David S. Wall

29 Hacking

Abstract: This chapter explores hackers and hacking. It looks at the changing role of the hacker over the years from its moralistic origins in cyberpunk social science fiction to its conceptual links with cybercrimes in the advanced computing technologies of the 21st century. The focus is mainly upon cyber-dependent (criminal) attacks upon the security of networked computers rather than cyber-enabled attacks which are primarily the domain of the fraudster. This differentiation is important if policymakers and law enforcement practitioners are to successfully identify and prosecute or manage cyber-malfeasance. It is also important because the cultural history of hacking explains it as both legal and illegal, so being able to delineate between the two levels of action is significant if law enforcement and cybersecurity agencies are to be effective in establishing trust in the integrity of computer networks and everything that they represent, including their services to users.

Keywords: hacking, cybercrime, changing role of hackers

This contribution looks at hackers, the process of hacking, and the changing role of the hacker over the years from its moralistic origins in cyberpunk social science fiction to its conceptual links with cybercrimes (Wall, 2012) in the advanced computing technologies of the 21st century (see Cybercrime by Holt and Holt). It presents the variations and developments in hacking that now focus mainly upon what are colloquially referred to as cyber-dependent (criminal) attacks upon the security of networked computers rather than cyber-enabled attacks which are mainly the domain of the fraudster (see Wall, 2024: 53–58). Such an understanding of the threats that hackers pose is important if the concept is used by policymakers and law enforcement practitioners to successfully identify and prosecute or manage cyber-malfeasance. Especially as the cultural (rather than solely legal) history of hacking means that it can be both licit and illicit, and legal and illegal, thus, being able to delineate between the two levels of action is an important focus of study. Without trust in the integrity of computer networks, everything that they represent, including their services to users becomes compromised. This contribution briefly describes the changing meaning of hacking over the years, the variation of actions and tactics that hackers use, and how they learn and reproduce their hacking skills. It then looks at the motivations and attractions for offending before concluding.

Funding note: This chapter is based upon research conducted for the EPSRC funded research project "Combatting cRiminals In The Cloud" (CRITiCal – EP/M020576/1) which contributed to Chapter 4 of Wall (2024).

Open Access. © 2025 the author(s), published by De Gruyter. BY-NC-ND This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. https://doi.org/10.1515/9783111062037-030

The changing meaning of hacking over the years

A broad reading of the literature relating to hacking reveals an etymology historically linked to developments in technology. These developments range from using an axe in medieval times to hack a way through obstacles (such as a forest), to using code in more modern times to hack through security protocols of computer programs and systems, often releasing the information within or modifying it. Hacking is therefore "an unconventional or unorthodox application of technology" (Sampson, 1959; 2005) to achieve one's goals. Sampson (2005) later expanded his 1959 definition to explain that a hacker is someone who not only "avoids the standard solution," but the hack itself becomes the basic concept to the point that the hacker becomes defined by the hack. And this captures the hacker spirit that inspired the early cyberpunk social science fiction of William Gibson, Bruce Sterling, Neal Stephenson, and Bruce Bethke (and many others); all of whom were informed by theoretical and practical developments in science and technology. These narratives subsequently helped to define the field of hacking and became a moral rallying point for the early computer hackers.

The term hacker was originally associated with broad set of moral principles as expressed in, for example, the 'Hacker's Manifesto' (Blankenship, 1986, and see also Wark, 2004). Paraphrasing Blankenship, he conceived of the hacker as a self-defined determined and curious individual who explores the new electronic world seeking knowledge that has hither to been restricted from public circulation. "You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity." (Blankenship, 1986).

Wark (2004) expands upon Blankenship's holistic notion of the hacker and hacking, however hacking and hackers have since become almost exclusively associated with computer misuse offending by those who commit "cybercrimes against the machine," as opposed to cybercrimes that use the machine (such as frauds) or cybercrimes in the machine (content crimes) (see Wall, 2008, 2024). Attempts during the early days of the internet to use the term 'cracking' to differentiate ethical from unethical hackers were abandoned because of the term's pejorative racial connotations in the US. So, like the term cybercrime, 'hacking' and 'hackers' are contentious, but have become firmly embedded in everyday language and therefore need to be unpacked to allow them to be understood (Wall, 2024). Not least because the concepts alone say very little about the actions or motivations of the hackers or their direction of travel, for example, whether they seek to improve security or commit crime. Even some users of social media apps who deliberately break the platform rule now present themselves as hackers, which indicate how the label has, in the spirit of its cyberpunk origins, become a rallying point for those wishing to use unorthodox applications of technology to achieve their goals (Sampson, 2005). The outcome is that the modern usage of the terms, which links hacking with criminality tends to obscure both its rather principled past and its professionalized future, for example, in Pentesting (Penetration Testing),

