The Scholar

Texas National Security Review: Volume 3, Issue 4 (Fall 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

THE SIMULATION OF SCANDAL: HACK-AND-LEAK OPERATIONS, THE GULF STATES, AND U.S. POLITICS

James Shires

Four hack-and-leak operations in U.S. politics between 2016 and 2019, publicly attributed to the United Arab Emirates, Qatar, and Saudi Arabia, should be seen as the "simulation of scandal" – deliberate attempts to direct moral judgment against their target. Although "hacking" tools enable easy access to secret information, they are a double-edged sword, as their discovery means the scandal becomes about the hack itself, not about the hacked information. There are wider consequences for cyber competition in situations of constraint where both sides are strategic partners, as in the case of the United States and its allies in the Persian Gulf.

Hack-and-leak operations (HLO) are a new frontier in digital forms of foreign interference, epitomized by the success of Russian intelligence agencies in obtaining and disseminating documents from the Democratic National Committee (DNC) during the 2016 U.S. presidential election campaign.[1] HLO and other information operations are widely seen as a severe threat to liberal democratic structures and U.S. policymakers have mobilized significant resources in response, including threat intelligence and cyber security protections, increased election and voting security, legislative pressure on social media companies, and even offensive cyber attacks.[2]

This "whole-of-nation" approach is largely based on the events of the 2016 U.S. election, and specifically Russian interference in the election process.[3] However, it is hard to pinpoint the exact impact of the Russian disinformation operations.[4] Controversial candidates, a combative and polarized media environment, and entrenched economic and social divisions were all key factors in the 2016 election result. Furthermore, foreign interest in the U.S. election was not limited to the Russian government; other state and nonstate actors also sought to influence candidate campaigns in their favor.[5] The danger is that academic and policy understandings of HLO are over-reliant on a single case. This article therefore asks: How do other HLO cases alter our understanding of this new phenomenon, including motives, means, and consequences?

HLO occur frequently worldwide, but their political contexts vary widely and have uncertain implications for U.S. politics.[6] Consequently, this article expands our understanding of HLO through a detailed qualitative analysis of four operations that targeted political figures in the United States in the period following the DNC operation (October 2016

[1] Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, Dec. 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[2] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, Feb. 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[3] Eric Rosenbach and Katherine Mansted, "Can Democracy Survive in the Information Age?" *Belfer Center for Science and International Affairs*, Harvard Kennedy School, October 2018, https://www.belfercenter.org/publication/can-democracy-survive-information-age.

[4] Renee DiResta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019" (Stanford, CA: Stanford University, Internet Observatory Cyber Policy Center 2019) https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf; Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (New York, NY: Oxford University Press, 2018).

[5] "United States of America v. Ahmad 'Andy' Khawaja et al., Case 1:19-Cr-374," United States District Court for the District of Columbia, May 7, 2019, https://www.coreysdigs.com/wp-content/uploads/2019/12/khawaja_Nader_indictment_unsealed.12.3.19.pdf; Paul Wood, "Andy Khawaja: 'The Whistleblower,'" *Spectator USA*, Feb. 24, 2020, https://spectator.us/whistleblower-andy-khawaja-micropayments/.

[6] James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy* 4, no. 2 (2019): 235–56, https://doi.org/10.1080/23738871.2019.1636108.

to January 2019), thus keeping the political and media environment constant as far as possible. These cases replicate many of the striking features of the DNC operation: access through phishing, the release of large collections of emails, publication in national media outlets, and even direct references to "DCLeaks," the identity assumed by the Russian intelligence agencies to disseminate the DNC documents. These cases have been publicly attributed to governments in the Middle East, namely Qatar, Saudi Arabia, and the United Arab Emirates (UAE), and thus broaden conceptions of digital foreign interference to allies as well as adversaries.

This article argues that HLO are the "simulation of scandal": deliberate attempts to direct public moral judgment against their target. The success of HLO depends on the shifting power dynamic between the scandal-maker and the scandal-subject, referred to in Arabic as *kāshif* and *makshūf*, respectively. At the center of this dynamic are the digital technologies used to obtain and release secret information. These hacking tools are a double-edged sword, as their discovery often means the scandal becomes about the hack itself, not about the hacked information; in other words, the *kāshif* becomes the *makshūf*. These cases also highlight other overlooked aspects of HLO: the utility of "activist" cover, the involvement of new actors such as public relations (PR) agencies and law firms, and the leaker's wary reliance on mistrustful relationships with traditional media. Finally, the article identifies wider consequences for cyber competition in situations of constraint where both sides are strategic partners. In such situations, HLO offer a powerful but indirect and unpredictable means of influence.

The first section places HLO within the literature on cyber conflict and information operations. The second section draws on sociological accounts of mediatized and digitalized leaks to explore the simulation of scandal. The rest of the article concerns the four case studies: The third section provides an overview of each case; the fourth analyzes their coverage in prominent media outlets; and the fifth discusses reasons behind their differing effects. A conclusion places this discussion in a broader strategic context, highlights limitations, and suggests further work.

Contextualizing Hack-and-Leaks

The contemporary media environment is congested, globalized, and securitized. Online publications and social media platforms compete for the scarce resource of users' attention, driven by logics of ranking, profiling, and advertising.[7] Users can access content from almost anywhere in the world, produced by a variety of actors with intertwined (geo)political, commercial, and normative motivations.[8] Media organizations and publications are increasingly enfolded into narratives of national security that demand urgent legislative and policy solutions. These three characteristics destabilize existing media authorities and gatekeepers with both positive and negative effects: They democratize debate while lowering editorial standards; provide a safe space for alternative identities while encouraging extremist positions; and offer new opportunities for both education and foreign interference. This Janus-like evolution is now most commonly represented with its uglier face forward, wearing the labels of "fake news," "post-truth," and "the end of objectivity."[9] Hastily proposed remedies are uncomfortable in some states where they strain creaking structures of liberal democracy. Yet these measures are music to the ears of authoritarian leaders in other states where repressive information controls and restrictions on speech resonate with efforts to mobilize the threat of foreign propaganda to bolster the incumbent regime.[10]

Leaks — the release of secret or confidential information into the public domain — occupy a special place in this divisive and frenetic world. In an era where trust online is frequently misplaced, the term "leak" is a rare marker of authenticity, intimating unmediated truth and unbalancing its targets. The amount of information released by leaks has increased dramatically, creating "mega" or "deluge" leaks, although this increase probably remains proportionate to the amount of data held by organizations.[11] Leaks have precipitated seismic recent events in world politics, from the U.S. cables that prompted Tunisian anger at elite corruption in late 2010 and contributed to the Arab Spring revolutions, to the Snowden revelations in 2013 that exposed the hypocrisy of the United States and

[7] Nick Couldry, "The Myth of 'Us': Digital Networks, Political Change and the Production of Collectivity," *Information, Communication & Society* 18, no. 6 (2015): 608–26, https://doi.org/10.1080/1369118X.2014.979216.

[8] Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality* (New York: Hachette Book Group, 2019).

[9] Nancy L. Rosenblum and Russell Muirhead, *A Lot of People Are Saying: New Conspiracism and the Assault on Democracy* (Princeton, NJ: Princeton University Press, 2019).

[10] Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (March 2015): 42–54, https://doi.org/10.1017/S1537592714003120.

[11] Margaret B. Kwoka, "Leaking and Legitimacy," *UC Davis Law Review* 48 (2015): 1387–1456, https://dx.doi.org/10.2139/ssrn.2494375.

its allies in extolling the benefits of global online access while simultaneously expanding digital surveillance architectures.

Unfortunately, not all mega leaks land on fortuitously aligned domestic and geopolitical fault lines. The documentation of horrifically bureaucratic torture and murder in Syrian jails, smuggled out by a former forensic photographer, has met the same silence and stalemate as other war crimes in that complex, grinding conflict.[12] Furthermore, although anonymous official sources and whistleblowers have always been an important element of political reportage, leaks are an everyday occurrence. Politicians and other media figures — and, unfortunately, ordinary young people — are now resigned to the expectation that classified documents, compromising photos, or candid conversations will eventually appear in their supposed (sometimes doctored) entirety.[13] Organizations, individuals, and digital devices are, in Wendy Hui Kyong Chun and Sarah Friedland's words, very "promiscuous": They "routinely work through an alleged 'leaking' that undermines the separation of the personal and the networked."[14]

Digital media are not only the *means* of dissemination for leaked information, but often also their *source*, through data breaches and HLO, also known as "doxing." Doxing — the acquisition and publication of another individual's private information — is one of the oldest practices in cyberspace. Originally, to "dox" (from "documents") someone meant simply revealing their offline identity, either for "lulz" — for little discernible reason beyond personal enjoyment — or to embarrass those who transgressed early norms of behavior on the internet.[15] As the internet grew, doxing became more sophisticated, using both intensive open-source investigation and intrusion into the target's systems to obtain sensitive information. The targets changed too, from tit-for-tat spats within hacker communities to the publication of personally identifiable information for thousands of government and corporate employees.[16] These later events are "public-interest hacks," in Gabriella Coleman's description of the hacker collective Anonymous,[17] or what Bruce Schneier has called "political" or "organizational" doxing.[18] Both leaks and doxes can release objects and capabilities in the form of computer code, as well as more traditional text documents.[19]

IN AN ERA WHERE TRUST ONLINE IS FREQUENTLY MISPLACED, THE TERM "LEAK" IS A RARE MARKER OF AUTHENTICITY, INTIMATING UNMEDIATED TRUTH AND UNBALANCING ITS TARGETS.

Finally, doxing and leaking actors have strong motivations to muddy the distinction between the two. Apparently leaked information may in fact result from an external intrusion obscured by journalists or lawyers for legal reasons, while victims may claim to have been hacked for the opposite reason, to facilitate insurance claims and avoid scrutiny. To make the overlap between doxing and leaking clear, I use "hack-and-leak operation (HLO)," which reminds us of both the usual sequence of events (hack *and then* leak), as well as the frequent blurring of boundaries between hacking and leaking.

HLO fit into a long history of the manipulation of information for national security purposes,

[12] U.N. Commission of Inquiry, "A Report into the Credibility of Certain Evidence with Regard to Torture and Execution of Persons Incarcerated by the Current Syrian Regime," S/2014/244, United Nations Security Council, April 4, 2014, https://digitallibrary.un.org/record/768578?ln=en#record-files-collapse-header.

