Canadian Journal of Law and Technology

Volume 17 | Number 2 Article 7

12-1-2019

Ethical Hacking by Alana Maurushat

Laura Ellyson
PhD Candidate, Schulich School of Law, Dalhousie University

Recommended Citation
Laura Ellyson, "Ethical Hacking by Alana Maurushat" (2019) 17:2 CJLT 335.

Book Review

Ethical Hacking
by Alana Maurushat
(Ottawa: University of Ottawa Press, 2019)

by Laura Ellyson[*]

Most books about hacking are geared towards IT specialists and cyber-security experts. In *Ethical Hacking*,[1] Alana Maurushat changes the genre and aims to reach a broader public, one composed not only of computer geeks, but also of jurists, scholars, policy-makers, and any other individual with a curiosity for the subject, who do not necessarily have the technical skills to pursue such activity themselves. Maurushat has impressive credentials when it comes to cyber security, including working at *Data to Decisions Cooperative Research Centre*, which specializes in big data and artificial intelligence for national security purposes, and being on the board of directors at IFW Global, an investigation firm, which has led her to cooperate with the FBI, the CIA, Interpol, and other law enforcement agencies.[2] Her wide experience in this area — including defining herself as an ethical hacker — not only makes her a leading expert on ethical hacking, but also provides a unique perspective on the subject.

But what is ethical hacking? Maurushat defines it as "the non-violent use of technology in pursuit of a cause, political or otherwise, which is often legally and morally ambiguous."[3] As Maurushat admits herself, this definition is larger than the one usually used in computer sciences, where the term "ethical hacking" usually refers only to penetration or intrusion testing.[4] She includes in her definition five types of behaviours: online civil disobedience, hacktivism, penetration/intrusion testing and vulnerability discovery, counterattack/hackback, and security activism. Ethical hacktivism can include a vast array of online behaviours, ranging from testing the security of a website on behalf of its owner, to unauthorized access to data in pursuit of a political cause. A good example of ethical hacking is when hackers attacked smart toys in 2015 (i.e. toys for children that utilize wireless technologies) to expose security vulnerabilities, not for potential ransom profit or to gain information.[5]

[*] LL.M., Université de Montréal; LL.B., Université de Sherbrooke; PhD candidate, Schulich School of Law, Dalhousie University; Lecturer, Polytechnique Montréal.

[1] Alana Maurushat, *Ethical Hacking* (Ottawa: University of Ottawa Press, 2019).

[2] *Ibid* at 4-5.

[3] *Ibid* at 7.

[4] See *ibid* at 21; Ronald I. Raether Jr., "Data Security and Ethical Hacking" (2008) 18:1 Bus L. Today 55; David M. Hafele, "Three Different Shades of Ethical Hacking: Black, White and Gray" Sans Institute (Feb. 23, 2004), online: < www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390 > .

[5] See Corinne Moini, "Mandated Ethical Hacking — A Repackaged Solution" (2017) 23:3 Rich. J.L. & Tech. 1.

Ethical Hacking's broad audience, of course, calls for a crash course in technological terms and concepts (chapter II), which Maurushat does simply enough for the readers with less technical knowledge to understand her arguments, without falling into overgeneralizations or oversimplifications. A key feature of Maurushat's work is that she does not solely rely on qualitative analysis to draw her conclusions, but also on quantitative work. The methodology used and the results it prompted (chapter III) — which includes work done in 2010 for Public Safety Canada but also more recent research done by Maurushat and her team — support an overview of the phenomenon of ethical hacking globally and sets out the raw material for further qualitative analysis found in the book. However, given that Maurushat herself acknowledges that some of the methodology used is not ideal, the actual validity of the results is open for discussion. Nonetheless, the quantitative work generally proves that ethical hacking is not a rare online behaviour limited to some countries.

While ethical hacking is not new, legal cases on the subject are rare. Even so, Maurushat catalogues case law from all Commonwealth countries and provides summaries for every case (chapter IV). Other incidences of ethical hacking which are not necessarily linked to a legal case are also examined in relation to major ethical-hacking groups, including *Anonymous* (chapter V), *Chaos Computer Club*, *CyberBerkut*, *LulzSec*, and others (chapter VI). Maurushat then addresses in more detail the five types of behaviours that she defines as ethical hacking (chapters VII to XII). This is probably where Maurushat gives her readers the clearest idea of what these different behaviours can look like concretely and how certain actions that qualify as ethical hacking are legal, while others are not.

From a policy perspective, the last two chapters of *Ethical Hacking* are probably the most interesting. By comparing ethical hacking with other types of dissent or protest, Maurushat pleads for a public interest and security research exception to be included in cybercrime and computer-crime provisions (chapter XIII). Indeed, this is where Maurushat's book is most interesting from a penal-policy perspective and provides real innovative insight on the subject.[6] She claims that the *Canadian Charter of Rights and Freedoms* should provide protection for online civil disobedience participants, mainly under freedom of expression. She also provides some recommendations that could be explored further in order to address the problem of ethical hacking (chapter XIV). These are (1) encouraging legitimate space for virtual protests; (2) creating governmental guidelines and policies; (3) creating a code of conduct for hackback and a white paper on hacktivism; (4) requesting more transparency from governments that engage in hackback; and, as mentioned (5) creating a security research exemption and public-interest consideration.[7]

[6] Similar arguments were made by Tiffany Marie Knapp in 2015. However, Maurushat does not refer to this work, which is surprising considering the resemblance in their respective arguments. See Tiffany Marie Knapp, "Hacktivism — Political Dissent in the Final Frontier" (2015) 49:2 New. Eng. L. Rev. 259.

While *Ethical Hacking* is a valuable tool for anyone interested in this phenomenon, some more negative aspects of the book also need to be mentioned. First, there are a few layout mistakes, such as unreadable figures (which Maurushat acknowledges and explains by mentioning that the book was conceived with web viewing in mind) and page headers that refer to the wrong chapter. Second, the book can sometimes be redundant, especially in the first few chapters where sections are plainly repeated. Finally, by catering to such a large audience, some interesting or important concepts are under-theorized. Most notably from a legal perspective, Maurushat's analysis would have benefited from a more in-depth approach, where her most interesting ideas could have been explained fully and put to the test in contrast with an opposed point of view. Furthermore, some additional details would have been useful on certain topics; for example, Maurushat does not mention that Canada only ratified the *Convention on Cybercrime* in 2015, when it adopted the *Protecting Canadians from Online Crime Act*.[8]

In short, Maurushat's book is definitely a manifesto in favour of ethical hacking, under certain conditions and circumstances. Maurushat's experience and the quality of her research definitely create a compelling and well thought out study of this phenomenon, in a global perspective. For this reason, the book seems like an essential read for anyone interested in the subject and living in a Commonwealth country, as long as the reader keeps in mind that it is a general book, aimed to a broad audience. While a more thorough analysis would have strengthened the final chapters, *Ethical Hacking* does deliver on what it sets out to do, which is to explore the issue of ethical hacking through the specific lenses of Maurushat's significant personal experience.

[7] This suggestion is not new. For example, Jim Kerstetter suggested in 1998 that copyright law should be amended to allow ethical hacking for research purposes. See Marcus Maher, "Open Source Software: The Success of an Alternative Intellectual Property Incentive Paradigm" (2000) 10:3 Fordham I.P. Media & Ent. L.J. 619 at 688.

[8] *Protecting Canadians from Online Crime Act*, S.C. 2014, c. 31.