Preface

It is becoming increasingly clear that cybersecurity will become one of the dominant security risks of the twenty-first century. It would not be an overstatement to say that virtually every person in the world who has access to any kind of computing device will be at risk and will likely experience adverse cyber-events. With the ubiquity of mobile phones around the world, as well as the expected explosion of computing capabilities through the advent of the "Internet of Things," we expect cyber-risk to grow as hackers find ever more creative ways to wreak havoc in the lives of unsuspecting users.

This book is about *risk*. Despite the heavy investment in cybersecurity by countries around the world, few of these countries have solid quantitative data assessing their risk and relating it to the general risk profile around the world. For instance, the deputy director general of an EU nation's intelligence agency recently attended a talk by the first author and remarked afterward that he did not have access to the type of data that we had when writing this book.

Our goal in writing this book was to take the first steps to quantify the risk to different countries via some simple, easy to understand, data-driven metrics. Thanks to Symantec's Worldwide Intelligence Network Environment (WINE), we had access to an amazing dataset that included over 20 billion telemetry records (both binary reputation and malware reports) from over four million hosts per year over a 2-year period. Symantec collected this dataset from users who had "opted in" to this collection using their antivirus products such as Norton Antivirus. We note that the data analyzed in this book is available for follow-up research as the reference dataset WINE-2013-001.

We note that this book represents just an *initial step* toward quantifying cyber-vulnerability of nations. We only studied Windows hosts and consumer machines. Some countries may have advanced military capabilities and/or have robust businesses that are less at risk than the ordinary consumers located in those countries. Moreover, no mobile hosts were studied—a flaw that we hope to correct in coming years. Last but not least, we note that all monitored hosts had Symantec antivirus products such as Norton Antivirus running on them. Attacks on these hosts were detected and blocked by Symantec's antivirus products. It is possible that other

hosts in the countries we studied that did not have an antivirus product running on them had a different cybersecurity profile. To guard against this, we only studied countries with at least 500 hosts reporting per year, so that the sample size was large enough. In fact, for most countries, we had well over 1000 hosts reporting—and our 2011 dataset had over 1000 hosts monitored in each of the 44 countries we studied. We believe the results of our study will provide important quantitative, data-driven insights to policy makers in at least these 44 countries.

We conclude with a note of thanks to all of those who helped us in our research. The research in Chap. 4 was funded in part by Cliff Wang and the Army Research Office under ARO Grant Number W911NF1410358, by Sukarno Mertoguno of the Office of Naval Research under ONR Grant Number N00014-15-1-2007, and the Maryland Procurement Office under contract number H98230-14-C-0137.

A big vote of thanks is due to Matt Elder of Symantec Corporation who spent an extensive amount of time reviewing the content of this book and providing valuable feedback. Without Matt's patient explanation of some of the Symantec WINE data and his hard work, this book would not have been possible.

At the University of Maryland, we would like to thank PhD student Noseong Park for helping in producing some of the figures and Barbara Lewis for helping in formatting this document. Aaron Mannes proofread the document diligently. At Virginia Tech., we would like to thank MS student Benjamin Wang for helping in some of the research presented in Chap. 4. At Springer, we would like to thank Susan Lagerstrom-Fife and Jennifer Malat for their kind support.

College Park, MD — V.S. Subrahmanian
College Park, MD — Michael Ovelgönne
College Park, MD — Tudor Dumitras
Blacksburg, VA — B. Aditya Prakash
August 30, 2015

http://www.springer.com/978-3-319-25758-7

The Global Cyber-Vulnerability Report

Subrahmanian, V.S.; Ovelgonne, M.; Dumitras, T.; Prakash, B.A.

2015, XII, 296 p. 399 illus., 398 illus. in color.,
Hardcover
ISBN: 978-3-319-25758-7