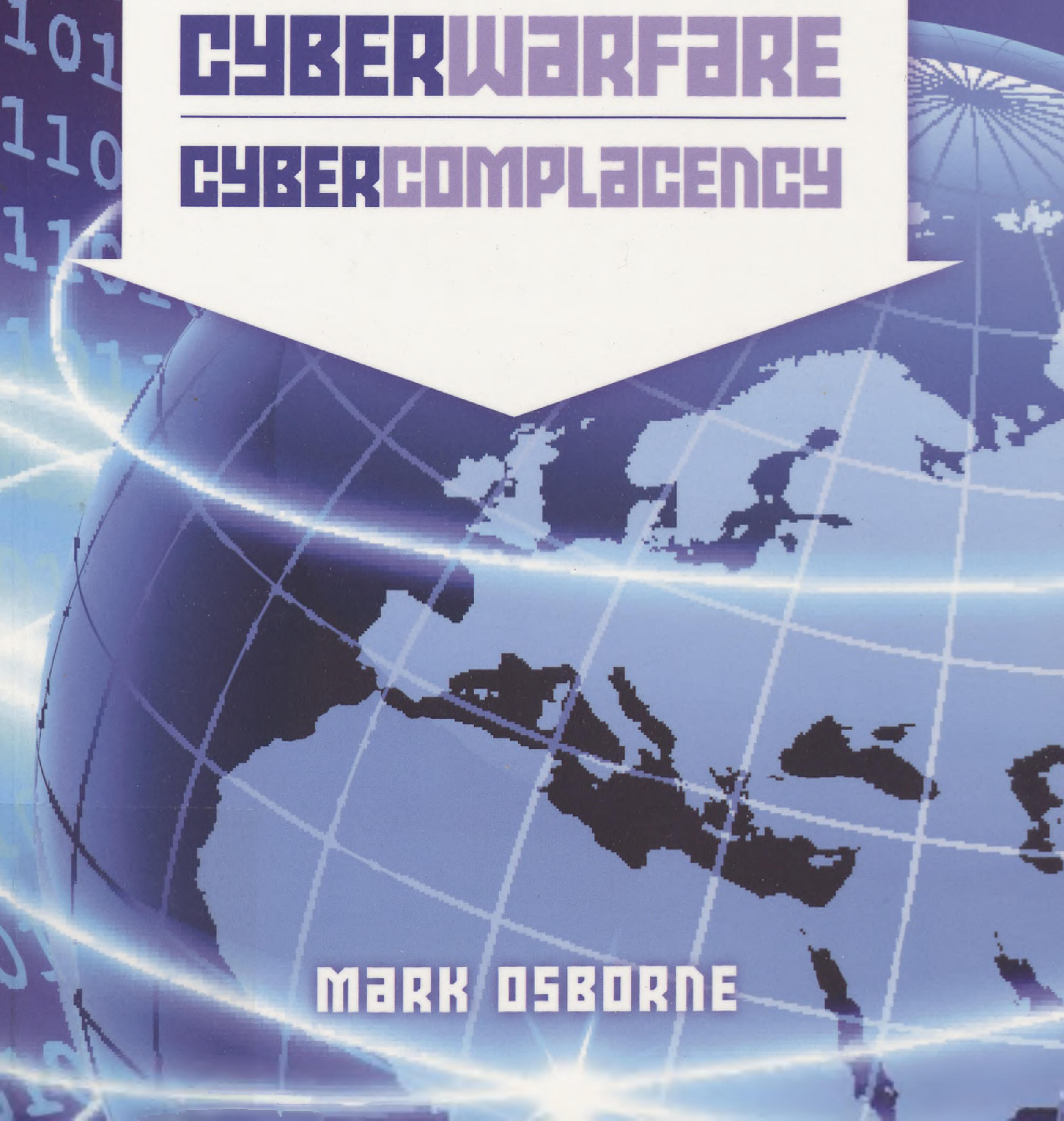
CYBERATTACK CYBERCRIME CYBERWARFARE

CYBERCOMPLACENCY



MARK OSBORNE

CYBERATTACK
CYBERCRIME
CYBERWARFARE

CYBERCOMPLACENCY

IS HOLLYWOOD'S BLUEPRINT FOR CHAOS COMING TRUE

MARK OSBORNE

ISBN: 1493581287
ISBN 13: 978-1493581283

Library of Congress Control Number: 2013920296
CreateSpace Independent Publishing Platform
North Charleston, South Carolina

PREFACE

Blanche DuBois:

"I have always depended on the kindness of strangers."

Streetcar Named Desire (1947)

Like the quote above—stranger, please be kind!!! Time (contrary to the song) wasn't on my side when I wrote this book. I tried hard to maintain a jovial style to help you enjoy it, but this could be my epitaph, my legacy, if you will. I couldn't afford to linger on every page because I was actually concerned that I might snuff-it and depart this mortal coil.

So here's the deal: just less than two years ago, I was the loud, fat, and obnoxious, yet usually right, security bloke that many of you in the UK security industry are probably familiar with. Despite the best available medical indifference (you have to make a joke, don't you!), I went into septic shock and had a twenty-by-twenty-inch alien mass, along with a two foot section of my gut and a lump of my spleen, removed. To save anyone any trouble or inconvenience, I slipped into a *coma.* It kept me nice and quiet.