which seeks to firmly distance itself from hackers. The modern colloquial usage, also confuses, for example, the actions of hackers who are mainly involved with breaking into systems with the actions of, say, fraudsters who use the machine to defraud their victims.

Describing the actions of hackers

For many years hackers were lauded by media as a celebration of youth genius and the pioneering spirit of America, but they have subsequently become demonized (see Chandler, 1996: 229; Duff and Gardiner, 1996; Ross, 1990: para. 4; Sterling, 1994; Taylor, 1999; Wall, 2008, 2012, and 2024; Steinmetz, 2016). Today, attempts by commentators are often made to distinguish between 'white hat hackers' who celebrate the original ethical hacking traditions and 'black hat hackers' who are driven by more unethical and even criminal, motivations (see later). The problem is that while both descriptions appear obvious, they are hard to apply in practice and formal attempts to 'color code' hackers by their activities are even harder to apply in practice. Moreover, although there remains some regard for the public service/civil liberties ethics of the ethical hacker, their skills and beliefs have arguably become co-mingled with those of the unethical hacker, and both are now largely distrusted and regarded as a threat to the point that their activities are outlawed by most computer misuse laws. As indicated earlier, the terms hacker and hacking still say little about the direction of travel of the hackers' activities. It is therefore necessary to identify in further detail the different actions that fall under the terms.

Ethical hackers, as indicated earlier, possess a high level of ethical standards which they express through specialized knowledge combined with a belief in the ethics of freedom of access to public information. From the early days of communication technologies hackers played a crucial role in the development of the internet. They tested systems and forced code writers to achieve higher standards of quality, while also lending their skills and imagination to shape the internet. Today, the ethical hacker's role is mainly to find vulnerabilities within systems and networks which could be exploited by criminals and therefore strengthen their security. Through brute force, or Black-Box, testing they work with IT departments to identify weaknesses in system and then them to help develop policies and procedures that make them safe to operate. As such, ethical hackers have become a significant part of the cybersecurity industry, which has emerged to protect systems and are distancing themselves from unethical hackers by professionalizing their role.

Unethical hackers, in contrast to their more ethical contemporaries, maliciously and illegally search for vulnerabilities within systems which they exploit for their own gain. They are driven by a range of motivations ranging from economic or political gain, excitement, seeking revenge, or simply to show their peers how skilled they are. The main distinction between ethical and unethical hackers, however, is that the latter are prepared to break the law to achieve their goals, whereas the former are not.

Grey hat hackers are groups who occupy the middle ground or grey area between the ethical and unethical positions. They vary in terms of balance of legality/illegality of their actions and also the level of maliciousness and harm they inflict and upon whom. Although, as stated earlier, attempts to color-code hackers largely fail, these grey hat hackers are different to the above. They may, for example, use illegal methods to find vulnerabilities which they then legally sell to companies offering a 'bug bounty' for knowledge about its own or competitors' security weaknesses, or they may be tempted to illegally sell this knowledge to the highest bidder. Alternatively, they may either undertake online vigilantism (digilantism; see Digilantism by Trottier) to inflict revenge on individuals or organizations who they feel offend their values or undertake various forms of political actions (called hacktivism). These actions may be carried out as part of an online moral grouping or even directly on behalf of governments. Although in such actions they often occupy the moral high ground to justify their actions, they often seem unclear as to what represents good or bad behavior or even if they have exceeded the limits of the law.

