Book Review

Review of Maurushat, Alana. 2019. *Ethical Hacking*. Ottawa: University of Ottawa Press. 368pp. Paperback. \$39.95. ISBN: 9780776627915.

Gary Genosko

University of Ontario Institute of Technology, Canada
Gary.Genosko@uoit.ca

Ethical Hacking has the prosaic qualities of a user's manual. Pages of specific and more general definitions unfurl into a kind of running glossary. Summarizing charts abound. Big picture graphs pop up here and there. Many of the graphics are unfortunately of poor quality. The edifice rests on the author's 2011 report for Public Safety Canada. Since that time up to 2018, methodological upgrades have been made with regard to data sets of various kinds in an effort to metricize global incidences of ethical hacking, a hard to define concept.

The term ethical hacking is used by Maurushat in a broad sense to include a range of activities including hacktivism, penetration tests, vulnerability discovery, counterattacks, security activism, all undertaken by a range of different hacker types not easily contained in standard distinctions between white and black hats. Maurushat wants to drill down into individual attacks and move away from the computer science version of ethics and hacking that is restricted to white hat actions. Hence, "ethical hacking is the non-violent use of a technology in pursuit of a cause, political or otherwise, which is often legally and morally ambiguous" (22).

In order to present an up-to-date global picture of increases in incidences of ethical hacking, we are walked through three searches run through analysis services (GDELT, BigQuery and DIBB-Dark Net forums). Of interest in the open database is that the results are skewed by restrictions on journalistic freedom to report ethical hacking in the first place and by a given state's manipulation of private media through advertising investments; yet what emerged was an important ligature between patriotism and hacktivism in the case of China, where reports made it through the state censor if they were couched in anti-foreigner and nationalist rhetoric. The Google search captured huge volumes of incidences, but didn't explain much; and the Dark Net data focused on cyber-jihad and malware forums collected by the Data Infrastructure and Building Blocks consortium of American universities, showed how cyber-jihad was actually "belittled" for its non-physical nature (50) and that despite language limitations (no Arabic or Russian) in the English-language searches, and the hope that social media might be searched in the future, there is no question that incidences of ethical hacking have been "escalating" across the planet (55). The challenge is how to contextualize this trend.

Looking at the global case-law is a case in point. It is relatively sparse compared to the generic hits of analytics run on databases that pick up any mention of ethical hacking. There are reasons, Maurushat explains, for such a paucity, but the catalogue she presents is overwhelmingly American, beginning with *United States of America vs. Bradley Manning*. Each summary in this catalogue of case-law conforms to set items and notes: case name; citation; jurisdiction; main URL; charged with; legislative provisions;

main target; motivation; convicted of; sentence; additional information. A handy summary, a bluffer's guide if you like, of each case is provided, running through the global Anonymous and LulzSec prosecutions and convictions, assorted trolls, Aaron Swartz, etc. Some lesser known cases discussed include Anat Kamm's efforts to expose classified Israel Defence Forces operations in the West Bank and Andreas-Thomas Vogel's successful DDoS protest against Lufthansa's profiteering from the deportation of asylum seekers. The problem with this mode of presentation is that it is merely a reference guide, with almost no substantive social science research into the persons or groups other than basic source coordinates, often using Wikipedia articles, and in this regard it falls short of the ethnographic impulse that characterizes some of the most compelling research into hacker cultures.

The awkward conversion of quantity into quality begins with two chapters devoted to ethical-hacking incidences by Anonymous, broken down summary-style, beginning with examples from 2010 operations up to 2015, and to various global incidences performed by many individuals and groups. This rather skeletal approach may be a useful reminder, perhaps, of the range of attacks, explanations, and consequences, but it is interpretively flat. Without belaboring the obvious, these docs would be more accessible if scrollable. However, they serve as lightly processed material for the construction of select timelines for case studies devoted to ethical quandaries arising from online civil disobedience.

The discussion of the hacktivist-online civil disobedience distinction, with nods to off-line actions, centres on the wide range of DDoS attacks, in addition to the "questionable legality" of stress test services and attack mitigating shields. The analysis of Anonymous' Titstorm Operation against Australian government servers, with the popular free software LOIC figuring heavily in the charge, conviction, and fine of Matthew George, is under-researched and out-of-date. The next case studies of the successful protest against Lufthansa's profiting from deporting illegal immigrants (94) and the Canadian #TellVicEverything Twitter campaign aimed at Conservative politician Vic Toews, are quite short. Just as the analysis reaches a stimulating point of how big data may be used by governments and corporations to predict which events will likely attract activist responses, it goes quiescent. The mode of pre-emption has been widely theorized and plays an important role in surveillance studies.