[13] Peter Swire, "The Declining Half-Life of Secrets and the Future of Signals Intelligence" (Washington, D.C: New America Foundation, July 23 2015) https://d1y8sb8igg2f8e.cloudfront.net/documents/2.26Declining_Half_Life_of_Secrets.pdf.

[14] Wendy Hui Kyong Chun and Sarah Friedland, "Habits of Leaking: Of Sluts and Network Cards," *Differences* 26, no. 2 (Sept. 2015): 3 https://doi.org/10.1215/10407391-3145937.

[15] Caitlin Dewey, "How Doxing Went from a Cheap Hacker Trick to a Presidential Campaign Tactic," *Washington Post*, Aug. 12, 2015, https://www.washingtonpost.com/news/the-intersect/wp/2015/08/12/how-doxing-went-from-a-cheap-hacker-trick-to-a-presidential-campaign-tactic/.

[16] Nellie Bowles, "How 'Doxxing' Became a Mainstream Tool in the Culture Wars," *New York Times*, Aug. 30, 2017, https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.

[17] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London: Verso, 2014).

[18] Bruce Schneier, "Organizational Doxing," *Schneier on Security,* July 10, 2015, https://www.schneier.com/blog/archives/2015/07/organizational_.html; Bruce Schneier, "The Rise of Political Doxing," *Schneier on Security*, Nov. 2, 2015, https://www.schneier.com/blog/archives/2015/11/the_rise_of_pol.html.

[19] Catalin Cimpanu, "Source Code of Iranian Cyber-Espionage Tools Leaked on Telegram," *ZDNet*, April 17, 2019, https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/; Graham Templeton, "The 'Shadow Brokers' NSA Theft Puts the Snowden Leaks to Shame," *Extreme Tech*, Aug. 19, 2016, https://www.extremetech.com/extreme/234031-your-guide-to-the-shadow-brokers-nsa-theft-which-puts-the-snowden-leaks-to-shame.

which is centrally the preserve and currency of intelligence agencies.[20] Espionage in the modern era relies as much on signals intelligence — telecoms, radio, and now internet communications — as traditional human sources, sometimes competing but now largely integrated.[21] Intelligence agencies have also dominated the weaponization of espionage tools for "effects" such as disruption or damage.[22] Intelligence practices have a complex relationship with leaking. First, third-party leaks are valuable sources and the extent of private information on the internet means open- or all-source intelligence can be as powerful as secret methods. Second, intelligence agencies in democracies rely on popular support, regularly shaping policy and public perception through non-classic routes, leading to David Pozen's description of the U.S. government as a strategically "leaky leviathan."[23] Third, leaking — and the threat of leaking — is an effective way to damage adversaries or to convince people to provide information.[24] Leaking, for intelligence agencies, is thus both a powerful tool and their greatest fear, leading to insularity and internal suspicion.[25]

HLO are at the pinnacle of digital disinformation operations conducted by intelligence agencies, combining intrusion into networks with coordinated and doctored dissemination through traditional and social media. The growing literature on cyber conflict in strategic studies and international relations has astutely recognized how cyber operations in general are one means of exploiting economic, social, and technological openness on the internet for strategic gain.[26] This scholarship has many insights relevant to HLO, indicating a propensity for actors to conduct operations in the "gray zone" between peace and outright conflict.[27] It also highlights the creative and improvisatory nature of such operations in the context of rapidly evolving legal and technological responses, including a shifting background of "cyber norms" that offer a set of apparent constraints but, more realistically, serve as guiding lights for how the strategic pressure created by such operations can best be applied.[28]

However, the characterization of HLO purely as an aspect of antagonistic foreign relations between states fails to appreciate the complexity of the globalized and congested media environment sketched above. Consequently, HLO, especially those linked to the idea of "scandal," need to be located within sociological models of digital media and information politics outside national security contexts.

Scandal and Simulation

Scandals are a subset of leaks, as there can be no scandal without a disclosure of secret information (even if this information is only "secret" in the oxymoronic sense noted by Eva Horn, i.e., spoken of *ad infinitum* as secret).[29] Although nearly all scholars of scandal agree that moral transgression is at the core of the concept, they disagree over how best to theorize it.[30] Some distinguish the *type* of transgression; John B. Thompson's influential work suggests that values of trust and reputation separate political scandals from other forms.[31] In contrast, more an-

[20] Although militaries have always conducted information operations. For an early statement of military adaption to the internet, see John Arquilla and David Ronfeldt ed., *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington, D.C: RAND Corporation, 1997) https://www.rand.org/pubs/monograph_reports/MR880.html.

[21] Jenna McLaughlin and Zack Dorfman, "'Shattered': Inside the Secret Battle to Save America's Undercover Spies in the Digital Age," *Yahoo! News*, Dec. 30, 2019, https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.

[22] Michael Warner, "Intelligence in Cyber—and Cyber in Intelligence," in *Understanding Cyber Conflict: Fourteen Analogies*, ed. George Perkovich and Ariel Levite (Washington, DC: Georgetown University Press, 2018): 17-29; Colin F. Jackson, "Information Is Not a Weapons System," *Journal of Strategic Studies* 39, no. 5–6 (2016): 820–46, https://doi.org/10.1080/01402390.2016.1139496.

[23] David Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review* 127 (Feb. 25, 2013): 512–635, https://scholarship.law.columbia.edu/faculty_scholarship/770.

[24] Jaclyn A. Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," *International Journal of Communication* 12 (2018): 3814–34, https://ijoc.org/index.php/ijoc/article/view/8542/2460.

[25] Calder Walton, "Spies, Election Meddling, and Disinformation: Past and Present," *Brown Journal of World Affairs* 26, no. 1 (2019): 107–24, http://bjwa.brown.edu/26-1/spies-election-meddling-and-disinformation-past-and-present/.

[26] See, Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2015); Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

[27] Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies*, Published On-line March 4, 2020, 1–34, https://doi.org/10.1080/01402390.2020.1732354.

[28] James Shires, "Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf," in *Governing Cyberspace: Behavior, Power and Diplomacy*, ed. Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield Publishers, Inc., 2020), https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf.

[29] Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Random House, 1989); Eva Horn, "Logics of Political Secrecy," *Theory, Culture & Society* 28, no.7–8 (2011): 103–22, https://doi.org/10.1177%2F0263276411424583.

[30] Aida A. Hozic and Jacqui True, eds., *Scandalous Economics: Gender and the Politics of Financial Crises* (New York: Oxford University Press, 2016).

[31] John B. Thompson, *Political Scandal: Power and Visibility in the Media Age* (Cambridge, MA: Polity, 2000).

thropological approaches focus instead on the role of scandals in maintaining and reinforcing existing societal norms and values by providing an opportunity — and an obligation — to condemn a specific action that transgresses those norms.[32] Scandal thus requires what might be termed *normative dissonance*: a divergence between expected and observed or practiced norms and moral standards.[33]

This is illustrated most clearly through the figure of a whistleblower: One who witnesses or participates in actions that are contrary to their values, and yet is informed by those around them that these actions are normal or otherwise legitimate.[34] Michael Walzer calls whistleblowing "moral risk-taking" due to the bet that the whistleblower's moral position will resonate more with society at large than that of their peers.[35] We can see the power of scandal in the DNC leaks, turning the release of private information into condemnation of a moral transgression.[36] These leaks portrayed a clear normative dissonance between Hillary Clinton's projected image of trust and competence and accusations of "crooked Hillary" representing the "swamp" which came after the leak.

Although the concept of scandal enriches our understanding of the impact of HLO, the scholarship on scandal above does not directly address the issue of disinformation. The focus of these works is the presence of moral norms and their violation, rather than whether leaked information is verifiably true. Other sociological thought on scandal, especially that of Jean Baudrillard, explicitly cautions us against seeing leaks as simply revealing the truth. Baudrillard extends the anthropological insight of social reinforcement through scandal from purely moral norms to norms of truth, rationality, and reason. In his words, "It is always a question of proving the real by the imaginary, proving truth by scandal, [and] proving the law by transgression."[37] Scandals thus not only involve the airing and confirmation of certain values, but also commitment to rational argument and standards of truth.

However, for Baudrillard, these standards are not objective and so scandals are "an *arbitrary* stop to this revolving causality," a last-ditch attempt to save "a principle of political reality."[38] This arbitrariness means there is no such thing as a "true" scandal. Instead, all scandals are *simulated,* an arbitrary attempt at resisting relativism within a world of ungrounded uncertainty. Hence, he declares that "Watergate is not a scandal" but that "Watergate succeeded in imposing the idea that Watergate *was* a scandal ... the reinjection of a large dose of political morality on a global scale."[39] Baudrillard's ideas, although developed half a century ago, have clear relevance today, when standards of truth are a frequent object of manipulation and a tool in power struggles.[40] We should be skeptical of taking scandals at face value and should instead see exposure, denunciation, and counter-denunciation all as part of a single phenomenon.

However, Baudrillard's view deliberately bypasses the specific motives, tactics, and identities of the entities involved. In contrast, more recent scholarship, especially the work of Tarek El-Ariss on digital culture and literature in the Arab world, highlights how people *confront* normative dissonance. As he argues, there are "two forms of knowledge: a knowledge that is already known or assumed to be true, and an embarrassing if not scandalous knowledge from which no one can turn away ... Simultaneous acts of reading and knowing – knowing together, all at the same time – constitute the scandalous effect of the leak and make it embarrassing to those in power."[41] El-Ariss' argument goes on to make a useful distinction between the subject and object of

[32] Sally Engle Merry, "Rethinking Gossip and Scandal," in *Toward a General Theory of Social Control: Volume 1, Fundamentals*, ed. Donald Black (London: Academic Press, 1984), 271–302; Luise White, *Speaking with Vampires: Rumor and History in Colonial Africa* (Berkeley, CA: University of California Press, 2000).