The tactics employed by hackers to breach systems and networks

Gaining access. Hackers can gain access to systems and networks by using their programming skills and knowledge of the organization of networks. Very often ethical hackers (such as penetration testers) are invited by an organization to seek weaknesses in their own systems. Prior to beginning work, the professionals will establish their legitimate rights to access the system to avoid prosecution. Unethical hackers, in contrast, can also gain access to systems and networks by scientific means, traditionally by using their expert programming skills and knowledge of the way that networks are organized. But unethical hackers are increasingly becoming less reliant upon their personal programming skills because these have been replaced by coded routines or apps and are now being sold online on fee for a service basis. This practice of buying in cybercrime services has created a cybercrime ecosystem that facilitates different types of cybercrime. This not only helps hackers scale up their levels of attack and add a layer of obscurity to evade the gaze of law enforcement, but also allows them to focus their efforts upon the bigger cybercrime picture (Wall, 2021, 2024).

A popular method to gain unauthorized scientific access to systems (using technological methods rather than social engineering) has been, and still is, by brute force. A brute force attack is where intruders probe systems for access by entering electronically created combinations of numbers and letters which eventually form the correct access credentials. This method, however, is probably more seen in popular media representations than in practice because, on the one hand, the amount of mathematical computing needed to identify the access credentials is considerable. On the other hand, the easy availability of stolen databases containing users' default usernames

and passwords are conveniently available for purchase online for prices that reflect the quality of the data. Furthermore, entry to systems can also obtained by utilizing zero-day exploits, which are weaknesses in computing systems, mostly unpatched vulnerabilities, that are unknown to the owners or operators, and which can be exploited by offenders to attack the systems.

Another method of gaining system access credentials is to launch a man-in-the-middle (or browser-in-the-middle) attack which involves the attacker positioning a replica login page between the user and the service they are trying to access to intercept communications. Whilst the victims believe that they are communicating directly with the service provider, they are also providing their login credentials and other personal information to the hacker. This information can be sold on and used to steal money, spy on victims, sabotage their communications, or corrupt their data (see Swinhoe, 2022). Alternatively, the attacker can alter the information given to the user by the service or upload malicious code if their device is attached.

Often the objective of the cybercrime is not to gain access to systems, but to prevent others from doing so and a popular method of achieving this is to mount a Distributed denial of service attack (DDoS). DDoS attacks prevent legitimate users from gaining access to their networks and systems by bombarding their access gateways with a stream of data to overload the login capacity. DDoS is used to discomfort or distract victims whilst other actions take place, such as data theft, or installing ransomware. Ransomware attacks, like DDoS attacks, also prevent customers or clients from accessing services by encrypting business systems and stealing their essential data to prevent them from operating. Once the business victim has met the attacker's ransom demand a decryption code is provided to unlock the computer. Hackers wishing to mount browser-in-the-middle, DDoS, or Ransomware attacks can buy the services from specialist providers (also a different type of hacker, see Wall, 2021, 2024) who sell their services[1] on markets located on the deep or darkweb (the ToR router—The Onion Router) which is an area of the internet that is not searchable by conventional search engines (see Darknet by Tzanetakis).

There are also a number of alternative means by which to gain illegal access to systems that rely on more 'social' than scientific means in which the hackers focus their attentions on tricking the individual user to give them access to the system rather than using technological methods. Social engineering has long been a practical method of grooming and obtaining trust from individuals or members of organizations enough to get them to give out system information and even access credentials. Within organizations are a number of groups of workers who may be vulnerable to social engineering approaches. They are usually the lower paid and less valued in the hierarchy and who may have little emotional investment in their job and the organization they work in, yet they have access credentials. There is also a different practice of targeting more

1 Please note that these 'services' also constitute a range of cybercrimes, such as gaining access to systems and others not covered here.

senior officers of organizations to get them to grant access rights. Disgruntled insiders, for example, may abuse their legitimate system access rights to obtain information or access credentials and send them electronically outside the organizational boundaries. Alternatively, insiders may intentionally or unintentionally (through being tricked by social engineering) install spyware or back doors into a system to allow others to enter. Finally, a much less dramatic and not always illegal method is to collate the open-source data (OSINT) emitted by organizations online and their websites to create potential victims' profiles (see Wall, 2024: 73–75).

