Asian Journal of Research in Social Sciences and Humanities
ISSN: 2249-7315 Vol. 11, Issue 11, November 2021 SJIF 2021 = 8.037
A peer reviewed journal

A REVIEW PAPER ON HACKING'S ANCESTORS

Manoj Agarwal*

* Associate Professor,
Department of Account & Maths,
Teerthanker Mahaveer Institute of Management and Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: manoj.management@tmu.ac.in
DOI: 10.5958/2249-7315.2021.00189.1

ABSTRACT

Hacking is now a widely studied and recognized phenomena, but it is still difficult to define and experimentally identify since it has come to refer to a broad range of material activities, some of which are incompatible. By briefly reviewing Foucault's idea of genealogy and interpreting its perspectival position via the feminist materialist concept of the situated observer, this article offers genealogy as a framework for understanding hacking. A history of hacking will be presented in four stages, using genealogy as a theoretical frame. The 'pre-history' of hacking is the initial phase, during which four fundamental hacking techniques were established. The second phase is the so-called "golden era of cracking," in which hacking becomes a self-aware identity and culture, with many people associating it with breaking into computers, even as non-cracking activities like free software develop. The growth of serious cybercrime, hacktivism, the separation of Open Source and Free Software, and hacking as a business and work ethic are all part of the third phase, which sees hacking split into a variety of new activities while old ones persist. The last phase involves widespread awareness of government-sponsored hacking, the resurgence of hardware hacking in maker labs and hack spaces, and the spread of hacking as a generalized "smart" activity. Finally, it will be argued that hacking is an interrogation of the rationality of information techno-cultures enacted by each hacker practice situating itself within a particular techno-culture and then using that techno-culture to change itself, both in terms of changing potential actions that can be taken and changing the nature of the techno-culture itself, across all of the practices surveyed.

KEYWORDS: *Computer, Cyber, Genealogy, Hacking, Idea.*

1. INTRODUCTION

Despite twenty years of continuous study into hacking, the definition of hacking remains a mystery. The UK 'phone hacking' incident, for example, confused the concept of hacking in the 2010s, a collection of activities that were largely different from getting into computers. While some accounts now locate a 'narrow' or 'pure' sense of hacking in illegal remote access to computer systems, abstract and general accounts such as those of Himanen and Wark describe a particular social practice as hacking and open up the possibility of hacking virtually anything, as seen in 'lifehacking.' Hacking's significance and public knowledge have increased, yet its meaning has remained elusive. In addition, hacking as a computer-mediated activity has been around for a while and has evolved; we have memories of hacking[1].

Hacking, I shall argue, should be seen as activities that reflect the logic of information techno-cultures. I'll do so by arguing that returning to Foucault's genealogy idea and expanding it via feminist materialism provides a framework for analysis that explains the meaning of hacking.

Within this genealogical framework, a history of hacking is described in four phases: diversity in the pre-history of hacking; the golden era of (cr)hacking; hacking divides; and hacking as both victorious and lost. Finally, this article ends by claiming, based on this four-part history, that the essence of hacking and its position in twenty-first-century society is that hacking reflects the rationality of information techno-cultures in the sense of logics and discourses. In their continuous information technology-enabled activities that reproduce the same technologies to allow new actions, hacking exposes the logics of the intersection of information technology and information cultures[2].

1.1 Genealogy and a Hacking Genealogy:

In the early 1970s, Foucault advocated for genealogy as a method of bringing the past into the present. Miller (1994) and Macey (1994) are two examples of this. Without going through the vast and important literature on the subject, I'll summarize the main concepts of genealogy and expand them quickly via a crucial feminist intervention in order to establish a framework for analyzing hacking. As a result, although this framing is not intended to be a complete study of such a genealogy frame, it does serve as a means of refining the nature of hacking[3].

Foucauldian genealogy is based on three distinct concepts, which are illustrated by the strategy of refusing to accept an origin as an explanation. The first is that genealogy is anti-teleological, in that it does not read history from the perspective of either the 'now,' in which past events are only significant if they lead to our current state, or, in a similar way, the 'victim,' in which past events are only significant if they contributed to whoever holds power in the present. Second, genealogy examines the functioning of things that seem to have no history—love, sexuality—and pays attention to how they operate in the present. Last but not least, genealogy is concerned with occurrences that aren't present and tries to understand the meaning of these omissions. The denial of origins as a legitimate explanatory concept brings these three views together[4]–[7].

The role Steven Levy's articulation of the "hacker ethic" has had in understanding hacking is an example of origin as explanation that will be recognizable to anyone who have done virtually any reading or study on hacking. (1984, Levy) Levy's work as a journalist was important in establishing the origins of hacking by outlining a history of hacking whose spirit he summed up in six principles. These ideas therefore serve as an articulated genesis narrative for hacking, since they recur often as the definition of hacking that crystallized at its inception. In summary, following Levy, the hack as an unexpected and spectacular work of technical detournement, as described in Levy's ethic, became the self-referential genesis and explanation for hacking. To build a genealogy of hacking, we must be skeptical of this oft-repeated genesis narrative, in which the hacking ethic comes from MIT's model train club, their friends and cognates, and their love for technical trickery. To propose variations to Levy's mainly USA-based narrative, we just need to look at the (so far) unrecorded histories of Fidonet (a global network of home computers linked through phone lines), the European computer organizations Chaos Computer Club, or XS4ALL[8].