[33] Edgar W. Mills, Jr., "Cult Extremism: The Reduction of Normative Dissonance," in *Cults in Context: Reading in the Study of New Religious Movements*, ed. Lorne L. Dawson (New Brunswick, N.J: Transaction Publishers, 1998), 385–96; Melissa S. Anderson, Brian C. Martinson, and Raymond De Vries, "Normative Dissonance in Science: Results from a National Survey of U.S. Scientists," *Journal of Empirical Research on Human Research Ethics: An International Journal* 2, no. 4 (2007): 3–14, https://doi.org/10.1525%2Fjer.2007.2.4.3; Dan Moore, "Reconciling Normative Dissonance in Canada and New Zealand: Comparing the Judicial and Political Paths to Children's Rights Implementation," *University of Toronto Faculty of Law Review* 68 (2010): 33–76.

[34] Kate Kenny, *Whistleblowing: Toward a New Theory* (Cambridge, MA: Harvard University Press, 2019).

[35] Michael Walzer, "Just and Unjust Leaks," *Foreign Affairs* 97, no. 2 (Mar/Apr. 2018): 48-59.

[36] James Lull and Stephen Hinerman, eds., *Media Scandals: Morality and Desire in the Popular Culture Marketplace* (Oxford: Polity, 1997).

[37] Jean Baudrillard, *Simulacra and Simulation*, trans. Sheila Faria Glaser (Ann Arbor, MI: University of Michigan Press, 1994), 12.

[38] Baudrillard, *Simulacra*, 10. Emphasis in text.

[39] Baudrillard, *Simulacra*, 9. Emphasis in text.

[40] James Der Derian, "The Desert of the Real and the Simulacrum of War," *International Affairs* 84, no. 5 (2008): 931–48, https://doi.org/10.1111/j.1468-2346.2008.00747.x; James Shires, "Cyber-Noir: Cyber security and Popular Culture," *Contemporary Security Policy* 41, no. 1 (2020): 82–107, https://doi.org/10.1080/13523260.2019.1670006.{\\i{}International Affairs} 84, no. 5 (2008

[41] Tarek El–Ariss, *Leaks, Hacks, and Scandals: Arab Culture in the Digital Age* (Princeton, NJ: Princeton University Press, 2019), 90.

the scandal: in Arabic, between *kāshif* (revealer) and *makshūf* (revealed).[42] He suggests that these two roles exchange and even overlap, especially as leaks develop and spread. Consequently, "scene-making and exposure … capture the breakdown of subject/object relation in a new digital landscape."[43]

> **… In a fast-flowing digital media environment with constant accusations and leaks, political actors seek to gain the upper hand through competing scandal-making…**

Like Baudrillard, El-Ariss traces the larger political implications of this delicately balanced and constantly shifting *kāshif/makshūf* relationship, concluding that "the dialectics of leaking and containing the leak expose the mechanism of prohibition and the failure or porousness of this mechanism at the same time."[44] We can see this political contest and shifting boundaries in the 2016 election, as both the Clinton and Trump campaigns repeatedly vied to portray themselves as *kāshif*, revealing lies and transgressions of their opponent, and avoid the identity of *makshūf*, the morally culpable and uncovered subject. More specifically, the DNC emails represented a crucial shift between the two, as a leaked recording of Donald Trump (the "Access Hollywood" tape) was overshadowed by the documents from the DNC focusing on Clinton's record in government.[45]

Our understanding of HLO is deepened in several ways by sociological works on scandal. First, scandal is prevalent across different moral contexts, leading to a focus on its mechanics rather than content. Second, the truth as revealed by scandal is always contested and challenged. Sometimes it is even simulated. Third, in a fast-flowing digital media environment with constant accusations and leaks, political actors seek to gain the upper hand through competing scandal-making, jostling to be *kāshif* rather than *makshūf*. Cases of HLO in U.S. politics demonstrate how hacking tools are the fulcrum of this struggle over identities, altering the balance of power between adversaries. The use of cyber tools brings the identity of whistleblower (*kāshif al-ʾasrār*, leaker of secrets) close to that of hacker (*hakar, mukhtariq*). When the hack becomes the focus of moral judgment and attention, rather than the leak itself, the *kāshif* becomes the *makshūf*.

HLO in U.S. Politics

The selected cases of HLO examined in this section all took place in the United States in the three years following the 2016 U.S. presidential election. This section provides an overview of the publicly available detail of each case in chronological order. The four cases, and selected characteristics, are summarized in Table 1. The cases were selected to keep the political and media environment constant as far as possible, in comparison to selecting cases from other countries. They were also selected because all four subjects are political actors of some form, even if they do not all hold official positions in government. Only one (Al-Otaiba) has such a position (as the UAE ambassador); the others are politically influential due to their connections and/or financial power. As such, the concept of politics I use for case selection is broad, encapsulating other individuals and organizations that have a significant influence over knowledge, policy, and action.[46]

In each case, as will become clear in the overviews, the individuals involved are enmeshed in a variety of schemes and relationships with Gulf leaders, local governments, or influential companies (and the three overlap to a significant extent). Consequently, these cases were selected not only because they all take place within the scope of U.S. politics, but also because they illustrate how domestic politics in the United States are inseparable from U.S. foreign policy, especially in the Middle

[42] El–Ariss, *Leaks, Hacks, and Scandals*, 98.

[43] El–Ariss, *Leaks, Hacks, and Scandals*, 176-77.

[44] El–Ariss, *Leaks, Hacks, and Scandals*, 37.

[45] David A. Fahrenthold, "Trump Recorded Having Extremely Lewd Conversation about Women in 2005," *Washington Post*, Oct. 8, 2016, https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html.

[46] James Shires, "Enacting Expertise: Ritual and Risk in Cyber security," *Politics and Governance* 6, no. 2 (2018): 31–40, http://dx.doi.org/10.17645/pag.v6i2.1329.

Table 1: Selected HLO in U.S. Politics

Subject of leak	Farhad Azima	Yusuf Al-Otaiba	Elliot Broidy	Jeff Bezos
Date of first leak	Oct. 22, 2016	June 2, 2017	March 2, 2018	Jan. 21, 2019
Public attribution (denied, all cases)	UAE/Iran	Qatar/Russia	Qatar	Saudi Arabia
Leaker's assumed identity	–	Activist	Activist	–
Intermediaries allegedly involved	PR agencies	–	PR agencies, cyber security companies	Commercial spyware company
Type of release	Coordinated with papers of record	Coordinated with papers of record	Coordinated with papers of record	Coordinated with tabloid
Type of scandal	Financial, political	Moral, financial, political	Financial, political	Moral
Responses from subject of leak	Lawsuits	Downplay relevance	Media messaging, lawsuits, technical investigation	Media messaging, lawsuits, technical investigation
Format	Emails, documents, iCloud	Email scans, emails	Emails, documents	Texts, photos

East.[47] Some media commentators cited below have therefore described the United States as merely a "battleground" for Gulf rivalries, but this goes too far in the opposite direction. Although U.S. politics is clearly not immune to the influences of other states, the United States is not a neutral place for Gulf struggles to play out: Domestic divisions and coalitions matter just as much as foreign interests or objectives.

Farhad Azima

Farhad Azima is an Iranian-American businessman in the aviation sector who was reportedly an asset for the CIA during the Iran-Contra scandal in the 1980s.[48] He was also named as the owner of a British Virgin Islands-based air transport company in the Panama Papers, a leak exposing corruption in tax havens, in early 2016. On Oct. 22, 2016, the UAE newspaper *The National* stated that Azima and the investment fund of the emirate Ras Al-Khaimah (RAKIA) had issued simultaneous lawsuits on Sept. 30, 2016, against each other in Washington, D.C. and London, regarding his role as a broker for a hotel purchase in Tbilisi, Georgia. Later lawsuits suggested that the dispute also involved accusations of arbitrary detention and prisoner abuse in Ras Al-Khaimah. Azima's 2016 submission claimed that "a massive volume of emails and other electronic data" had been taken by RAKIA through an intrusion into his computers in August 2016.[49]

RAKIA denied the claim and sympathetic Arab media only covered RAKIA's submission.[50] Later court documents stated that Azima's devices had

[47] James Shires, "Disinformation in the Gulf," in *Cyber War and Peace in the Middle East*, ed. Michael Sexton (Washington, D.C: Middle East Institute, forthcoming); James Shires, "The Cyber Operation against Qatar News Agency," in *The Gulf Crisis: Origins, Implications, Repercussions.*, ed. Mahjoob Zweiri (Berlin Heidelberg: Springer Nature, forthcoming).

[48] Jon Gambrell, Jack Gillum, and Jeff Horwitz, "'Worth Killing Over:' How a Plane Mogul Dodged US Scrutiny," *AP NEWS*, June 21, 2017, https://apnews.com/4a4b6e9dfc0949e698ee0ada284414ed/'Worth-killing-over':-How-a-plane-mogul-dodged-US-scrutiny.

[49] Shaun Cronin, "Panama Papers Aviation Executive in Legal Battle with Rakia over Georgia Hotel," *The National*, Oct. 22, 2016, https://www.thenational.ae/business/panama-papers-aviation-executive-in-legal-battle-with-rakia-over-georgia-hotel-1.194281.

