

Cybersecurity in Context



Chris Jay Hoofnagle

MANA

Copyright © 2022 Chris Jay Hoofnagle

PUBLISHER TBD

BOOK-WEBSITE.COM

This book is set in the Legrand Orange Style by Mathias Legrand. Cover image: Evelyn De Morgan's Cassandra before the burning Troy

DRAFT June 17, 2022



Contents

Preface	i
Authors	iii
Acknowledgments	iii
Introduction	v

I What is Cybersecurity?

1 What is Cybersecurity?	1
1.1 What is the Cyber in Cybersecurity?	2
1.1.1 Cyberspace's Places and the Problem of Internet Sovereignty	5
1.2 The Traditional View: The CIA Triad	6
1.2.1 Computer Security Versus Cybersecurity	9
1.2.2 Building on the CIA Triad	12
1.2.3 Cybersecurity definitions	13
1.2.4 Cyberpower: Erasing the Civilian/Combatant Distinction	13
1.3 Assignment: Definitions	16
1.4 Should Cybersecurity Encompass Information Quality Problems?	16
1.4.1 From Information Scarcity to Glut	17
1.4.2 Psychology and the Information Domain	18
1.4.3 Influence Campaigns	19
1.4.4 Frameworks for Disinformation	20
1.4.5 The US Approach	22

1.4.6	Information Domain and Terrorism	23
1.4.7	Election Interference	24
1.4.8	Information Domain Problems and Economic Incentives	25
1.4.9	Is There Really Reason to be Concerned?	26
1.4.10	Alternatives to a Security Frame	27
1.5	International views	28
1.6	Conclusion: A Broad Approach	29
1.7	Assignment: “Cybersecurities”	30
2	Technology Basics & Attribution	31
2.1	Technology basics	31
2.1.1	Fundamentals	32
2.1.2	Reliance is a fundamental element of computing and the internet ...	35
2.1.3	Internet layers	36
2.2	Assignment: NSA’s Advice	44
2.2.1	Cybersecurity Depends on Generations of Legacy Technologies	46
2.2.2	“Controlling” the internet	52
2.2.3	Why Not Start Over?	53
2.3	Assignment: Technical Exercises	55
2.4	The People Behind the Technology	55
2.5	Assignment: Prof. Eichensehr’s Public-Private Cybersecurity	57
2.6	Assignment: Governments’ Many, Conflicting Interests	57
2.7	Attribution	57
2.7.1	Types of Attribution	61
2.7.2	Attribution Process	62
2.7.3	Don’t Be Surprised: Common Dynamics in Attribution	66
2.7.4	The Future of Attribution	70
2.8	An End to Anonymity?	71

II

Cybersecurity’s Contours

3	Economics and the Human Factor	75
3.1	Economics of cybersecurity	75
3.1.1	Asymmetry and the Attack/Defense Balance	77
3.1.2	Incentive “Tussles”	79
3.1.3	Tragedies of the Un-managed Commons	81
3.2	Assignment: The Startup Market	81
3.3	The Human Factor—The Psychology of Security	83
3.3.1	Attackers as Behavioral Economists	83
3.3.2	Institutions as Rational Choice Economists	85
3.3.3	User Sophistication	86

3.3.4	The Role of Emotion and the Body	87
3.3.5	Security as Afterthought	89
3.3.6	RCT: The User View	89
3.4	Conclusion: Getting to Security as a Primary Concern	90
3.5	Assignment: Assessing Risk	91
4	The Military & Intelligence Community	93
4.1	Why Cybersecurity is Center Stage	95
4.2	Are Cyberattacks War?	97
4.2.1	Cyber War Will Not Take Place	98
4.2.2	Cyber War is Coming	100
4.2.3	The Law of War	101
4.2.4	Cyber Realpolitik	104
4.3	Computers and the Future of Conflict	105
4.3.1	The Changing Nature of Conflict	106
4.3.2	Assignment: Cross-Domain Deterrence	112
4.4	Cybersecurity and the Intelligence Community	113
4.4.1	The Intelligence Community	115
4.4.2	The Vulnerabilities Equities Process	125
4.4.3	Cyber Soldiers and/or Cyber Spies?	127
4.5	conclusion	130
5	Cybersecurity Theory	131
5.1	Deterrence Theory	131
5.1.1	Deterrence Theory Contours	132
5.1.2	Deterring with Entanglement and Norms	137
5.1.3	Cyber "Power"	138
5.1.4	The Deterrence Theory Critique	141
5.2	Security Studies: Anarchy, Security Dilemma, and Escalation	143
5.2.1	The Security Dilemma	144
5.2.2	Escalation and the Security Dilemma	145
5.2.3	Nissenbaum Revisited	148
5.2.4	The Problem of Referent Object	149
5.2.5	Nissenbaum's Alternative Vision: Cyber Attacks Are Just Crimes	149
5.2.6	A Response to Nissenbaum: Strategic Risks Do Exist	150
5.3	The Tragedy of the Cybersecurity Commons	150
5.3.1	The Free Problem	151
5.4	The Public Health Approach	153
5.5	Gerasimov and "Hybrid War:" Information Domain Revisited	155
5.5.1	The US Reaction	156