed to mention that it was certainly timely that just when the three-letter forefingers were poised to point, Guccifer 2.0 was overcome with grandiloquence. Do the intelligence agencies have the goods on someone? It's impossible to tell from this side of the veil of government secrecy. That's by design.[24]

In any case, state-sponsored cyberwarriors certainly have the technical capacity to identify adversaries biometrically. As I mentioned above, modern intelligence agencies have enormous resources to draw upon, including various cyberweapons merchants and others who provide a cornucopia of communication and media interdiction tools, rootkits, remote session hijacking tools, worms, viruses, zero-day exploits, and sundry other tools to spy on cyberadversaries in situ. That said, the other side has comparable access to such tools and are aware that these tools can be used against them. Rooting a journalists' computer is very different from rooting the computer of a highly skilled security specialist in the employ of a state sponsor. This is very much a case of cyber cat and mouse where neither has the predictably clear advantage. Could Western intelligence agencies root computers of state adversaries? Sure, but it's not very likely unless the target has a rookie asleep at the console.

It's interesting to note that an equally wobbly soufflé of speculation about alleged Trump/Putin ties was offered to the DNC in 2016 by an unnamed paid source.[25] This report, recently made public, has much the same character as the ODNI report: no verifiable claims and no ground-truth data mentioned. While these claims seem vague on the surface, on deep analysis they're seen to be nothing more than attributibabble. This is the stuff of which dime-store novels are made.

> Plausible deniability is the matron to every controversial or unpopular big government initiative.

As Carr points out, there are disincentives to criticizing the received view of anything.[26] The choice of reflection over simple absorption of a received view is intellectually demanding, time-consuming, unlikely to be profitable, and will win few friends among the controlling elite. However, it's precisely this unpopular and unprofitable "truth to power" approach that will yield the truth. The choice intellectuals have before them is between investing in the search for truth or living in the world of alt-facts. The latter is the substance of George Orwell's and Aldous Huxley's dystopia.

I would be remiss if I failed to direct attention to the real problem of the

DNC hack: the content of the emails. A more shameful display of partisan myopia and disregard for democratic principles is difficult to imagine.

## REFERENCES


1. F. Heider, *The Psychology of Interpersonal Relations*, Martino Fine Books, 2015 (originally published 1958).
2. A. Tversky and D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, vol. 185, no. 4157, 1974, pp. 1124–1131.
3. J. Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America*, Anchor, 2009.
4. J. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, Anchor, 2002.
5. T. Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing*, Simon & Schuster, 2009.
6. A. Greenberg, "Shopping for Zero- Days: A Price List for Hackers' Secret Software Exploits," *Forbes*, 23 Mar. 2012; www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.
7. A. Greenberg, "Here's a Spy Firm's Price List for Secret Hacker Techniques," *Wired*, 18 Nov. 2015; www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques.
8. "Vulnerability Equities Process Highlights," 2015; www.wired.com/wp-content/uploads/2015/03/Vulnerability-Equities-Process-Highlights-7.8.10-DOC-65-redactions_Redacted1.pdf.
9. R. Dillet, "The FBI Is Working with Cellebrite to Unlock San Bernardino iPhone, Reports Say," *TechCrunch*, 23 Mar. 2016; techcrunch.com/2016/03/23/fbi-is-working-with-cellebrite-to-unlock-san-bernardino-iphone-reports-say.
10. E. Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *The Washington Post*, 12 Apr. 2016; www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.
11. A. Ghosh, "Playing the Blame Game: Breaking Down Cybersecurity Attribution," *Help Net Security*, 19 Dec. 2016; www.helpnetsecurity.com/2016/12/19/cybersecurity-attribution-blame-game.
12. J. Carr, "Faith-Based Attribution," 10 July 2016; medium.com/@jeffreycarr/faith-based-attribution-30f4a658eabc#.bqsg92u70.
13. H. Berghel, "Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole," *Computer*, vol. 48, no. 2, 2015, pp. 77–80.
14. H. Berghel, "Faith-Based Security,"

*Comm. ACM*, vol. 51, no. 4, 2008, pp. 13–17.
15. Office of the Director of Nat'l Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6 Jan. 2017; www.dni.gov/files/documents/ICA_2017_01.pdf .
16. J. Carr, "Can Facts Slow the DNC Breach Runaway Train?," 26 July 2016; medium.com/@jeffreycarr/can-facts-slow-the-dnc-breach-runaway-train-lets-try-14040ac68a55#.3b569guwt.
17. D.D. Clark and S. Landau, "Untangling Attribution," *Proc. Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Nat'l Research Council, 2010, pp. 25–40.
18. D.A. Wheeler and G.N. Larsen, *Techniques for Cyber Attack Attribution*, IDA Paper P-3792, Inst. for Defense Analyses, Oct. 2003; handle.dtic.mil/100.2/ADA468859.
19. W. Blum, *Killing Hope: U.S. Military and C.I.A. Interventions since World War II*, 2nd ed., Common Courage Press, 2012.
20. T. Weiner, *Legacy of Ashes: The History of the CIA*, reprint ed., Anchor, 2008.
21. W.E. Boebert, "A Survey of Challenges in Attribution," *Proc. Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Nat'l Research Council, 2010, pp. 41–52.
22. J. Carr, "The DNC Breach and the Hijacking of Common Sense," 19 June 2016; medium.com/@jeffreycarr/the-dnc-breach-and-the-hijacking-of-common-sense-20e89dacfc2b#.ocq9keju6.
23. NCCIC/FBI, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, Joint Analysis Report JAR-16-20296, 29 Dec. 2016; www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
24. H. Berghel, "Secretocracy," *Computer*, vol. 49, no. 2, 2016, pp. 63–67.
25. "Trump Intelligence Accusations," contributed 10 Jan. 2017; www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html.
26. J. Carr, "An Attribution Skeptic's FAQ," 28 Dec. 2016; medium.com/@jeffreycarr/an-attribution-skeptics-faq-42805f0ee6b3#.9x128sw0q.

**HAL BERGHEL** is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.