[50] Sky News Arabia, "*ʾamrīkī min ʾaṡal ʾirānī yuwājihu tuhm ikhtilās fī al-ʾimārāt* [American of Iranian Origin Faces Allegations of Fraud in the Emirates]," *Sky News Arabia*, Oct. 25, 2016, https://www.skynewsarabia.com/business/886466 .

first been compromised in October 2015, and then in mid-2016 websites had appeared with names such as "Farhad Azima Scammer," including BitTorrent links to Azima's emails and iCloud data.[51] Eight months later, on June 21, 2017, the *Associated Press* published an article on Azima's past relying on "a recently obtained collection of tens of thousands of emails his lawyers say was stolen by hackers."[52] This was accompanied by a separate article detailing how contact between Azima and *Wall Street Journal* correspondent Jay Solomon had led the paper to terminate Solomon's contract. The *Wall Street Journal* claimed that Solomon had violated ethical obligations and professional standards in his contact with Azima.[53]

Solomon's own account of this contact emphasized that the hacked data, posted online on Sept. 13, 2016, included a file named "Fraud Between Farhad Azima and Jay Solomon." Solomon thus inferred that he was one of the targets of the hack, and blamed Iranian state-sponsored actors due to the Iranian focus of his reporting at the *Wall Street Journal*.[54] Solomon also repeated Azima's lawyers' claim that the hackers "inserted spyware into his [Azima's] computer." Solomon claimed that RAKIA's public relations consultants, Bell Pottinger, had sent the hacked data to international media outlets, including the *Wall Street Journal*, suggesting that "the information operation had been incredibly effective." A friend of Solomon's published an article in *Bloomberg* stating that the "biased curation" of the data by the *Associated Press* constituted a clear information operation.[55] In June 2018, the Qatari outlet *Al Jazeera* used further court documents to attribute the hack to RAKIA, noting that the judge found it was "beyond dispute" that hackers had been involved and that Azima's claim of RAKIA's involvement was "plausible."[56] Most recently, a court judgment in the United Kingdom in May 2020 found against Azima on the matter of the Tbilisi hotel, instructing him to pay $4 million to RAKIA, and decided that his claim of RAKIA's responsibility for the HLO was not proven by the circumstantial evidence provided.[57]

This case demonstrates the complexity of HLO. The provenance of the leak in a hacking operation was quickly seized upon by Azima's opponents and questioned by his supporters, with subsidiary effects on Azima's contacts, such as Solomon. Lawsuits ongoing before, during, and after the leak struggled to deal adequately with the information revealed, but their careful conclusions were nonetheless leveraged by polarized media to shift the scandal as it developed.

Yusuf Al-Otaiba

On June 2, 2017, three days before a diplomatic split between Qatar on one hand and the UAE, Saudi Arabia, Bahrain, and Egypt on the other, several news organizations in the United States received messages from a group called GlobalLeaks, containing copies of emails from the Hotmail account of the UAE ambassador to the United States, Yusuf Al-Otaiba, between 2014 and 2017. As reported by the *Daily Beast*, the purpose of GlobalLeaks was to "reveal how million[s] of dollars were used to hurt [the] reputation[s] of American allies and cause policy change," and thus show "how a small rich country/company used lobbyists to hurt American interests and those of it[s] allies."[58] Although GlobalLeaks claimed the emails came from a paid whistleblower based in Washington, D.C., the *Daily Beast* suggested they were printed out directly from a hacked Hotmail account. GlobalLeaks used a free email account with a Russian provider, and the subject line of their email was "DC Leaks - The Lobbyist Edition Part 1," referencing the website used to publish emails from the DNC hack. According to the *Huffington Post*, GlobalLeaks denied any

[51] Ketanji Brown Jackson, "Memorandum Opinion No. 16-Cv-01948 (KBJ)" (United States District Court for the District of Columbia, March 30, 2018) https://casetext.com/case/azima-v-rak-inv-auth.

[52] Gambrell et al., "'Worth Killing Over."

[53] Jeff Horwitz, Jon Gambrell, and Jack Gillum, "Wall Street Journal Fires Correspondent over Ethics Conflict," *AP NEWS*, June 21, 2017, https://apnews.com/d71bf1b8c2304329866441ec4089760f/Wall-Street-Journal-fires-correspondent-over-ethics-conflict.

[54] Jay Solomon, "The Source: How Hacked Emails and a Yacht in Monaco Ended My Career at *The Wall Street Journal*," *Columbia Journalism Review*, March 5, 2018, https://www.cjr.org/special_report/the-source.php.

[55] Eli Lake, "The New Threat of 'Leak-Flavored' Propaganda," *Bloomberg*, March 20, 2018, https://www.bloomberg.com/opinion/articles/2018-03-20/hacked-and-leaked-real-messages-can-paint-a-false-portrait.

[56] Jamie Merrill, "Exclusive: UAE Company 'Hacked US-Iranian Magnate's Email,'" *Al-Jazeera*, June 6, 2018, https://www.aljazeera.com/news/2018/06/exclusive-uae-company-hacked-iranian-magnate-email-180606070945940.html.

[57] Andrew Lenon Q.C., "Approved Judgment between Ras Al-Khaimah Investment Authority and Farhad Azima," HC-2016-002798, [2020] EWHC 1327 (Ch) (Royal Courts of Justice, London, May 22, 2020) https://www.matrixlaw.co.uk/wp-content/uploads/2020/05/RAKIA-v-AZIMA-Final-Judgment2.pdf.

[58] Kevin Poulsen, "Hackers Vow to Release Apparent Trove of U.A.E. Ambassador's Emails," *Daily Beast*, June 2, 2017, https://www.thedailybeast.com/hackers-vow-to-release-apparent-trove-of-uae-ambassadors-emails.

allegiance to Qatar or another government.[59]

Other news outlets continued to publish revelations from Al-Otaiba's account after what the *Wall Street Journal* called a "new release" of emails at the end of July 2017. The *New York Times* published a story about the opening of a Taliban embassy in Doha rather than Abu Dhabi,[60] while the *Wall Street Journal* focused on Al-Otaiba's relationship with a Malaysian state development fund. The *Wall Street Journal* named GlobalLeaks as their source, with the stated motivation to "expose corruption, [and] financial frauds which are done by rich governments."[61] At the end of August 2017, *The Intercept* reported on Al-Otaiba's personal life, including sexual conduct and a "party" lifestyle, using emails beginning in 2007. This story claimed that some of Al-Otaiba's emails had already been posted to an online chatroom in 2009 but were then removed. These emails were seen by the journalist for *The Intercept* in 2015.[62] A further release occurred on Sept. 13, 2017, including stories in *The Intercept* and *Middle East Eye* on Egyptian lobbying in the United States.[63]

In terms of political consequences, the Al-Otaiba leaks were significant in demonstrating how Al-Otaiba worked both sides of the aisle in Washington, D.C. He was close to the Obama administration, arranging closed high-level meetings and disparaging the Trump campaign. He then became equally close to the Trump administration, with some media reports suggesting that the investigation into election interference by Special Counsel Robert Mueller took an "interest" in the emails as evidence of contact with Trump advisers prior to the election.[64] Although UAE contacts are dealt with extensively in the Mueller report, redactions mean it is unclear what role, if any, these leaked emails played in Mueller's investigation. [65]

This case demonstrates how a single HLO has a bearing on several domestic and geopolitical planes simultaneously, including the Qatar split, U.S. strategy in the Gulf, investigations into Russian interference and other influences on the U.S. election, and salacious stereotypes of rich Arab lifestyles in the United States. It also reveals how closely HLO actors can mimic other operations, sowing confusion about attribution.

Elliott Broidy

Elliot Broidy is a Republican lobbyist with extensive business ties to the UAE. The *Huffington Post* first reported leaked emails from Broidy's email account on March 2, 2018, from a group named "L.A. Confidential" whose stated purpose was to "expose people associated with Hollywood" (Broidy's wife, Robin Rosenzweig, is a Hollywood lawyer). The documents included emails Broidy wrote to himself, offering insights into his personal thoughts as well as private communications.[66] A second release of documents was published by the *Associated Press* on May 21, 2018.[67] The *New York Times* published a comprehensive story on Broidy's relationships with other lobbyists and fixers at the same time.[68] The BBC used Broidy's emails to reveal that former U.S. Secretary of State Rex Tillerson was under political pressure prior to his resignation, and quoted a spokesman for Broidy claiming that "we have reason to believe this hack was sponsored and carried out

[59] Akbar Shahid Ahmed, "Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador," *HuffPost UK*, June 3, 2017, https://www.huffpost.com/entry/otaiba-ambassador-uae-leaked-emails_n_5932bf04e4b02478cb9bec1c.

[60] David D. Kirkpatrick, "Persian Gulf Rivals Competed to Host Taliban, Leaked Emails Show," *New York Times*, July 31, 2017, https://www.nytimes.com/2017/07/31/world/middleeast/uae-qatar-taliban-emails.html.

[61] Bradley Hope and Tom Wright, "Stolen Emails Show Ties Between U.A.E. Envoy and 1MDB Fund's Central Figure," *Wall Street Journal*, Aug. 1, 2017, https://www.wsj.com/articles/stolen-emails-show-ties-between-u-a-e-envoy-and-1mdb-funds-central-figure-1501579801.

[62] Ryan Grim, "Diplomatic Underground: The Sordid Double Life of Washington's Most Powerful Ambassador," *The Intercept* (blog), Aug. 30, 2017, https://theintercept.com/2017/08/30/uae-ambassador-yousef-al-otaiba-double-life-prostitutes-sex-work/.

[63] Olivia Alabaster, "Leaked UAE Emails: Saudi Arabia Came Close to 'Conquering' Qatar," *Middle East Eye,* Sept. 14, 2017, https://www.middleeasteye.net/fr/news/saudi-arabia-came-close-conquering-qatar-new-leaked-emails-show-1491607860; Zaid Jilani, "The UAE Secretly Picked Up the Tab for the Egyptian Dictatorship's D.C. Lobbying," *The Intercept* (blog), Oct. 4, 2017, https://theintercept.com/2017/10/04/egypt-lobbying-uae-otaiba-trump-sisi/.

[64] Akbar Shahid Ahmed, "Ambassador Slammed Donald Trump Amid UAE Campaign To Isolate Qatar," *HuffPost UK*, June 5, 2017, https://www.huffpost.com/entry/yousef-al-otaiba-emails-trump_n_59358e71e4b013c48169d5dc; David Hearst, "Revealed: How Trump Confidant Was Ready to Share inside Information with UAE," *Middle East Eye,* June 29, 2018*,* https://www.middleeasteye.net/news/revealed-how-trump-confidant-was-ready-share-inside-information-uae.

[65] Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," Submitted Pursuant to 28 C.F.R. § 600.8(c) (Washington, D.C: US Department of Justice, March 2019), https://www.justice.gov/storage/report.pdf.

[66] Maxwell Strachan and Jessica Schulberg, "Leaked Emails Appear To Show A Top Trump Fundraiser Abusing His Power," *HuffPost*, March 2, 2018, https://www.huffpost.com/entry/elliott-broidy-trump-malaysia-doj_n_5a988471e4b0a0ba4ad18d65.

[67] Desmond Butler and Tom LoBianco, "The Princes, the President and the Fortune Seekers," *AP NEWS*, May 21, 2018, https://apnews.com/a3521859cf8d4c199cb9a8567abd2b71/The-princes,-the-president-and-the-fortune-seekers.

