Damaging the opponent 'the new way'

James Shires

Understanding the tactics behind hack-and-leak operations

On November 27, 2019, Jeremy Corbyn, then-leader of the UK Labour Party, held up some official-looking papers, heavily redacted with thick black lines, at a campaign press conference shortly before a crucial second election in three years after the UK's vote to leave the European Union in June 2016. These documents purported to show the details of discussions between the UK and US governments on a potential post-Brexit trade deal, including demands by US representatives to open access to the UK's National Health Service for US companies, an inflammatory issue for many voters. Corbyn's opponent, Conservative Prime Minister Boris Johnson, went on to win the election by a landslide, confirming the UK's departure on January 31, 2020.

Corbyn resigned shortly afterwards, but discussion of the documents themselves, and their provenance, has outlasted Corbyn's leadership. Shortly after Corbyn revealed the documents, cybersecurity company Graphika reported that documents with the same content and metadata – likely identical to Corbyn's intended bombshell – had been posted on Reddit in a manner remarkably similar to a disinformation operation identified by the Atlantic Council's Digital Forensics Research Lab earlier in the year, attributed in the media to individuals in Russia.[1] In August 2020, Reuters confirmed this connection when it reported that "suspected Russian hackers" had obtained the documents from the compromised email account of former Secretary for Trade and Defence Liam Fox.[2]

These documents are an example of 'hack-and-leak operations' (HLO), where malicious actors use cyber tools to gain access to sensitive or secret material and then release it in the public domain. The most well-known example of HLO is 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. Although both the Clinton and Trump campaigns repeatedly revealed lies and transgressions of their opponent, the DNC emails represented a crucial shift between the two. A leaked recording of Trump (the "Access Hollywood" tape) was overshadowed by the documents from the DNC focusing on Clinton's record in government.

But these are not the only examples, and HLO have occurred worldwide in a range of political contexts. Leaks from the anti-doping organization WADA in 2016 and 'Macronleaks' in the 2017 French election are other well-known instances. Overall, the hacking and leaking of sensitive information is widely seen as a severe threat to liberal democratic structures, and policymakers have in turn mobilized significant resources in response, including threat intelligence and cybersecurity protections, increased election and voting security, legislative pressure on social media companies, and even offensive cyberattacks.

However, HLO are complex phenomena, combining cyber intrusion with media manipulation. It is difficult to work out how they occur, and even more difficult to understand their motivations and effects. This article provides one part of the answer to this puzzle, arguing that HLO should

Jeremy Corbyn, then-leader of the UK Labour Party, held up some official-looking papers, heavily redacted with thick black lines, at a campaign press conference in November 2019. In August 2020 Reuters confirmed that "suspected Russian hackers" had obtained the documents from the compromised email account of former Secretary for Trade and Defence Liam Fox (photo: Flickr/Jermy Corbyn)

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. This article draws on several previous works on hack-and-leak operations, including an investigation of HLO in Saudi Arabia and a recent article in *Texas National Security Review* where I make a similar argument.[3]

THE WEAKENED GATEKEEPERS OF THE MEDIA

To understand hack and leak operations, we first need to understand the information space in which they occur. 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. Users can access content from almost anywhere in the world, produced by a variety of actors with intertwined (geo)political, commercial, and normative motivations. Media organizations and publications are increasingly enfolded into narratives of national security that demand urgent legislative and policy solutions. These 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 now usually has its uglier face forward, wearing labels of fake news, post-truth, and the end of objectivity.

Leaks

The leaking of secret or confidential information into the public domain — occupies 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

Hack-and-leak operations are at the pinnacle of digital operations conducted by intelligence agencies, combining intrusion into networks with coordinated and doctored dissemination through traditional and social media (photo: JARIRIYAWAT/Shutterstock.com)

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.

Although anonymous official sources and whistleblowers have always been an important element of political reportage, leaks are now 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.

Leaks have precipitated seismic 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 U.S. and 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. For example, 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.

In sum, leaks are an evergreen aspect of political contest, and can –in certain contexts – change the course of world events, including wars, elections, and geopolitical rivalries. But leaks, in the contemporary media environment, are also a symptom of an inversion of privacy norms as individuals, organizations and states turn inside-out, offering up their secrets to the world. How, then, do certain leaks, including hack-and-leak operations, have an effect in this noisy and chaotic space? For that, we need to look at the concept of scandal.