And here's the clincher!! The excellent chief surgeon and other wonderful lung specialist that saved me say that most of my bits and pieces are fixed, but with the caveat that I am only here out of an act of sheer bloody-mindedness. The episode has reduced my MTTF ("Mean-Time To Failure"). Judging by the pain and the screaming headache I get at the end of each working day, I tend to agree with them (but hey, dear reader, I bet that many of you have jobs that do the same thing to you despite your good health). However, my General Practioner (GP) sniffs and says I'm all fixed—but bear in mind that this is the same guy that missed all the symptoms in the first place. This presents a dilemma but all things considered I think you'll understand why I "felt pressed" to finish the book.

Please be kind!! With my other whitepapers, books, exploits, and software I have noticed a trend. There are always comments on newsgroups or forums that say that:

- "They" could solve a 10GB/s SynFlood by using a laptop with a 486 cpu, 100Mb Ethernet card, and the netstat command
- "They" could have discovered the *zero-day* themselves if only they had looked
- "They" could have produced a much better IDS than me—if they only had the time, could write C, knew about device drivers, and had a computer ("Oh, by the way, before I start, can you remind me what an IDS does?")

"Woulda! Coulda! Shoulda!" or as my granny used to say, "If *'ifs and ands' were* 'pots *and pans,' there'd be no work for tinkers' hands.*"

So if you are that guy, *be* kind. If you notice a mistake, email me, and if you don't like it, let's keep it a secret—it can be our own zero-day, our own special thing. Please don't share it with the world. If you feel so negatively about my book, maybe you should just write a better one.

Having said that, if you love this book then tell everyone, write great reviews, and buy ten copies of it. Marge, the kids and the charities that will benefit from sales will appreciate it. That being said, nobody writes a security book or publishes open-source security tools for the money—I do it because it entrances me; I am bewitched.

So what's the book about, you ask? Please consider for a moment this statement made by J. Saiteerdou, Head of Computer Crimes at the FBI: "Give me ten carefully chosen hackers, and within ninety days I would then be able to have this nation lay down its arms and surrender."

At first glance, that about sums up the book—or at least my intent when I started it. A while ago, I realised that a *digital attack* could easily cripple a country like the UK, especially if the attackers have the resources of a sovereign power supporting them. If they don't have such resources, a blended attack which combined digital attacks with physical attacks could still be as effective. There seems to be so little public awareness about how real this possibility is and how it could come about, I felt the need to communicate what information I have gathered on this subject.

This isn't a "how-to" book and is rather designed to provide business insights into the field of digital security for the more technical people. It also provides concrete and easy-to-follow technical examples for business people who may be unfamiliar with all the technical references.

New Media

Modern media is ubiquitous and all-encompassing, spread over a wide variety of digital channels. I have tried to embrace this, as it is in-keeping with the theme of the book. I have provided:

- example code and exploits on *packetstorm (dns_spquery.c & obeseus.c)*
- example and supporting Android Apps on Google *Play*
- code and "config" files on my usual site www.loud-fat-bloke.co.uk
- presentations and lectures on *FaceBook*

I have already presented some of these at public events; if you get a chance to come and see me, you are more than welcome – Likewise, if you are hosting an event. I am much better live (over 18s only).

Much Thanks

Lastly, thanks to...well...everybody who helped.

And as a postscript, thanks to the ever-so-nice editor bloke, Dave, who gently helped some of it make sense and also curbed my natural laddish enthusiasms by removing the woefully inappropriate expression of my appreciation for “big guns” and “Sandra Bullock”. Like they say, you can lead a horse to water!

TABLE OF CONTENTS

CYBER ATTACK, [illegible]
CYBER WARFARE – [illegible]

Is Hollywood's blueprint [illegible] true?

Will hackers or hacktivists shut down the banks, the gas and the electricty supply—Can terrorists invade cyberspace, then use malware and BotNets to put an "out of lunch" sign on UK PLC. What are the techniques used to detect this type of attack and do those in power have a clue about the exposure.

Mark Osborne, also known as loud-fat-bloke, will explain all – After a lifetime of running the cyber security functions at the largest Security Consulting, ISPs and Technology providers, he designed Europe's largest cyber-monitoring system and has managed his way out of more than his fair share of Cyberattacks.

In this book, armed by real world experience, Osborne shows how exposed we all really are.

The Book covers:

- Economics of cyberspace and cyber-security.
- Who's monitoring cyberspace and Why.
- The monitoring techniques used and why they fail to protect the general population from Cyber- attack.
- How to detect, mitigate and measure the cost of a DDOS attack.
- The mechanics of BotNets and their C&C servers.
- How to exploit vulnerabilities in the Physical, BGP, DNS, IPV6 and SCADA components of the Internet & cyberspace.
- Finally, it describes a "Fire-sale" where all these techniques are used to turn off the gas, electric and all the lights just like in the movies.

What they say about the author:

"Osborne is one of the most charismatic and blatantly funny people you could hope to meet."
Communication News

"One for the bookshelf"
Information Security Magazine

"Mark Osborne's article was a useful resume on this important subject (internet Security)"
Buckingham palace

"An informative and often entertaining introduction to information security…
an informative and valuable read."
****(four stars) *SlashDot/ Ben Rothke*

Osborne's last book "How To Cheat at Managing Information Security" reached the Amazon.com Top-500. It has consistently appeared as 1st in category since publication.

About the Author

Mark Osborne has held Security leadership roles at KPMG, Interoute and HP/T-Systems. This gave him daily exposure to large scale cyber-attacks. He never forgot his software/security engineering background which included penetration testing, developing Zero-Day security vulnerabilities, coding exploits and creating open source mitigation tools like IDS/IPS. Most pertinently he designed and coded one of the largest Cyber Security System in the world to detect cyber-attacks.

ISBN 9781493581283

9"781493"581283"