[68] David D. Kirkpatrick and Mark Mazzetti, "How 2 Gulf Monarchies Sought to Influence the White House," *New York Times*, March 21, 2018, https://www.nytimes.com/2018/03/21/us/politics/george-nader-elliott-broidy-uae-saudi-arabia-white-house-influence.html.

by registered and unregistered agents of Qatar."[69] In May 2018, *Bloomberg* reported that the compromise probably occurred when Rosenzweig received an email on Dec. 27, 2017, with an apparent Gmail security alert. She reportedly reset her password while on the spoofed page, allowing the malicious actor access to a Google Doc with more passwords including an account at Broidy's finance company.[70]

THIS CASE DEMONSTRATES HOW A SINGLE HLO HAS A BEARING ON SEVERAL DOMESTIC AND GEOPOLITICAL PLANES SIMULTANEOUSLY...

Further details of the compromise have emerged from a series of lawsuits issued by Broidy against the state of Qatar and its agents. The first lawsuit claimed that from January to March 2018 an email server at Broidy's finance company had been compromised, with an initial forensic analysis identifying IP addresses for VPN services in the Netherlands and the United Kingdom. Later analysis also identified non-VPN connections from Qatari IP addresses.[71] The lawsuit was dismissed as the court had no jurisdiction over foreign sovereign entities.[72] A separate lawsuit in a New York court against a U.N. official was also dismissed.[73] According to Broidy's lawsuits, Qatar's public relations firms called many news outlets during this period and spoke frequently with the *Associated Press* just before the story about Broidy's emails was published. The most recent lawsuit, in documents filed in March 2020, alleges that a company named Global Risk Advisors was responsible for the hack, although no further evidence is provided.[74] Overall, one of the main consequences of the leaked documents was to expose Broidy's commercial relationships with the UAE and Saudi governments through a military contracting company, Circinus. The documents also highlighted his contacts with individuals indicted for channeling "illicit donations" from the UAE to the Trump presidential campaign, and Broidy is reportedly under federal investigation for his relationship to the UAE.[75]

This case reinforces several aspects of the first two, including supposedly activist or ideological motivations and a swift descent into "lawfare" (legal warfare) as a response to the leak. This leak was assimilated into several orthogonal agendas, again including the Qatar split and election interference, and highlights the key role of PR companies on both sides of the HLO.

Jeff Bezos

Jeff Bezos is the founder and CEO of Amazon and owner of the *Washington Post*. On Jan. 21, 2019 the *National Enquirer* published a report about Bezos' extra-marital relationship with Lauren Sanchez, a television host in Los Angeles, based on text messages between the two in late 2016.[76] Within days, several news outlets speculated that the leak was politically motivated due to the *Washington Post*'s coverage of President Trump, although at this stage

[69] Suzanne Kianpour, "Emails Show UAE-Linked Effort against Tillerson," *BBC News*, March 5, 2018, https://www.bbc.com/news/world-us-canada-43281519.

[70] David Voreacos and Michael Riley, "Elliott Broidy and the GOP's Bad Hacking Karma," *Bloomberg*, May 4, 2018, https://www.bloomberg.com/news/articles/2018-05-04/elliott-broidy-and-the-gop-s-bad-hacking-karma.

[71] David K. Willingham and Boies Schiller Flexner LLP, "Complaint and Demand for Jury Trial Case" No. 2:18-Cv-2421 (United States District Court, Central District of California, Western Division, March 26, 2018) https://www.courtlistener.com/recap/gov.uscourts.cacd.705090/gov.uscourts.cacd.705090.1.0_3.pdf.

[72] Julie Bykowicz, "U.S. Judge Dismisses Qatar from Elliott Broidy Hacking Lawsuit," *Wall Street Journal*, Aug. 8, 2018, https://www.wsj.com/articles/u-s-judge-dismisses-qatar-from-elliott-broidy-hacking-lawsuit-1533768624.

[73] Nathan Layne, "Trump Fundraiser Broidy Hit with Another Setback in Qatar Lawsuit," *Reuters*, Dec. 21, 2018, https://www.reuters.com/article/us-usa-trump-russia-broidy/trump-fundraiser-broidy-hit-with-another-setback-in-qatar-lawsuit-idUSKCN1OK2EA.

[74] Dabney L. Friedrich, "Broidy Capital Management LLC, et al., Plaintiffs, v. Nicholas D. Muzin, et al., Defendants. Memorandum Opinion," No. 19-Cv-0150 (DLF) (United States District Court for the District of Columbia, March 31, 2020), https://casetext.com/case/broidy-capital-mgmt-llc-v-muzin.

[75] David D. Kirkpatrick and Kenneth P. Vogel, "Indictment Details How Emirates Sought Influence in 2016 Campaign," *New York Times*, Dec. 5, 2019, https://www.nytimes.com/2019/12/05/us/politics/indictment-uae-influence.html.

[76] James Robertson, Andrea Simpson, and Dylan Howard, "Jeff Bezos' Raunchy Text Messages That Prove Illicit Affair," *National Enquirer* (blog), Jan. 21, 2019, https://www.nationalenquirer.com/videos/jeff-bezos-lauren-sanchez-text-messages-affair-scandal/.

"a digital forensic analysis turned up no evidence of a hack and the theory was quickly discounted."[77] On Feb. 7, 2019, Bezos wrote an article claiming that the owner of the *National Enquirer* had attempted to blackmail him with "intimate photos" Bezos had sent to Sanchez. Bezos linked this attempt to his own investigation of how his text messages had been leaked, as well as the *Washington Post*'s coverage of murdered Saudi journalist Jamal Khashoggi, because the letter he claimed to have received stated he should publicly state that he has "no knowledge or basis for suggesting that [the *National Enquirer*'s] coverage was politically motivated or influenced by political forces."[78] The Saudi foreign minister, Adel Jubair, denied any involvement.[79] On Feb. 12, 2019, the *Associated Press* published a story claiming that Bezos' investigation had determined that Lauren Sanchez's brother, Michael Sanchez, was the source of the message and photos.[80]

In March 2019, Bezos' private investigator published his own account, stating that "our investigators and several experts concluded with high confidence that the Saudis had access to Bezos' phone, and gained private information."[81] He did not provide any further details other than interviews with "leading cyber security experts who have tracked Saudi spyware." He also stated that the *National Enquirer* appeared to have access to Bezos' messages before contacting Michael Sanchez, basing his conclusion on media reports. The private investigator implied that the Saudi government targeted Bezos in several ways due to the *Washington Post*'s coverage of the Khashoggi killing, including on social media, and that the leaked messages were

[77] Lachlan Markay and Asawin Suebsaeng, "Bezos Launches Probe Into Leaked Texts to National Enquirer," *Daily Beast*, Jan. 30, 2019, https://www.thedailybeast.com/bezos-launches-investigation-into-leaked-texts-with-lauren-sanchez-that-killed-his-marriage.

[78] Jeff Bezos, "No Thank You, Mr. Pecker," *Medium* (blog), Feb. 7, 2019, https://medium.com/@jeffreypbezos/no-thank-you-mr-pecker-146e3922310f.

[79] Ed Pilkington, "Saudi Arabia Denies Role in Leak of Jeff Bezos's Messages to National Enquirer," *The Guardian*, Feb. 10, 2019, https://www.theguardian.com/technology/2019/feb/10/jeff-bezos-texts-national-enquirer-saudi-arabia-denies-role.

[80] Staff Report (via Associated Press), "Jeff Bezos Investigation Finds Lauren Sanchez's Brother Leaked Information to Enquirer, Source Says," *Los Angeles Times*, Feb. 12, 2019, https://www.latimes.com/business/la-fi-bezos-enquirer-leak-michael-sanchez-20190212-story.html.

[81] Gavin de Becker, "Bezos Investigation Finds the Saudis Obtained His Private Data," *Daily Beast*, March 30, 2019, https://www.thedailybeast.com/jeff-bezos-investigation-finds-the-saudis-obtained-his-private-information.

part of this targeting. Saudi Arabia repeated its denial of involvement following this article.[82] Finally, in January 2020 several news outlets used the leaked contents of a technical investigation into Bezos' phone to conclude that it was likely compromised with malware that behaves in a manner similar to a commercial product alleged to be used by the Saudi government.[83] This report contained only circumstantial evidence,[84] but the association with Saudi Arabia was repeated by United Nations special rapporteurs investigating Saudi Arabia's human rights record.[85]

Following this report, media articles stated that Bezos met and swapped phone numbers with Saudi Crown Prince Muhammad bin Salman at a dinner with other Silicon Valley investors several weeks before the alleged hack, during bin Salman's visit which was promoted heavily by the *National Enquirer*.[86] However, disagreements over sourcing continued, as the *Wall Street Journal* used leaked documents from a federal investigation to argue that Michael Sanchez provided the original texts to the *National Enquirer*.[87] These explanations are not mutually exclusive: It is possible that Bezos' phone was infected *and* that Michael Sanchez provided the texts, or that the leak was double-sourced, or that either is incorrect.

This case amplifies the prurient strains of the Al-Otaiba case, with headlines dominated by details of the affair, divorce, and division of assets of the world's richest man. But there was also a constant political undertone, with Saudi overtures to Silicon Valley and subsequent fissures generating ample grist to a speculative mill well before the results of any investigation. Overall, these four cases have both evident similarities and several key differences. The trajectory of each case turns on whether the media chooses to focus on the leaker or the subject of the leak as their main story: in other words, whether the scandal is about the *kāshif* or the *makshūf.*

Media Coverage

Although it is extremely difficult to judge the overall impact of a HLO, there were several immediate consequences from the four cases considered here. According to the U.K. judge, the Azima leak was decisive in his decision instructing Azima to pay $4 million to RAKIA.[88] Although the Azima leak led to the termination of Solomon's employment at the *Wall Street Journal*, Solomon was apparently only an incidental target. Bezos and those in his personal life were severely affected by the leak, but his political and economic influence has not diminished. In the Al-Otaiba and Broidy cases, their targets were temporarily excluded from their usual lobbying circuits. For example, Broidy's lawyers cite in a claim document WhatsApp messages between Qatari agents, indicating some direct consequences for Broidy's lobbying career.[89] However, Broidy and Al-Otaiba returned quickly to these political circles afterwards.[90] Due to redactions, it remains unclear whether Broidy is mentioned in the Mueller report following connections revealed through his and Al-Otaiba's leaked emails, though Broidy is reportedly under investigation for other activities during the election.