Scandals

Scandals are a subset of leaks, as there can be no scandal without a disclosure of secret information. 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. Some distinguish the *type* of transgression, while more anthropological 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.

Scandal thus requires what might be termed *normative dissonance*: a divergence between expected and observed or practiced norms and moral standards. This is illustrated most clearly through the figure of a whistleblower, 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.

Scandals not only involve the airing and confirmation of certain values, but also commitment to rational argument and standards of truth. However, in a fast-flowing digital media environment with constant accusations and leaks, political actors seek to gain the upper hand through competing scandal-making. Consequently, the truth as revealed by scandal is always contested and challenged.

Moreover, various actors seek to *simulate* scandal to gain advantage in domestic and international political struggles. This tactic carefully curates moral outrage to appeal to the values and concerns of a target audience. Importantly, the target of a simulated scandal is not merely the subject of the leak, but also those reporting and using the leak for their own ends. In the Corbyn example above, the leaked documents appeared to be selected to embarrass the Conservatives' post-Brexit plans, and to appeal to a core British audience that prizes the NHS highly. But they were probably also designed to manipulate Corbyn and his Labour advisors, with the intent that they would do exactly as they did and reveal the scandal in dramatic fashion.

So far, the leak element of hack-and-leak operations is coming into focus. But what about the hack?

HACK-AND-LEAK OPERATIONS

Hack-and-leak operations fit into a long history of the manipulation of information for national security purposes, which is centrally the preserve and currency of intelligence agencies. Intelligence practices have a complex relationship with leaking.

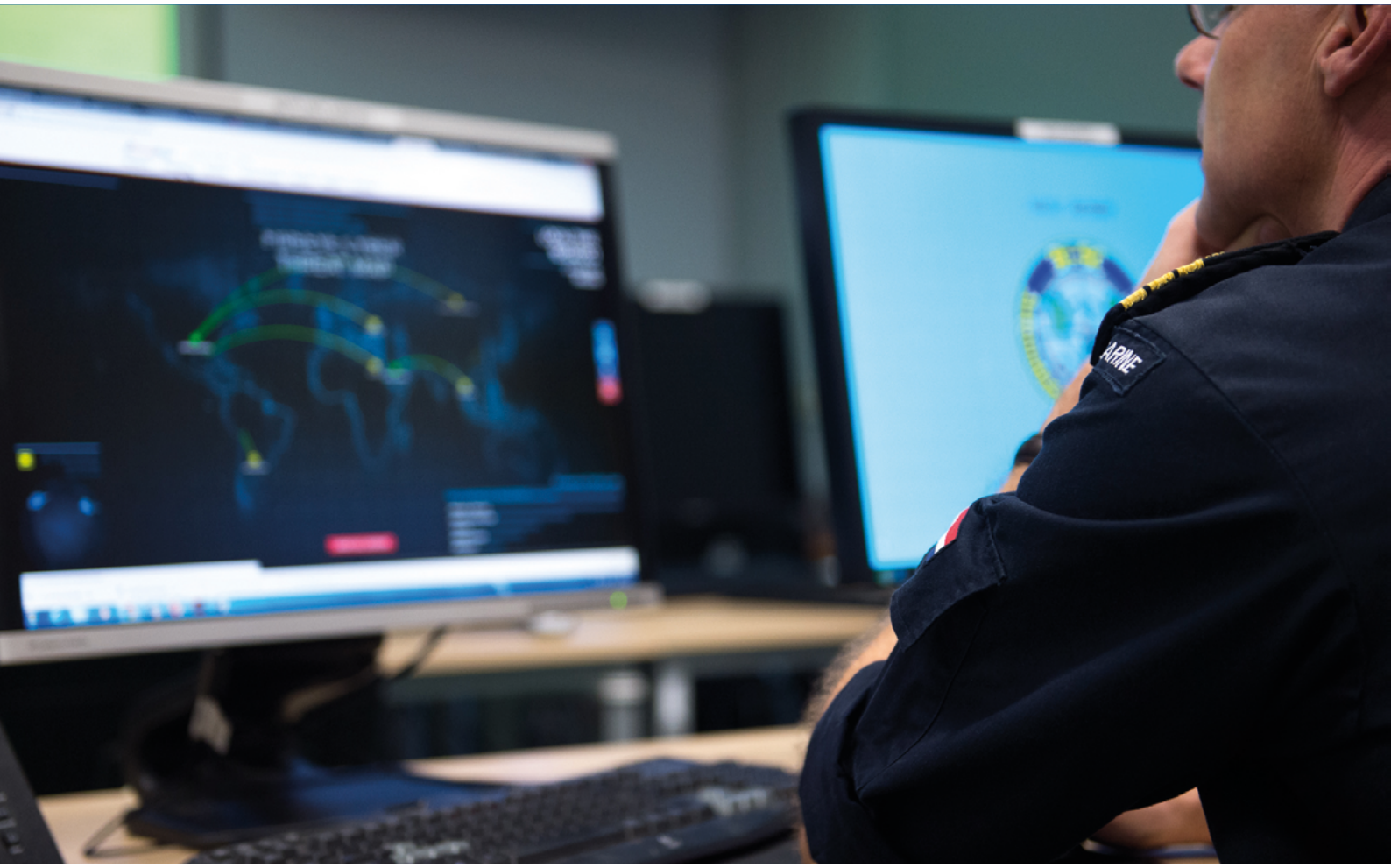
- **First**, third-party leaks are valuable sources, and the extent of private information on the internet means open- or all-source intelligence can be as powerful as secret methods.
- **Second**, intelligence agencies in democracies rely on popular support, regularly shaping policy and public perception through non-classic routes.
- **Third**, leaking – and the threat of leaking — is an effective way to damage adversaries or to convince people to provide information. Leaking, for intelligence agencies, is thus both a powerful advantage and their greatest fear, leading to insularity and internal suspicion.