The distrust of Levy and origins suggests the use of genealogy to explain hacking. Foucault's thesis is that historical study, rather than uncovering a "timeless and eternal secret," inevitably disappoints in its quest for the beginning. He cites the pursuit of the origin of reason as an example of how it can be seen as an invention of the ruling class rather than an inviolable element of human nature, or how the pursuit of the origin of liberty can be seen as an invention of the ruling class rather than an inviolable element of human nature. (P. 142, Foucault, 1977) 'What is discovered at the historical beginning of things is not the inviolable integrity of their origin; it is the discord of other things,' Foucault says, rather than the unity and truth provided by the start[9].

1.2 Part 1 of A History of Hacking: Phones, Trains, and Mainframes:

The origins of hacking may be seen in four strands that intertwined and flowed around each other, not creating an originary assemblage but complexly linking differentiations. Jordan (1999b), Taylor (1999), and Thomas (2003) Conceptions of cyberspace as a place, techniques for manipulating materialised information, communities in virtual environments, and the rise of programming as a profession involving both free software programmers and the programming proletariat were all early and multiple threads of hacking as the internet became more widely used. These will be discussed one by one[10].

Early on in the rise of networked computer communication, including non-internet networks like local bulletin board systems and globalised computer mediated communication like Fidonet (a globally connected network of home computers), the notion that wherever discussions were taking place could be conceptualized spatially grew. There was a feeling that there was a 'place' out there somewhere between all of the non-virtual chairs from which people were talking. Many people conveyed a feeling of going ‘somewhere' even though they were sitting at a computer typing, whether in the early illegal conference calls set up by phone phreaks (a word for individuals who exploited phone networks) or in voluminous postings in places like major discussion site Usenet. This gave rise to the idea that this place and area, commonly referred to as cyberspace, had its own ethics and politics, as well as its own set of values. Optimists advocated for a code of ethics based only on the value of the words individuals were giving, while pessimists decried the constant rudeness and abuse (or flaming), and both were probably correct. Hacking arises from the idea that cyberspace is a separate entity with its own set of values. Techniques for modifying technology that focused on information manipulation also developed.

These originated from a variety of places, probably most notably from phone "phreaks," who tampered with telephone transmission and were frequently inspired by amateur radio, as well as (famously in Levy's account) by operating a sophisticated model railroad, pranks, and lock picking. These are technological tinkerings that accomplish things that they weren't intended or anticipated to achieve. While such ingenious applications of technology are not exclusive to hacking, such grassroots and "do-it-yourself" approaches to altering information technologies contribute to the nature of hacking. Within settings characterized by information networks, in particular, a dynamic develops in which it is frequently impossible to show someone has effectively exploited a technology until the manipulation is taught to someone else. You can see a lock open if someone successfully unpicks it, but manipulation across a network is typically difficult to prove unless someone is also shown how to do it. This is not true of all operations; software, for example, may simply be run to demonstrate its functionality; but, demonstrating that any code was an elegant or smart solution would almost certainly require explaining how it was created, thus requiring training in the solution. Manipulation of technologies can only be demonstrated in a large number of networked information settings if others are also taught how to control the technology. This implies that there are a variety of methods for altering information technology, as well as a dynamic of peer education in making such changes.

The development of a feeling of community in online locations is related to, but different from, both the idea of cyberspace as a place and the production of information manipulation methods used to that place. These virtual communities, as Rheingold memorably dubbed them, have gained in popularity in the twenty-first century, especially via different implementations in social media networks. These locations, which were often text-based at first, fostered social relationships that resulted in the formation of specific collectives or communities. While community is a tough term to define, in this case it refers to an online place where the daily is performed. This also gives birth to the feeling of sub-communities and sub-cultures that emerge on the internet as a result of its ability to transcend isolation and distance, allowing people with similar interests to connect with others who share their interests. Many 'virtual communities of interest' arose, including hackers who created journals and face-to-face conferences, through which their shared interests fueled the

growth of a new community.

1.3 Part II of A History of Hacking: The Golden Age of (Cr)Hacking:

The term "golden era" of hacking refers to a period when the difference between cracking and hacking was almost non-existent (and it should be noted was hardly a golden age for computer administrators or security professionals). 'Cracking' is a term used to describe illegally getting into another person's computer through a variety of methods, such as social engineering (fooling someone into providing access) or exploiting technical flaws. A focus on cracking in police arrests and media coverage, combined with a growing interest in 'exploring' computer and network technologies, led to a near-identification of cracking and hacking during this period, something that was often contested only within (at the time) arcane and obscured communities like the still-emerging free software programming community or the cypherpunks. (According to Levy, 2001) As hacking evolved as a self-conscious and widely noticed community of practice, hacking as an intellectual pursuit, hacking as a political community, and the almost unnoticed growth of other kinds of hackers, three different frames can be used to understand how the threads discussed in the previous section were integrated, fragmented, and reformed during this period. We can see how they interact with technologies that generate restricted fields of activity in order to change those technologies and develop new limited fields of action in all three.