Overall, in contrast to the DNC leaks, the long-

[82] Sherisse Pham, "Saudi Arabia Denies Any Role in Jeff Bezos' Affair Leak," *CNN*, April 3, 2019, https://www.cnn.com/2019/04/03/media/jeff-bezos-national-enquirer-saudi/index.html.

[83] Kim Zetter and Joseph Cox, "Here Is the Technical Report Suggesting Saudi Arabia's Prince Hacked Jeff Bezos' Phone," *Vice*, Jan. 22, 2020, https://www.vice.com/en_us/article/v74v34/saudi-arabia-hacked-jeff-bezos-phone-technical-report.

[84] Bill Marczak, "Some Directions for Further Investigation in the Bezos Hack Case," *Medium*, Jan. 22, 2020, https://medium.com/@billmarczak/bezos-hack-mbs-mohammed-bin-salman-whatsapp-218e1b4e1242.

[85] Agnes Callamard and David Kaye, "UN Experts Call for Investigation into Allegations That Saudi Crown Prince Involved in Hacking of Jeff Bezos' Phone," *United Nations Office of the High Commissioner for Human Rights*, Jan. 22, 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488&LangID=E.

[86] Troy Wolverton, "The Saudi Crown Prince Accused of Hacking Jeff Bezos' Phone Met with More than a Dozen Tech Execs and Celebs during the Same US Trip," *Business Insider*, Jan. 22, 2020, https://www.businessinsider.in/slideshows/miscellaneous/the-saudi-crown-prince-accused-of-hacking-jeff-bezos-phone-met-with-more-than-a-dozen-tech-execs-and-celebs-during-the-same-us-trip-from-tim-cook-to-oprah-heres-everyone-mohammed-bin-salman-met-with-/slidelist/73510379.cms.

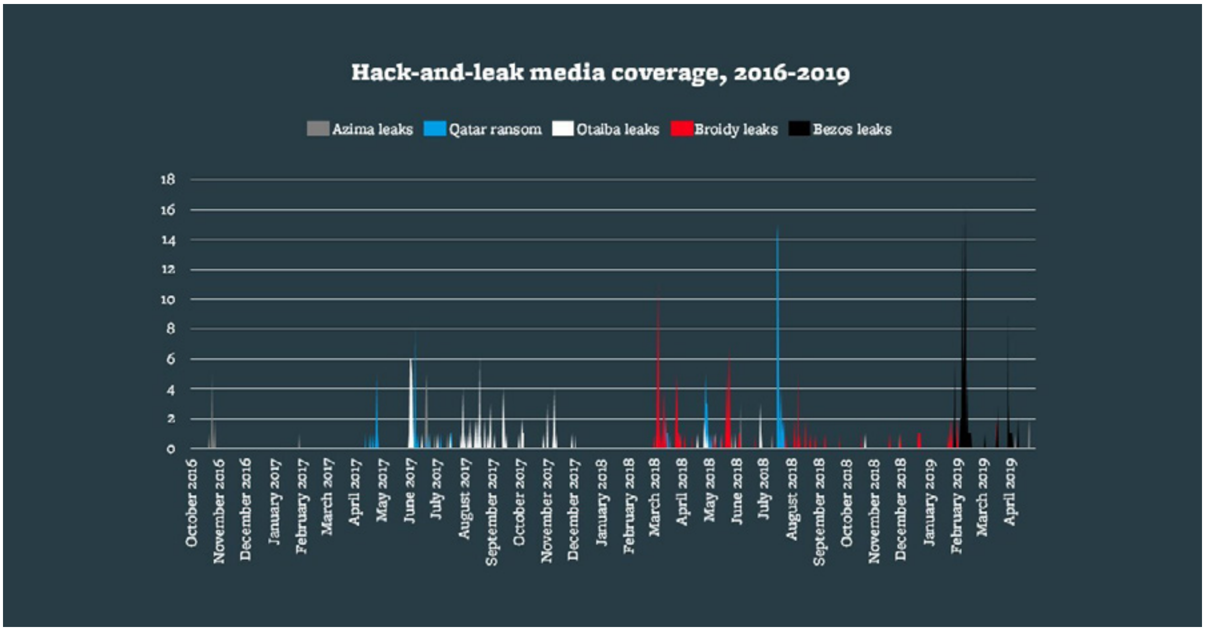
[87] Joe Palazzolo and Corinne Ramey, "Prosecutors Have Evidence Bezos' Girlfriend Gave Texts to Brother Who Leaked to National Enquirer," *Wall Street Journal*, Jan. 25, 2020, https://www.wsj.com/articles/prosecutors-have-evidence-bezos-girlfriend-gave-texts-to-brother-who-leaked-to-national-enquirer-11579908912.

[88] Lenon Q.C., "Approved Judgment," 127.

[89] On March 15, 2018, Muzin exclaimed to Allaham, via WhatsApp, "Elliott Broidy was not at the fundraiser!" Dabney L. Friedrich, "Broidy Capital Management LLC, et al., Plaintiffs, v. Nicholas D. Muzin, et al., Defendants. Memorandum Opinion," No. 19-Cv-0150 (DLF) (United States District Court for the District of Columbia, March 31, 2020), https://casetext.com/case/broidy-capital-mgmt-llc-v-muzin.

[90] Anna Palmer, Jake Sherman, and Daniel Lippman, "POLITICO Playbook: Best Lines from the Alfalfa Club Dinner," *POLITICO*, Jan. 27, 2019, https://www.politico.com/newsletters/playbook/2019/01/27/best-lines-from-the-alfalfa-club-dinner-382142; Ryan Grim, "The UAE's Powerful Ambassador Is Still Hobnobbing in Washington After Jamal Khashoggi's Murder," *The Intercept* (blog), Oct. 23, 2018, https://theintercept.com/2018/10/23/yousef-al-otaiba-khashoggi-washington/.

Figure 1: Hack-and-leak Media Coverage, 2016-2019



term impact from these leaks remains uncertain. However, it is possible to gauge the impact of each leak through the coverage in major media outlets. All four cases involved relationships with traditional media outlets: Broidy, Al-Otaiba, and Azima were associated with highly regarded news services or papers of record, while the Bezos case involved the celebrity tabloid the *National Enquirer*. This focus on traditional media seems slightly anachronistic, as people now consume much of their news and commentary through social media. However, traditional media outlets still play a foundational role in political debate. Although their role as gatekeepers is no longer well-defined, many such outlets have adapted to the new media environment, though they now have new commercial incentives for production and content. Moreover, this focus appears to have been a strategic choice by the leakers. In the Azima case, Solomon describes the leaker contacting many media outlets until the *Associated Press* “bit” and published the documents.[91] The Broidy case suggests even closer relationships with specific organizations, as there were allegedly repeated conversations with news organizations prior to each release.[92]

I measured the media coverage of these cases by identifying the top 50 results of a structured Google search conducted in June 2019 (Figure 1).[93] Google’s algorithm ranks websites based on a complex mix of content, search frequency, and connections, serving as an adequate proxy for the popularity of an online news article without measuring specific page visits or visitor behavior.[94] In each case nearly all results were news articles and the total count was sufficient to capture the main waves of publication, as relevant results after 50 were usually recycled articles from secondary sites. The exception is the Azima case, where there were 31 results in total. Plotting the dates of these results shows that media coverage of these leaks occurred in short spikes, representing a brief news cycle: The story hits the press, is covered by various outlets in the following days, then disappears. These spikes occur multiple times for each case, so there are repeated “waves” when new documents are leaked.

Although the analysis above provides an indication of media coverage over time, it does not distinguish between two forms of coverage crucial to my argument on the simulation of scandal: stories that focused on the content of the leak, and sto-

[91] Solomon, "The Source."

[92] Agusti et al., "Complaint and Jury Demand."

[93] The analysis therefore does not include later stories referenced above, such as the Bezos developments in 2020.

[94] The search contained two keywords, detailed in the labels for Figure 1. I used "Otaiba" without the definite article, rather than "Al-Otaiba," to follow standard usage in the American press. Biases in Google's search algorithm were minimized by conducting each search on a clean browser with an IP address in the Eastern United States. Results without dates or with missing links and those on different topics were excluded. The results were not mutually exclusive: Some stories referenced multiple cases and so appeared in more than one search. The Google algorithm may also have favored websites for other reasons that are not discussed here, such as different extent of search optimization.

Table 2: Headlines of Disinformation Stories on Selected HLO Cases [95] [96] [97] [98] [99]

	Qatarileaks		**Emiratesleaks**	
	English	*Arabic*	*English*	*Arabic*
Broidy leaks	Broidy files new lawsuit against Qatar	Qatari mercenaries accused of Broidy email hack are in trouble	n/a	Emirati academic boasts of his country's role in the toppling of U.S. foreign minister
Al-Otaiba leaks	n/a	n/a	Millions of dollars spent by UAE to lobbyists in Washington	Arrangement with Trump advisers to give UAE "sensitive" information

ries that focused on the details of the hack. The former implies that the *kāshif* (revealer, divulger) responsible for the HLO has successfully portrayed their target as *makshūf* (revealed, uncovered). The latter implies that these roles have been reversed, and the actor that conducted the HLO has become *makshūf* — they are the one whose secrets have been revealed. The relationship between these two forms of coverage demonstrates the weight of coverage of the scandal overall, with each story's focus directed towards the hacking operation itself or towards the content revealed by the hack. Although most stories collected in Figure 1 mentioned both elements, there was usually a clear prioritization of one angle over the other.

This prioritization is illustrated in an extreme form by two disinformation websites present in the media coverage analyzed here: one, promoting negative stories about Qatar, called Qatarileaks, and the other doing the same for the UAE, called Emiratesleaks. The Qatarileaks website and Twitter account were created in May 2017, while the Emiratesleaks website was created on Jan. 2, 2018. The Qatarileaks website covered Broidy's accusations of hacking by Qatar and did not mention the Al-Otaiba leaks at all. Conversely, the Emiratesleaks website covered the revelations in Broidy's emails but not the accusations of hacking (Table 2).