Digital media are not only the *means* of dissemination for leaked information, but often also their *source*, through data breaches and hack-and-leak operations, also known as "doxing." Doxing — the acquisition and publication of another'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 the sheer hell of it - or to embarrass those who transgressed early norms of behavior on the internet.

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 publishing of reams of personally identifiable information of thousands of government and corporate employees. These later events are "public-interest hacks," in anthropologist Gabriella Coleman's description of activities of the hacker collective Anonymous, among whom she conducted extensive fieldwork, or what noted cybersecurity expert Bruce Schneier has called "political" or "organizational" doxing.[4] Both leaks and doxes can release objects and capabilities in the form of computer code, as well as more traditional text documents. I use "hack-and-leak operation" 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.

ESPIONAGE IN THE DIGITAL AGE

Espionage in the modern era relies as much on signals intelligence — telecoms, radio, and now internet communications — as traditional human sources. Digital signals intelligence can be obtained passively through collection 'on the wire' (e.g. undersea internet cables), as well as actively through targeted hacks - or a combination of the two. Hack-and-leak operations are at the pinnacle of digital operations conducted by intelligence



NATO partners should develop a coherent strategy and thorough understanding of the dynamics of hacking and leaking, based on academic research on both cyber conflict and digital media. Pictured is Alex de Nijs from the Royal Netherlands Navy during NATO Exercise Cyber Coalition 16 in 2016 in Tallin, Estonia (photo: Flickr/Shape NATO)

agencies, combining intrusion into networks with coordinated and doctored dissemination through traditional and social media.

Accusations of HLO are not limited to Russia. The US also likely operates in this sphere, as illustrated by the shift to 'persistent engagement' in the Department of Defense's cyber strategy, and more recent leaked executive orders that make it easier for the CIA to "engage in the kind of hack-and-dump operations that Russian hackers and WikiLeaks popularized."[5] Putin already believes that the Panama Papers leak was a targeted US intelligence operation, and last year's releases of Iranian offensive cyber tools online look like exactly the kind of operation that would be authorized under this order.[6]

Do they work? HLO are complex, multi-causal events, but their outcome generally hinges on whether an opponent's use of hacking tools could be successfully exploited as a superior scandal to the original leak. We can understand this dynamic by examining the weight of media coverage, between stories that focus on the content of the leak and stories that focus on the details of the hack. The relationship between these two forms of coverage suggests the trajectory of the scandal overall, directed towards the hacking operation itself or away from it, towards the content revealed by the hack. Consequently, while 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: that the target of the scandal will successfully portray the hack as more media-worthy than the content of the leak.