The next set of timelines are more elaborate and follow Anonymous and Chaos Computer Club operations, with other mixed examples. The emphasis is on high-skill tech development as online civil disobedience moves into hacking for a cause. Beginning with the Post-Christmas Charity Donations by Anonymous, involuntarily offered by Stratfor clients on their hacked credit cards to mainstream charities, with a brief stop on the attack on a Finnish neo-Nazi website, and finally to LulzSec's Operation Payback, a DDoS against MasterCard and PayPal in support of WikiLeaks. What we end up with, however, as the attack-counter-attacks scenarios play themselves out is Jeremy Hamond's justification for his actions in the effort to "unmask unlawful surveillance and intelligence-gathering efforts" (218). This appears to serve as an exemplar of how prosecution does not serve as a deterrent. No philosophical reflection on ethical hacking is undertaken, as the author is content to have recourse to a critical mass as a measure of ethicality: "the stronger the cause, the more likely hacktivist activity will be seen as ethical" (219).

A further timeline is constructed with regard to security testing undertaken on behalf of or with the permission of an owner's system in some form of penetration testing. The competitive culture of bug bounty hunting, leading to the direct sale of the discovered vulnerability, or the use of an intermediary broker, engages with a number of curious case studies. Security researchers are wary that lawsuits may arise due to copyright infringement (Michael Lynn's 2005 Cisco router vulnerability disclosure), but in some instances like Glenn Mangham's downloading of Facebook's source code, the ethical character consists in the refusal to broker the find or to anonymize the researcher's identity (232). Ethical considerations arise here on the basis of a commitment to ensuring that vulnerabilities are eventually addressed, come Hell *and* highwater!

A short chapter on "hackback" or self-help counter-attacks designed to mitigate damages notes the controversial nature of the practice by corporations and that it is largely unlawful. Some movement toward

its restricted legalization in the US is broached. “Active defence” (245) remains a troubling prospect and a number of reasons why are given.

The so-called “curious beast” (253) of security activism follows. It dovetails with hackback since what is at stake is the inconsistent understanding of unauthorized access against committed ethical hacking as a vocation driven by the desire to expose security flaws. Here there is a fine-toothed analysis of the delicate matter of access by researchers and hackers working in the public interest by taking down botnets, cleaning up infected computers, often with inter-institutional cooperation and the blind eye of law enforcement. Neither zeal for research nor public service exempt one from prosecution, however. Maurushat makes the case for a reconsideration of unauthorized access and argues convincingly for exemptions from criminal prosecution for security activists.

Canada is signatory to the EU Convention on Cybercrime and as a result criminalizes a wide range of offences against confidential materials, interference with, and misuses of devices. Along with the procedural issues and international cooperation mandates, this agreement makes any form of unauthorized access, and hence ethical hacking, by definition illegal. One exemption is around copyright (266). But making a copy for encryption research requires authorized access, otherwise it is not exempt under the criminal code. All sorts of issues bedevil investigation: attributions problems, traceback minefields, jurisdictional fuzziness, sentencing quirks, evidence fragility, and finally damages. A bit more in and around such statements as “the amount is often pure conjecture” (274) would have been helpful as the posting of big numbers is rhetorically effective and influential in prosecutions yet completely suspect.

One of the most original contributions in *Ethical Hacking* is a section cowritten with Hannah Rappaport on the prevalence of autism within a largely young male hacker culture (274). Although this subject is understudied, it certainly deserves more scrutiny, and it seems more promising than the addictions approach. The manner in which it is handled in this book raises some questions about why the exploitation of autistic talent by military forces and corporations is accepted uncritically. At the same time, this forms part of the inherent messiness of ethical hacking. Yet one would like to see a broader context for the discussion of the many intersections of disability and hacking here, and a more generous use of historical examples beginning with phone phreaking and bringing the area up to date through shifts in the neurodevelopmental literature, not to mention the prevalence of hacking as an epistemological metaphor in descriptions of autistic difference.

Ethical Hacking concludes with several recommendations. Working from an offline-online comparative framework, Maurushat stakes her claims on the establishment of legal and legitimate virtual protest spaces; advancing definitions of acceptable and lawful methods of hacking and making these public; establishing a code of conduct for hackback; creating exemptions for research and public interest hacks. Indeed, perhaps the simplest is left for last: introducing into existing cybercrime conventions regarding computer offenses a misdemeanour—minor, non-indictable, offense—where no equivalents currently exist, despite the incredible difficulty of adapting this to different domestic legal regimes.