These two forms of coverage were also represented in the other news articles collected, albeit in a less extreme form. I therefore coded all articles as prioritizing either the hack or the leak elements of the scandal, based on a qualitative judgment of the headline of the article (Figure 2). The results indicate interesting variation: Media coverage of the Al-Otaiba case mainly focused on the leak contents; coverage of the Bezos case focused on the hack; and the Broidy and Azima cases were split roughly evenly, with more coverage overall of the Broidy case.[100]

Explaining the Trajectory of Simulated Scandals

There are several potential explanations for the differing media coverage pertaining to each of the four hack-and-leak case studies. These HLO cases are complex, multi-causal events, and the explanations are complementary rather than competing. The fluid identities of *kāshif* and *makshūf* are rele-

[95] Qatarileaks, "Broidy Files New Lawsuit against Qatar," *Qatarileaks*, Jan. 26, 2019, https://qatarileaks.com/en/leak/broidy-files-new-lawsuit-against-qatar.

[96] Qatarileaks, "*Murtaziqa Qatar Al-Mutawaraṭīn Biqurṡanat ʾīmailāt Brwaidī Fī Maʾaziq* [Qatari Mercenaries Accused of Broidy Email Hack Are in Trouble]," *Qatarileaks*, June 9, 2019, https://qatarileaks.com/ar/leak/.

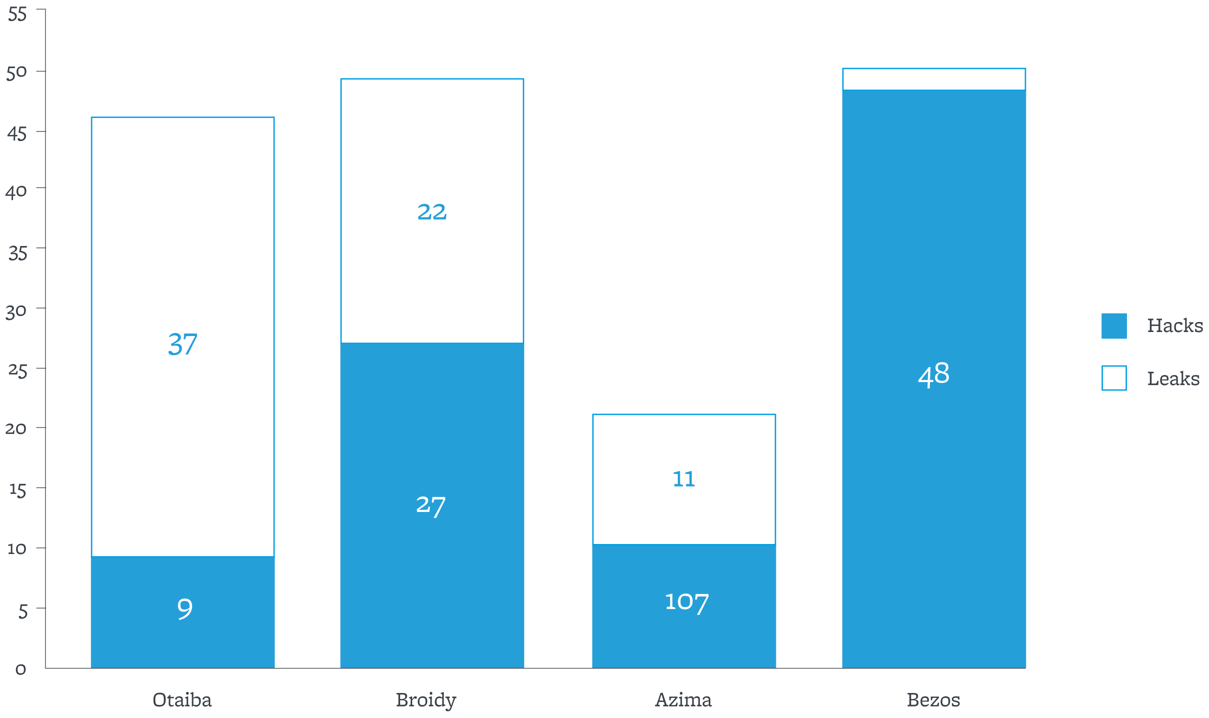
[97] Emiratesleaks, "*ʾakādīmī ʾimārātī Yatafākhiru Bidūr Balādihi Fī Al-ʾiṫāḣa Biwazīr al-Khārijīyya al-ʾamrīkī* [Emirati Academic Boasts of His Country's Role in the Toppling of US Foreign Minister]," *Emiratesleaks*, March 15, 2018, https://emiratesleaks.com/%D8%A7%D9%84%D8%A5%D9%85%D8%A7%D8%B1%D8%A7%D8%AA-15/.

[98] Emiratesleaks, "Millions of Dollars Spent by UAE to Lobbyists in Washington," *Emiratesleaks*, April 19, 2019, https://emiratesleaks.com/en/millions-dollars-spent-uae-lobbyists-washington/.

[99] Emiratesleaks, "*Tansīq Maʿa Mustashārīn Litrāmb Litazwīd Al-ʾimārāt Bimuʿalūmāt Ḣasāsa* [Arrangement with Trump Advisors to Give UAE "Sensitive" Information]," Emiratesleaks, June 28, 2018, https://emiratesleaks.com/%D8%B5%D8%AD%D9%8A%D9%81%D8%A9-10/.

[100] There are a few methodological problems with focusing on explicit mentions of "hacks" and "leaks" or allusions to them in the title, as it may lead to undercounting of leaks. This is especially true in the salacious coverage of the Bezos case, where the editor may not wish to include any information of hacks or leaks in the title. But this is not the case for others; for example, Al-Otaiba stories generally mention leaked emails in the title even when focusing on their content.

Figure 2: Hack-and-leak Media Coverage Focus, 2016-2019



vant throughout, with both sides vying to maintain control of the narrative and avoid being portrayed as the object of scandal.

First, in terms of comparative analysis with the DNC leaks, one potential explanation is that political affiliation influences coverage, so that in the case of the DNC leaks the Russian HLO received greater coverage than the contents of Clinton's emails due to the leftward leanings of the "mainstream media." If treated as a serious hypothesis rather than conspiracy theory, a political spectrum explanation is neither clearly supported nor disproved by the cases considered here. Three cases do not have a clear domestic political affiliation (Al-Otaiba, Azima, Bezos). The one case with a clear affiliation, Broidy, has evenly split media coverage. Recognizing that these cases are transnational as well as domestic, a similar argument based on different sides of political divisions in the Gulf is also unsupported, as these cases come from both sides of the 2017 Qatar split, with differing results.

The scandal literature suggests that the *type* of scandal — moral, political, financial, and so on — may affect impact. In these cases, the leaking actor occasionally named a specific type of transgression. For Al-Otaiba, the claimed rationale was to "expose corruption" and "hurt [the] reputation of American allies and cause policy change."[101] In the Broidy case, the alleged leakers sought to "expose" him, although a court judged that leaking details of political and business meetings did not constitute a disclosure of private facts in Californian law because they did not sufficiently "shock ... decency and propriety."[102] Although there is no explicit rationale available in the Azima or Broidy cases, the content of the initial publications — "scammer" for Azima and "illicit affair" for Bezos — also point to specific types of transgression. Overall, the leaked information covers a broad range of topics, neither supporting nor disproving the view that a certain kind of scandalous information has greater impact.

More specifically, it is not clear that "moral" scandals lead to a focus on content rather than hacking. Both the Bezos and Al-Otaiba cases highlighted supposedly transgressive sexual conduct, with an opposite focus for media coverage.[103] The common element between these cases is therefore not a particular type of scandal, but that the HLO aimed to show that expected standards were not met — what I earlier termed "normative dissonance."

Other potential explanations include the compe-

[101] Poulsen, "Hackers Vow to Release Apparent Trove of U.A.E. Ambassador's Emails."

[102] Friedrich, "Broidy Capital Management LLC, et al., Plaintiffs, v. Nicholas D. Muzin, et al., Defendants. Memorandum Opinion."

[103] It is possible that stories "about" the hack were an excuse or pretext for more salacious discussion of moral and sexual subjects; this is difficult to determine from the data here.

tence and resources of the leaking actor. Competence does not appear to be a good explanation, as reported attributions in all cases suggest highly motivated foreign state actors that are familiar with U.S. politics and possess sufficient financial and technical resources to accomplish their aims. Furthermore, all four cases appeared to use either relatively simple but effective techniques, such as spear-phishing (sending emails deliberately crafted to convince their recipient to click on a malicious link), suggesting a relatively low level of investment for state actors. The news organizations that covered these stories also saw them as part of strategically planned operations. One journalist claimed that "there was thought and calculation behind how this material was being distributed."[104] Others labelled it a new level of cyber security threat.[105] Journalists published these stories despite being aware of this strategic aim. As the *New York Time*'s David Kirkpatrick explained: "If we were to start rejecting information from sources with agendas, we might as well stop putting out the paper."[106] Nonetheless, the format of leaked information may have played a role in deciding the impact of the scandal: Extensive document leaks lend themselves to multiple releases, while a few texts and pictures have limited potential to sustain attention across news cycles.

THE SCANDAL LITERATURE SUGGESTS THAT THE TYPE OF SCANDAL — MORAL, POLITICAL, FINANCIAL, AND SO ON — MAY AFFECT IMPACT.