Learning and reproducing hacking skills

Participation in chat groups or forums is important in the transmission of hacking skills as they enable more experienced hackers to pass down their wisdom and experience to new members of the group. The more junior and inexperienced hackers, often called 'Script Kiddies,' 'newbies,' 'wannabes,' or 'lamers' are curious and are eager to learn hacking skills. Typically, they have low levels of competency and frequently solicit help from experienced hackers who participate in specialist chat forums. They are schooled by expert members, such as, 'Gurus' who impart their considerable knowledge and experience or 'Wizards' who have deep expert knowledge on specific areas, or 'Samurai' who have experience in carrying out practical hacking tasks:

> 'Script kiddies' tend to be inexperienced and unskilled hackers who try to infiltrate or disrupt systems by running pre-made tools. They 'vandalize websites both for the thrill of it and to increase their reputation among their peers' (Mead et al., 2005).

Lemos has referred to them as 'ankle-biters' (2000). Although denigrated for their lack of IT skills, they can nevertheless cause significant disruption to their victims' computing systems and networks. Such forum participation can also contribute to, what has been termed, the 'digital drift', from thoughts into actions and minor actions into more serious offending (see further Goldsmith and Brewer, 2015; Goldsmith and Wall, 2022).

Motivations and attractions for offending

In the 21st century, the common understanding of hacking appears to have shifted from its moral and idealistic origins towards the actions of hackers' intent upon criminal gain, especially since the emergence of the cybercrime ecosystem of skilled hacking specialist activities which facilitate modern cybercrimes. However, there is also an underlying assumption that hacking is purely for economic gain, when in fact there are a number of other motivations that can either standalone or combine to drive cyber-

crime. The need to achieve commercial advantage over competitors can be a commercial driver, as can revenge for a misdemeanor by a second party. Individual hackers may be motivated by the self-satisfaction gained from achieving a goal, or the need to obtain for peer respect for their work, or to get 'Sneaky Thrills' from the activity (Katz, 1988). Alternatively, the driver could be simply to impress potential employers and a number of hackers have written viruses that contained in the source code their employment CV. This reveals a contradiction in hacking today based upon the fact that hackers are attracted by the anonymity of the internet and the fact that hackers can distance themselves from victims, and yet they want to be known for their actions and be respected for them. This segues into politically motivated cyber-conflict and espionage hackers. Whereas hackers have traditionally wanted to be noticed for their skills, even if they did not wish to be caught, cyber-spies, who seek to conduct political or industrial espionage, in contrast do not. Their goals are to enter and exit sites discreetly, avoiding detection in order to obtain restricted information such as government or trade secrets, which might, for example, enable the possessor to gain a marketplace, or political, advantage over their competitors.

During the past decade cyber-conflict has brought a sharp realism to early apocalyptic predictions that the internet would become a hot bed of espionage and terror. Conflict has attracted hackers, and the overall number of active cyber-conflict groups has increased in as various conflicts have emerged, for example, since Russia's 'special operation' in Ukraine in 2014 and 2022 and then the Israel and Gaza conflict in 2023. The groups allied to each side in conflict comprise of sympathetic non-nation-state and nation-state actors, indicating some significant state involvement in government promoted cyber activities (Wall, 2024). These groups are very fluid and ephemeral, regularly breaking up and reforming because of internal disagreements, counter actions, deliberately evading the gaze of law enforcement. Importantly, some non-nation state (mainly criminal offenders), openly draw some credibility from geo-political affiliation in order to hide their criminality, especially economic crime. At the same time nation-state actors also exploit the economic criminals to hide their own strategic goals, not least the damage caused to the 'enemy' by cyber-campaigns and the intelligence obtained from any stolen data (see further, Wall, 2024: 69).

Four main groupings of cyber-spies exist: 'cyber-warriors' who are specialized black hat hackers acting like 'guns for hire' and selling their skills to the highest bidder; industrial spies, who focus upon enterprises and are money-driven and who infiltrate organizations and exfiltrate data; government agents, who are highly trained, skilled and seek to achieve political goals; military hackers who seek to achieve military goals.

Conclusions

Although the 'hacking' and 'hackers' were born out of moral values that emphasized curiosity, freedom of information, and curiosity for knowledge, the common understanding of the terms is now synonymous with illicit or illegal cyber-dependent activ-

ities that attack security or control systems. Not only has their meaning adapted to social and technological change over the years, but so has the variation of the actions and tactics that carry the hacking label. The latter is continuing to change via the emergence of a cybercrime service ecosystem that allows hackers to access specialist skills for a fee for which they get in return an increase in efficiency and scalability and a level of deniability to evade law enforcement. The skills-base of hacking has arguably become more complex and sophisticated as hacking skillsets have become specialized in the facilitating cybercrime ecosystem, mentioned earlier. This will arguably develop further as hackers increasingly employ generative artificial intelligence to improve the quality of their service delivery. The organization of modern cybercrime, then, reflects a business studies manual than the organized crime playbook.

