Hacking/Journalism

Philip Di Salvo explores the trading zone between journalism and hacking.

JOURNALISM AND HACKING ARE GETTING closer in recent times. WikiLeaks, the Snowden case and the other published "megaleaks" have blurred the boundaries between newsrooms and hackers and inspired the rise of a hybrid form of reporting, where elements historically associated with hacking are now also visibly involved in journalism. This hybridization is the result of a process of boundary-crossing, whose most visible manifestation is in the adoption of new technologies. For instance, reporters increasingly rely on encryption tools to protect their sources and their work. Whistleblowing cases have been where this process has taken place in the most extensive way.

Whistleblowers have always supplied investigative reporters with leaks, leads, and documents. The notable US instances from the 70s, like the Watergate and the Pentagon Papers cases, established whistleblowing-led journalism and made it mainstream and part of the popular record. The act of blowing the whistle hasn't changed much since. A substantial game changer was WikiLeaks and the digital "megaleaks" it published starting from 2010. WikiLeaks' Afghan and Iraqi War Logs, together with the Cablegate leaks, were an unprecedented novelty for journalism: they were composed of a hundred thousand documents in digital format that were leaked through encrypted channels to a hacker organization by Chelsea Manning, a US soldier turned whistleblower with cultural ties to the hacking community. When it comes to journalistic and newsroom practices, the most disruptive change came when WikiLeaks began to partner with major news organizations to publish material; encryption played an enabling role in that whistleblowing. The WikiLeaks and journalists "consortium" represented a turning point in the relationship between journalism and hacking and it was able to put hackers and reporters at the same table, working jointly by sharing goals, skills, tools and practices. On that occasion, WikiLeaks contributed the source material and the technology, a resource that newspapers didn't have at the time, while journalists brought their editorial skills and knowledge and, moreover, access to their audiences and influence.

In 2013 the Snowden case strengthened further the connection between hackers and journalists. Whistleblower Edward Snowden had strong affinities with the hacking community; the subjects of the leak – surveillance and cybersecurity – were core issues for hackers and, once again, encryption tools played a fundamental part in facilitating communication between the source and the journalists. Allegedly, Glenn Greenwald risked losing the story of the decade by not following Snowden's request to communicate via safer channels. The debate about encryption that followed the Snowden case inspired more journalists and media outlets to adopt cybersecurity strategies and practices in order to better protect their work in times of pervasive digital surveillance. At the same time, other similar hacking-influenced instances of journalism based on digital leaks have also multiplied: Offshore Leaks (or the "Panama Papers", "Swiss Leaks" and "Luxembourg Leaks"), published by the International Consortium of Investigative Journalists (ICIJ) and the "Drone Papers", published by *The Intercept*. These cases helped set new standards for reporting on leaked material and showed the potential of a proactive attitude towards encryption.

As Baack argues (2016), digital leaks have now become normalized for

"Everybody Needs a Hacker"
PHOTO BY ALEXANDRE DULAUNOY / FLICKR CC / BY-SA 2.0

contemporary journalism and, because of the recurring presence of hackers and their technology, it is possible to look at some of these instances in order to describe how journalism is becoming more like hacking. The encryption tools used by Snowden and Greenwald to communicate with one another, for instance, exemplifies how journalists and reporters are now routinely embedding traditional hacking tools within their toolbox. Pretty Good Privacy (PGP) encryption software, the Off-the-record (OTR) encryption chatting protocol, and the mobile app Signal are now commonly included in the journalism toolbox; digital security literacy is now directly associated with the duty of protecting sources in the digital era. WikiLeaks pioneered a peculiar tactic to digital whistleblowing with its own online encrypted anonymizing submission system, whose approach is now used, via the hacker-coded GlobaLeaks and SecureDrop open source software, also by several major news organizations such as *Associated Press*, *Washington Post*, *The Guardian* and *Vice*, among others. Encryption has now become a crucial strategy for reporters in need of a safe digital environment, or to apply "data disobedience" to shield their work (Brunton & Nissembaum, 2015: 62).

The adoption of encryption in journalism has created a hybridization of practices between hackers and journalists that can be described as a "trading zone" (Galison, 1997; Lewis and Usher, 2014). "Trading zones" are symbolic spaces where actors hailing from different backgrounds work with shared purposes. For hackers, encryption has always held connotations of political resistance and the stress on privacy protection and anonymity safeguards is often part of the definition of the identity of hackers as well. For journalists encryption helps protect not only themselves and their work, but also their sources, giving them robust safeguards and protection from tracking and retaliation. In their tripartite analysis, Coleman and Golub (2008) have identified "cryptofreedom" to indicate how encryption is used by hackers as one "moral expression of hacking." In the "trading zone" between hackers and journalists what is being adopted by the latter is an approach to technology—and encryption tools in particular—that wasn't at all routinized in journalism before WikiLeaks and Snowden. Charlie Beckett (2012: 32-33) defines "networked journalism" as the transformation of journalism from "a closed to an open system," where elements that were not once included in the journalism ecosystem are now being embedded in it. In recent times, "networked journalism" has been used to explain the context in which new formats of news making, new identities, and new professional boundaries have been set. Data journalism is a good example of this process, as it embodies elements – such as data analysis and data visualization – that are not defining elements of journalism per sé. Consequently, the "boundaries of journalism" have expanded (Carlson and Lewis, 2015) to the extent that tactics whose roots are not entirely in journalism – such as adopting encryption tools in our case – can now have a role in the media ecosystem and can contribute to the news-making process.