By the 1990s, the concept of cyberspace as a location with both communities and a certain politics or set of values in which specific methods were employed to change information infrastructures had already been established (as noted earlier). These concepts coalesced into the concept of hacking as the act of breaking into networked systems for the sake of intellectual inquiry. This is one of the definitions of hacking that is becoming more difficult to remember as the twenty-first century progresses, for reasons that will become apparent when cracking evolves into large-scale criminal and nation-state sabotage and spying activities. Yet, according to hacker stories, interviews, and retellings of their exploits from the time, they cracked open sites through technical innovation, tricking operators, finding software flaws, and other means, and once they had cracked open sites, they explored them primarily for the intellectual thrill of being able to work out the problems that needed to be solved in order to break in. Whatever method is utilized, the practice is one of doing previously forbidden activities (computer access) and modifying technologies to perform new actions (access). Hackers at the time developed methods that demonstrate their commitment to intellectual inquiry. Hackers, for example, became renowned for getting into systems and then informing the system's controllers how they did it and offering (usually unwelcome) suggestions on how to repair them. Hackers exploited a number of regular procedures used by academics and others who want to exchange knowledge, the most apparent of which are public conferences and publications, neither of which are often associated with criminal subcultures.

1. DISCUSSION

The author has discussed about thehacking's ancestors,the data focuses on major shifts in hacking techniques, as well as the cultures and communities that surround them. This focus on practices, cultures, and communities in my research on hacking harkens back to my days as a sociologist studying hackers when they were often categorized as solitary, anti-social, and troubled young men. Hackers, on the other hand, should be understood as developing a decentralized and dispersed collective identity, and as being only physically isolated by being at a computer, but always in communication with others over the internet, as well as having a strong tendency to form groups that met in person. If hackers were a "social movement" in this sense, they were an information technology-focused movement, not in the sense that they were determined by their technologies, but in the sense that their material and collective practices were constantly attacking

technologies and the determinations they produce in everyday situations in order to change those determinations. This link between practices and communities supports the idea that if hacking is to signify anything, it can't be stretched too far to the point where any activity might be called a hack, or it will become a phantom. The key example from the last forty years of hacking is how hacking was reduced to cracking practices in the late twentieth century and then shifted such that by the first ten years of the twenty-first century, free software practices had become so widely recognized that their constructive creativity in making software was seen by many as a model of a new social or business practice called hacking.

2. CONCLUSION

The author has concluded about thehacking's ancestors, this essay provides genealogy as a framework for understanding hacking by briefly revisiting Foucault's notion of genealogy and analyzing its perspectival position through the feminist materialist concept of the situated observer. A four-part history of hacking will be presented using genealogy as a theoretical framework. The first phase of hacking is known as the "pre-history," and it is at this time that four basic hacking methods were developed. The second phase is the "golden age of cracking," in which hacking becomes a self-aware identity and culture, with many people connecting it with breaking into computers, even as non-cracking activities such as free software grow in popularity. The third phase, which sees hacking divide into a number of new activities while old ones continue, includes the development of serious cybercrime, hacktivism, the separation of Open Source and Free Software, and hacking as a business and work ethic. The last phase includes increased public knowledge of government-sponsored hacking, a revival of hardware hacking in maker labs and hack spaces, and the expansion of hacking as a generic "smart" hobby.

REFERENCES

1. A. Bittau, A. Belay, A. Mashtizadeh, D. Mazières, and D. Boneh, “Hacking blind,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 227–242, 2014, doi: 10.1109/SP.2014.22.

2. J. Erickson, *Hacking: The Art of Exploitation, 2nd Edition*. .

3. “Title: A Genealogy of Hacking Professor Tim Jordan, University of Sussex Word Count: 8,253 (9,554 with Bibliography included),” vol. 253, pp. 1–34.

4. Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, “Hacking, protection and the consequences of hacking,” *Communications - Scientific Letters of the University of Zilina*. 2018, doi: 10.26552/com.C.2018.2.83-87.

5. T. Jordan, “A genealogy of hacking,” *Convergence*, 2017, doi: 10.1177/1354856516640710.

6. B. O. Omoyiola, “The Legality of Ethical Hacking,” *J. Comput. Eng.*, 2018.

7. U. S. Barros and M. S. Barros, “A Survey of Ethical Hacking process and Security,” in *International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2015.

8. J. Billig, Y. Danilchenko, and C. E. Frank, “Evaluation of google hacking,” in *Proceedings of the 5th Annual Conference on Information Security Curriculum Development, InfoSecCD ’08*, 2008, doi: 10.1145/1456625.1456634.

9. C. Lakshmi and P. I. Basarkod, “BASICS OF ETHICAL HACKING,” 2015.

10. V. V. N. Suresh Kumar, “Ethical Hacking and Penetration Testing Strategies,” *Int. J. Emerg. Technol. Comput. Sci. Electron.*, 2014.