CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi - 110025, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107043466
DOI:10.1017/9781107338548

First published 2019

Printed and bound in Great Britain by Clays Ltd, Elcograf S.p.A.

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication data
Names: Joseph, Anthony D., author. | Nelson, Blaine, author. | Rubinstein, Benjamin I. P., author. |
Tygar, J. D., author.
Title: Adversarial machine learning / Anthony D. Joseph, University of California, Berkeley, Blaine Nelson,
Google, Benjamin I.P. Rubinstein, University of Melbourne, J.D. Tygar, University of California, Berkeley.
Description: Cambridge, United Kingdom ; New York, NY : Cambridge University Press, 2019. |
Includes bibliographical references and index.
Identifiers: LCCN 2017026016 | ISBN 9781107043466 (hardback)
Subjects: LCSH: Machine learning. | Computer security. | BISAC: COMPUTERS / Security / General.
Classification: LCC Q325.5 .J69 2017 | DDC 006.3/1 – dc23
LC record available at https://lccn.loc.gov/2017026016

ISBN 978-1-107-04346-6 Hardback