Another explanation suggested by these cases is that a cover identity for the leaking actor shifts focus onto the content of the leak, even if such a cover is *implausibly* deniable.[107] Attribution is a notoriously difficult element of any cyber intrusion.[108] In addition to limited information and ulterior motives on the part of the attributing party, state actors in general rarely claim responsibility for cyber operations, either staying silent or issuing denials (as in these cases). Attribution is also affected by the interests and capabilities of investigating experts. For example, some commentators linked the Al-Otaiba case to a spoof website registered by the Russian intelligence services for the UAE Ministry of Foreign Affairs; it is unclear whether the two are in fact related.[109]

Consequently, fake identities that deliberately confuse attribution, acting as "false flags,"[110] may prevent media coverage focusing on the hack and shift attention to the content, changing the direction of the scandal. In the Al-Otaiba and Broidy cases — the two with the most media coverage of leaked content — the leak came from "activist" identities (GlobalLeaks and L.A. Confidential, respectively). This tactic echoes other HLO activist identities such as the DNC's DCLeaks, Football Leaks, and Hollywood Leaks.[111]

It is likely that the target's response to the initial leak also partly determines whether media coverage focuses on the hack or the leak elements of the incident. Al-Otaiba's response consisted mainly of downplaying the relevance and credibility of the leaked information. In the Bezos case, the impact of the "blackmail," as Bezos termed it, was diminished because he published the same information himself, accompanied by blogs speculating on the origin of the hack and followed by professional technical reports. Both the Azima and Broidy cases involved

[104] Kevin Collier, "How Persian Gulf Rivals Turned US Media Into Their Battleground," *BuzzFeed News*, May 9, 2018, https://www.buzzfeednews.com/article/kevincollier/qatar-uae-iran-trump-leaks-emails-broidy.

[105] Lake, "The New Threat of 'Leak-Flavored' Propaganda."

[106] Terry Gross and David D. Kirkpatrick, "Reporter Tells Of Persian Gulf Rivalries, Hacked Emails And A Mueller Subpoena," *NPR.org,* March 29, 2018, https://www.npr.org/2018/03/29/597783188/reporter-tells-of-persian-gulf-rivalries-hacked-emails-and-a-mueller-subpoena.

[107] Rory Cormac and Richard J. Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability," *International Affairs* 94, no. 3 (May 2018): 477–94, https://doi.org/10.1093/ia/iiy067.

[108] Brian Krebs, "Blowing the Whistle on Bad Attribution," *Krebs on Security*, Aug. 18, 2017, https://krebsonsecurity.com/2017/08/blowing-the-whistle-on-bad-attribution/; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cyber security* 1, no. 1 (Nov. 2015): 53–67, https://doi.org/10.1093/cybsec/tyv003; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (Jan. 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

[109] Threat Research Team, "FANCY BEAR Has an (IT) Itch That They Can't Scratch," *Fidelis Cyber security*, Aug. 1, 2016, https://fidelissecurity.com/threatgeek/archive/fancy-bear-has-it-itch-they-cant-scratch/.

[110] Brian Bartholomew and Juan Guerrero-Saade, "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," *Virus Bulletin Conference* (Oct. 2016), https://www.virusbulletin.com/blog/2016/november/vb2016-paper-wave-your-false-flags-deception-tactics-muddying-attribution-targeted-attacks/.

[111] Adrian Chen, "Meet the Hollywood Hackers Coming For Your Nude Pics," *Gawker*, Aug. 29, 2011, https://gawker.com/5835611/meet-the-hollywood-hackers-coming-for-your-nude-pics; Sam Knight, "How Football Leaks Is Exposing Corruption in European Soccer," *New Yorker,* May 27, 2019, https://www.newyorker.com/magazine/2019/06/03/how-football-leaks-is-exposing-corruption-in-european-soccer.

exchanges of lawsuits between the target and the claimed intruder, as well as PR agencies. Some of these PR agencies and associated cyber security firms were reportedly involved in the initial leaks: Bell Pottinger for the Azima case and Stonington Strategies, Bluefort Public Relations, and Global Risk Advisors in the Broidy case.[112]

Overall, a strong and carefully managed publicity campaign, whether conducted on highly visible open sources (as for Bezos), or through lawsuits and lobbying (as for Broidy), seems to deflect media attention from the content of the leak. Crucially, these responses supplied a clear alternative message, capitalizing on a recognized media appetite for cyber security and hacking topics to portray the incident as primarily a hack rather than a leak.[113] Hacking tools were no longer just a useful means to generate a story; they became the story itself. In these cases, the struggle between *kāshif* and *makshūf* hinged on whether an opponent's use of hacking tools could be successfully exploited by supportive media or commercially retained PR agencies as a superior scandal to the original leak.

Finally, this reversal of the *kāshif/makshūf* relationship is not merely a simple dynamic of punch and counterpunch, but becomes more complicated when we examine the details of Broidy's response. Specifically, it appears that Broidy's lawyers and PR agents used digital tools in at least two ways to obtain evidence which they then deployed to accuse Qatari agents of the original hack. First, they engaged in standard cyber security incident response including legal and technical measures. For example, once Broidy's team had identified a TinyURL shortening service used to construct the initial phishing website, they then reportedly "issued subpoenas for every website created by the TinyURL user who made the phishing websites."[114] It is possible the L.A. Confidential email address used to leak the documents was registered by the same person who registered these websites and shortened links, which would have enabled Broidy's team to link them together. Second, and more importantly, Broidy's lawsuits rely on phone records and WhatsApp messages from the devices of individuals employed by PR agencies contracted by Qatar for the period in which the leaks occurred. There is no public data to indicate how these records and messages were obtained, although a story by the *New York Times* suggests that a private conversation between these individuals had been covertly recorded in addition to the collection of metadata with call times and contacts.[115] If those investigating the hack-and-leak also engaged in covert recording and leaking of private conversations, then the delicate balance between *kāshif* and *makshūf* could shift once again.

Conclusion

This article has sought to widen the empirical basis of academic and policy debates around hack-and-leak operations by analyzing four cases of HLO in U.S. politics in the three years following the 2016 presidential election. These HLO are examples of what sociological theories term the simulation of scandal: strategic attempts to exploit normative dissonance — a divergence between expected norms and standards and actual practices — to gain advantage in domestic and international political struggles.

Although hacking tools provide a new and relatively accessible means to obtain secret information necessary to simulate scandals, they pose an equal danger for those who use them: The risk that the target of the scandal will successfully portray the hack as more media-worthy than the content of the leak, reversing identities of *kāshif* (revealer) and *makshūf* (revealed). The cast list in this manufactured morality play is wider than a typical list of state actors, one that includes elected officials or government employees. It is also wider than the usual cast list of cyber conflict, already extended to include many non- and semi-state actors, and now extended still further to the wide range of legal, reputational, and PR services that are called upon during scandals caused by HLO.

This article has multiple limitations, which highlight the importance of further work on this topic. These cases continue to evolve, with new data emerging between the initial analysis and the time of writing. The media analysis conducted here could be augmented in many ways. For example, more data on the impact of these cases, rather than inferred impact from popular news articles, could

[112] Friedrich, "Broidy Capital Management LLC, et al., Plaintiffs, v. Nicholas D. Muzin, et al., Defendants. Memorandum Opinion."

[113] Robert M. Lee and Thomas Rid, "OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy," *The RUSI Journal* 159, no. 5 (2014): 4–12, https://doi.org/10.1080/03071847.2014.969932.

[114] Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," *Bloomberg*, Sept. 18, 2018, https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about; Agusti et al., "Complaint and Jury Demand." According to this document, Broidy's assistant was targeted in January 2018 with similar fake Google security alerts, this time from Owly rather than TinyURL.

[115] David D. Kirkpatrick, "'Be Very Careful': Conversation Cited to Link Qatar to Hack of G.O.P. Donor," *New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/be-very-careful-conversation-cited-to-link-qatar-to-hack-of-gop-donor.html.

be included in the data set. Data on participation in the reception of scandal by consumers of these news articles, especially on large social media platforms, would also test this article's conclusions. It is beyond the scope of this article to tackle in detail the relationship of HLO to other forms of disinformation. But the theoretical stance taken here poses a note of caution for studies of HLO impact, as it is difficult for such studies not to be caught up in the unfolding dynamic of scandal itself.

The qualitative judgments taken throughout this article represent a position on how the scandal unfolded, including an assessment of source reliability and the events of the HLO, that is inescapably *part* of the continued development of these events. This article therefore cannot hold on to a pretense of complete objectivity. Furthermore, judgments of strategic intent are especially tentative in this environment. Although the HLO considered here sought to induce normative dissonance, a separate and possibly secondary strategic goal may simply to be to instill doubt and uncertainty about the event itself — the operations may have been designed to generate apathy rather than condemnation. Measuring HLO impact against that aim would be still more difficult.

Nonetheless, this article has several implications for strategic cyber competition. It highlights the risks of engaging in hack-and-leak operations, which can easily backfire and create scandal around the operation itself, rather than its intended subject. It emphasizes that cyber threats to the United States from adversarial states such as Russia and China should not be the only policy focus, as states that are strong military allies and strategic partners also employ cyber techniques to influence U.S. domestic politics. Such relationships mean that the strategic options for interference available to allied actors are limited, making covert cyber operations even more attractive. Such actors seek to bend rules and norms around interactions between allies, carefully pushing boundaries rather than breaking them. The involvement of multiple commercial entities, from cyber security companies to the less frequently noticed actions of PR agencies, makes clear rule-setting even more difficult. Finally, the erratic dance between *kāshif* and *makshūf* in HLO means that their impact is difficult to determine, let alone predict, both for perpetrators and targets. Successes are likely to be temporary, creating just enough pressure and distraction to prevent action in other areas. In a landscape of permanently competing narratives, this *kāshif/makshūf* dynamic is never fully decided and a new scandal, especially one revolving around illicit hacking, can open a crucial window of opportunity for adversaries.

James Shires *is an assistant professor in Cyber security Governance at the Institute of Security and Global Affairs, University of Leiden, in the Netherlands. He is also a nonresident fellow with the Cyber Statecraft Initiative at the Atlantic Council. He was formerly a postdoctoral fellow at the Cyber Project of the Belfer Center for Science and International Affairs, Harvard Kennedy School, where the bulk of the research for this paper was conducted.*

Acknowledgements: *I would like to thank the editors of the special issue, Max Smeets and Robert Chesney, and the editors of* Texas National Security Review, *Doyle Hodges and Gregory Brew, for their feedback, assistance, and encouragement throughout the process. I would also like to thank two anonymous reviewers for their insightful comments, although of course all remaining errors are mine. Finally, I would like to thank everyone at the Belfer Center Cyber Project and elsewhere who provided feedback on this article prior to publication, including several earlier drafts, in no particular order: Andrew Leber, Bruce Schneier, David Eaves, Julia Voo, Lauren Zabierek, and Talia Gifford.*

Photo: Max Pixel