For the Corbyn documents, the weight of coverage has shifted in the direction of the hack. As the UK's Intelligence and Security Committee prepares to release a report into Russian interference in the Brexit referendum, public interest in attempts to change the course of the 2019 election is also growing, while the global pandemic and a lull in trade talks mean that 'selling' the NHS is no longer as salient. This balance may, of course, change as the transition period ends, the pandemic becomes part of normal life, and the UK's economic relationship with the US comes under renewed scrutiny.

CONCLUSION

HLO are a frontier in digital forms of foreign interference. They are a manufactured morality play on the digital stage, with hacking tools as the fulcrum of a constant

struggle for attention in a complex and unpredictable media environment. The common element between different HLO cases, in the UK, US, France, and elsewhere, is not a particular type of scandal, but that the hack-and-leak operation aimed to show that expected standards were not met, what I term "normative dissonance."

However, as attempts at the simulation of scandal, the success of HLO depends on the shifting power dynamic between the scandal-maker and the scandal-subject. There are clear risks in engaging in HLO, as they can easily backfire and create scandal around the operation itself rather than its intended subject. The erratic dance of hack-and-leak operations 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 dynamic is never fully decided, and a new scandal, especially one revolving around illicit hacking, can open a crucial window of opportunity for adversaries.

NATO partners should develop a coherent strategy and thorough understanding of the dynamics of hacking and leaking, based on academic research on both cyber conflict and digital media. In a time when information spreads almost unfiltered and unhindered through the digital space, where state *and* media control is limited, it is crucial to respond in a timely and proportionate manner to hacking and disinformation campaigns conducted by adversaries.

For NATO, the development of both defensive and offensive policy on hack-and-leak operations needs to acknowledge their risks at tactical, strategic, and normative levels, building these risks into operational decision-making, especially in key democratic junctures such as national or regional elections. The impact of hack-and-leak operations should also be analyzed along gender-based and intersectional lines (race, class, and other forms of inequality). Cybersecurity already has a blind spot for some gender-differentiated harms, and HLO are likely to disproportionately impact women and people of color due to prevalent societal expectations around what constitutes scandalous behavior.[7] Previous Russian information operations have sought to inflame racial tensions in the U.S., and women in politics around the world already face extensive misogynist abuse online. Hack-and-leak operations could easily provide fuel for sexist or racist targeting of specific individuals or political parties in NATO states.

Overall, in addition to 'hard cyber' threats which could lead to disruption of digitally connected infrastructure, NATO partners must also understand the dynamic of leaking and hacking in a more 'soft power' sphere. New ways of influencing the public, ever easier with the rise of the internet and social media, might be as dangerous as the next Stuxnet. But countering evolving threats to the online public sphere while protecting fundamental rights and freedoms such as privacy and freedom of expression – a core part of NATO's mission – is an even harder task, and the most important one.

James Shires is an Assistant Professor in Cybersecurity 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.

Would you like to react?
Mail the editor: redactie@atlcom.nl.

1. For an overview of the operation, and timeline of disclosures on the Secondary Infektion group, see Ben Nimmo et al., "Secondary Infektion" (Graphika, June 2020).
2. Jack Stubbs and Guy Faulconbridge, "Exclusive: Papers Leaked before UK Election in Suspected Russian Operation Were Hacked from Ex-Trade Minister - Sources," Reuters, August 4, 2020, https://uk.reuters.com/article/uk-britain-russia-hack-exclusive-idUKKBN24Z1UL.
3. James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," Journal of Cyber Policy 4, no. 2 (2019): 235–56; James Shires, "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics," Texas National Security Review, August 2020.
4. Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (London: Verso, 2014); Bruce Schneier, "Organizational Doxing," Schneier on Security, July 10, 2015, https://perma.cc/R3LV-ZT5R; Bruce Schneier, "The Rise of Political Doxing," Schneier on Security, November 2, 2015, https://perma.cc/5RGW-UTB3.
5. Zack Dorfman et al., "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks," Yahoo News, July 15, 2020, https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html; Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," Intelligence and National Security 0, no. 0 (February 15, 2020): 1–10, https://doi.org/10.1080/02684527.2020.1729316.
6. Catalin Cimpanu, "New Leaks of Iranian Cyber-Espionage Operations Hit Telegram and the Dark Web," ZDNet, May 9, 2019, https://perma.cc/MRN6-QUFC.
7. Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity," St. Anthony's International Review 15, no. 1 (May 1, 2019).