Yet, the motivations for hacking and becoming a hacker have not changed and are unlikely to do so. Hackers, since the emergence of the internet, have honed their skills in chat and other online forums which also serve to reproduce and perpetuate hacking skills and maintain the hacking culture (see Accessing Online Communities by Kaufmann). This indicates that the prime motivation for hacking is not purely to commit crimes to achieve economic gain, but they vary in terms of activity, often depending upon their peer group. What is clear it that hacking has its basis in intellectual curiosity and also the pursuit of 'thrills' but can be shaped by peers into various forms of actions such as revenge, exposure (doxing), or even changing broader moral or political opinions. Finally, regardless of their legal, illicit, or illegal intentions and recalling Sampson's 1959 and 2005 commentary, hackers are characterized by their "unconventional or unorthodox application of technology." They "avoid the standard solution" and importantly, the hack itself is a function which defines the hacker.

Suggested reading

Grimes, R. (ed.) (2017). *Hacking the Hacker: Learn from the Experts Who Take Down Hackers.* New York: John Wiley & Sons, Inc.

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* New York: John Wiley and Sons.

Steinmetz, K. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime.* New York: New York University Press.

References

Blankenship, L. (aka The Mentor). (1986). The conscience of a hacker (Hacker's Manifesto). *Phrack*, 1 (7): phile 3. Available at https://en.wikisource.org/wiki/The_Hacker_Manifesto

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law*, 24, 229 – 251.

Duff, L., & Gardiner, S. (1996). Computer crime in the global village: Strategies for control and regulation – in defence of the hacker. *International Journal of the Sociology of Law*, 24, 211 – 228.

Goldsmith, A, Brewer, R (2015) Digital drift and the criminal interaction order, *Theoretical Criminology*, 19(1): 112 – 130.

Goldsmith, A. and Wall, D.S. (2022) The seductions of cybercrime: adolescence and the thrills of digital transgression, *European Journal of Criminology*, 19(1):98 – 117.

Katz, J. (1988). *The Seductions of Crime.* New York: Basic Books.

Lemos, R. (2000). Script kiddies: The Net's cybergangs. *ZDNet*, 13 July, www.zdnet.com/article/script-kiddies-the-nets-cybergangs.

Mead, N., Hough, E., & Stehney, T. (2005). *Security Quality Requirements Engineering (SQUARE) Methodology Report*, 31 October, Carnegie Mellon University.

Ross, A. (1990). Hacking away at the counterculture. *Postmodern Culture*, 1/1. http://jefferson.village.virginia.edu/pmc/issue.990/contents.990.html.

Sampson, P. (1959). *Dictionary of the TMRC language*, Tech Model Railroad Club of M.I.T. https://www.gricer.com/tmrc/dictionary1959.html

Sampson, P. (2005). *An Abridged Dictionary of the TMRC language*, Tech Model Railroad Club of M.I.T. https://www.gricer.com/tmrc/dictionary1959.html

Steinmetz, K. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime.* New York: New York University Press

Sterling, B. (1994). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* London: Penguin.

Swinhoe, D. (2022). Man-in-the-middle (MitM) attack definition and examples, CSO Online, 25 March, https://www.csoonline.com/article/566905/man-in-the-middle-attack-definition-and-examples.html

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime.* London: Routledge.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction and the production of knowledge about cybercrime. *Information Communications and Society*, 11(6), 861 – 884.

Wall, D. S. (2012). The Devil Drives a Lada: The social construction of hackers as cybercriminals. In C. Gregoriou (ed.), *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'* (pp. 4 – 18). London: Palgrave Macmillan.

Wall, D. S. (2021). The transnational cybercrime extortion landscape and the pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending, *European Law Enforcement Research Bulletin* (SCE 5), 5 October, 45 – 60.

Wall, D. S. (2024). *Cybercrime: The Transformation of Crime in the Information Age, 2nd Edition*, Cambridge: Polity.

Wark, M. (2004). *A Hacker Manifesto.* Cambridge, MA: Harvard University Press.