This said, the encounter of journalism with hacking can't be explained by changes in journalism alone. This hybrid "trading zone" has also been enabled by the growing process of politicization of hacking and the new political stances that emerged among hackers engaged in direct action or civil disobedience as tactics (Coleman, 2017). Politicization has become more visible especially in regards to leaks in the service of civic and public goals and with media exposure as an aim. Hackers and hacktivists have become

BIBLIOGRAPHY

Baack, Stefan. (2016). "What big data leaks tell us about the future of journalism – and its past." *Internet Policy Review – Journal on Internet Regulation*, available at: link.

Beckett, Charlie. (2012). *WikiLeaks. News in the Networked Era.* Cambridge: Polity Press.

Brunton, Finn & Nissenbaum, Helen. (2015). *Obfuscation. A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.

Carlson, Matt & Lewis, Seth. C. (eds.). (2015). *Boundaries of Journalism. Professionalism, Practices and Participation.* London: Routledge.

Coleman, Gabriella & Golub, Alex. (2008). "Hacker practice: Moral genres and the cultural articulation of liberalism." *Anthropological Theory*, 8(3): 255-277.

Coleman, Gabriella. (2017). "From Internet Farming to the Weapons of the Geek". *Current Anthropology*, vol. 58(15): 91-103.

Edward Snowden
PHOTO BYGAGE SKIDMORE / FLICKR CC / BY-SA 2.0

more involved in the communication field and more interested in "work traditionally ascribed to journalists, expanding what it means to be involved in the production of news and, in the process, gaining influence over how traditional news stories and genres are constructed and circulated" (Russell, 2016: 7). This process was also helped by the "fluidity" of the hacker identity which, despite a loose acceptance of a common ethos, has always been "pliable, performative and fluid" (Fish & Follis, 2016) and consequently open to the widening of the spectrum of their activities.

According to Adrienne Russell, this hybridization is also visible in the rise of what she calls a new "media vanguard" composed of "journalists, activists, communication-technology hackers" who "are exerting significant influence in today's media environment through innovation and media competence" (2016: 9-10). At the current stage, it is important to point out how this hacking-influenced form of reporting has received differential forms of acceptance within the journalism community. It would be wrong to claim this represents a globally accepted status quo. Some news outlets, especially in the US, have embraced working with hackers and technology more explicitly and have made it the defining element of their editorial strategy: Glenn Greenwald's *The Intercept*, for instance, has put "adversarial journalism" in the field of surveillance and cyber-affairs at its core. Together with the wide adoption of encryption as a central component of its reporting, *The Intercept* has been extensively covering hacking cases, establishing a generally positive attitude towards hackers. *ProPublica* also frequently works with hackers and coders of different backgrounds, including digital security or data journalism, and has also published first-hand reporting on the Snowden documents.

Other outlets' acceptance of hacking has been far more reserved: while still covering news or documents coming from hacking cases, for instance, the *New York Times*, has been notably critical of hackers and hacktivists such as Julian Assange; and they have been more aloof than other news outlets while covering Edward Snowden (Di Salvo & Negro, 2015). *The Washington Post*, despite having reported on the Snowden files, having won a Pulitzer Prize for its own coverage of the NSA case, and being a SecureDrop adopter, called for President Obama not to pardon Snowden (Washington Post, 2016). Further research, and ethnographic research in particular, will help in grasping the new boundaries of journalism and how they are set, established and influenced by hacking. When it comes to digital security, encryption and source protection, for instance, the contribution of hackers is crucial for literacy, knowledge sharing and tools-crafting in the journalistic field. Moreover, hacking-influenced journalism has proven to be a catalyst for investigative reporting; some of the most interesting journalistic investigations of recent times has involved some form of hacking. For newsrooms, in times of pervasive digital surveillance, journalists are put under new threats and pressures. Being proactively ready to assist whistleblowers and sources with proper encryption tools will become increasingly urgent. ■

PHILIP DI SALVO *is a researcher and a journalist. Currently, he is a doctoral student at Università della Svizzera Italiana (Lugano, Switzerland), doing research on digital whistleblowing and the relationship between hacking and journalism. As a journalist, he writes for* Wired *and* Motherboard, *among others. He is also* The European Journalism Observatory *Italian editor.*

Di Salvo, Philip & Negro, Gianluigi. (2015). "Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States." *Journalism*,17(7): 805-822.
Fish, Adam & Follis, Luca. (2016). "Gagged and Doxed: Hacktivism's Self-Incrimination Complex". *International Journal of Communication*, 10: 3281-3300.
Galison, Peter. (1997). *Image & logic: A Material Culture of Microphysics*. Chicago: The University of Chicago Press.
Lewis, Seth. C., & Usher, Nikki. (2014). "Code, collaboration, and the future of journalism: a case study of the Hacks/Hackers global network." *Digital Journalism*, 2(3): 383-393.
Russell, Adrienne. (2016). *Journalism as Activism. Recoding Media Power*. Cambridge: Polity.
Washington Post. (2016). "No pardon for Edward Snowden." *The Washington Post*, September 17. Available at: link.