Behold A Pale Farce

Cyberwar, Threat Inflation, & the Malware-Industrial Complex

Bill Blunden & Violet Cheung

A functioning republic requires *well informed* citizens
who exercise *sound judgment.*

Hence, this book is dedicated to:

Deborah Natsios and John Young

For showing how secrecy undermines democracy.

Noam Chomsky and Edward Herman

For their research on the propaganda model.

War is a way of shattering to pieces, or pouring into the stratosphere, or sinking in the depths of the sea, materials which might otherwise be used to make the masses too comfortable, and hence, in the long run, too intelligent.

–**George Orwell**, *1984*

Table of Contents

Prologue – The Wonder of It All
Preface – Media Massage
First Hand Experience
The Public Relations Industry
Behold a Pale Farce
Organization
Acknowledgments

Part I – Rampant Hyperbole

Chapter 1 – A Backdrop of Metaphors
Never Mind: False Alarm
The Madness of Crowds
An Electronic Pearl Harbor
A Cyber-Katrina
The Hiroshima of Cyberwar
A Cyber 9/11
The Executive Responds
CNCI – Part I
CNCI Reloaded
CYBERCOM
The Question of Offensive Operations
Stuxnet
A Picture Emerges
Rumors Abound

Black Hat or Just Old Hat?
Stuxnet as a Joint Venture
Impact on Iran's Program
DuQu: The Son of Stuxnet?
Platform Tilded
Flame, Gauss, and miniFlame
All Roads Lead to Uncle Sam
Plan X
Presidential Policy Directive 20
Hacking Foreign Targets for Years
Oz the Great and Powerful

Chapter 2 Our Frenemy in Asia

A Plurality of Actors
Rule of Law Breaks Down
The Internet's Frontier Town
Opposing Models for Reform
The Extent of China's Capabilities
Joined at the Hip
Both Sides Keep the Other in Business
The #1 Threat to Economic Security

Chapter 3 Cyberwar as a Misdiagnosis

Dialing 911
War
Terrorism
Espionage
Crime
Looking Ahead

Part II – A Series of Unfortunate Events

Chapter 4 Cybercrime

The Ecosystem
- Breaking In
- Fencing the Goods
- Evading Capture

A Snapshot of Cybercrime
- The TJX Hack
- The Heartland Payment Systems Breach
- The DarkMarket Sting
- Torpig Takedown
- The RBS WorldPay Attack
- The Return of the Analyzer
- The Ballad of Max Butler
- Operation Trident Breach
- From China with Love
- Sony Under Siege
- Citigroup Comes Clean
- The FIS Breach
- Operation Trident Tribunal

The Big Picture
- Loss Statistics

The Punch Line

Chapter 5 Espionage

Moonlight Maze
Titan Rain
Operation Byzantine Hades
GhostNet
Joint Strike Fighter Breach
Operation Aurora
Shadows in the Cloud

Night Dragon
RSA and SecurID
Operation Shady RAT
The Nitro Attacks
Targeting Certificate Authorities
Comodogate
Operation Black Tulip
Multistage Attacks Emerge
Operation Red October
Patterns Emerge

Chapter 6 The Scope of U.S. Espionage

Booby-Trapped Chips
U.S. Subversion Programs
U.S. Economic Espionage
Apologists and Opposing Views
American Exceptionalism
The Malware Industrial Complex
Mass Surveillance Systems
Exploits and Arms Dealers
Falling Barriers to Entry
Independent Operators
History Repeats Itself
Spies Abound…
But Some Groups Spy More Than Others

Chapter 7 The Infrastructure

The Financial System
The Stock Exchanges
The Federal Reserve
Serious Threats

The Power Grid
The Telecoms
Aerospace
The Internet: Denial of Service Attacks
Estonia
Georgia
Kyrgyzstan
South Korea and the United States
South Korea, Again
McAfee
Commercial Bank Attacks
Spamhaus
A Nuisance at Best
The Internet: Manipulating Traffic

Chapter 8 Threat Inflation

Conflicts of Interest
Moving Towards Cyber Security

Part III – The Futility of Offensive Solutions

Chapter 9 The Quandary of Attribution

Achieving Anonymity Online
Do-It-Yourself Anonymity
Browser Profiling
Defense in Depth
Retail Products
Government-Funded Efforts
The Origins of Tor
Attribution for Everyone… But The Inner Party
The Folly of Attribution
Anti-Forensics
False Flag Operations

Deterrence
Arms Control Treaties

Chapter 10 – Shades of Orwell

The Golden Age of Surveillance
Warrantless Wiretapping
FISA Amendments Act of 2008
Violations Occur
Mass Interception
An Aside: Files on Everyone
Verizon FISC Order
PRISM
The NSA's MUSCULAR Project
Opting Into Surveillance
Vengeful Librarians
The DHS Monitors Social Media
Corporate Compliance
CISPA
The Hemisphere Project
Spying as a Business Model
The Public-Private Partnership
A Global Panopticon
Questioning the Official Narrative
Watching America's Adversaries
By The Numbers
The End of the Middle
Terrorism Is the New Communism
Coda: Extorting Privacy

Part IV – The Road to Cyber Security

Chapter 11 – The Origins of Cyber-Insecurity
A Layered Perspective

Exciting Causes
Human Factors
Misconfiguration
Buggy Software
The Software Depression
Critical Bugs Are Pedestrian
The Presumption of Security
Assurance is Lacking
Inadequate Endpoint Security
Predisposing Causes
Remote Causes
Market Forces
Negative Externalities
A Word on Bug Bounties
Security for the 1%

Chapter 12 – Cyber -Security for the 99%

Building Resilient Software
Prevention versus Response
Compartmentalization
Poor Man's Tactics
Sandboxes and Virtual Machines
Formal Verification
Treating the Symptoms
International Cooperation
Managing Externalities
Regulation
Liability
Catch-22
Other Barriers to Change
Strength in Numbers

Summation

The Hazards of a Misdiagnosis

Securitization In-Depth
Threat Inflation
The Folly of Deterrence
In Search of Enemies
American Hypocrisy
Subverting Attribution
Turning to Big Brother
Root Causes of Cyber-Insecurity
Cyber Security for the 1%
Cyber Security for the 99%

Prologue

The Wonder of it All

Behold a cavalcade of legislators, government officials, and think tank fellows. They claim that the United States waivers perilously at the brink of catastrophe. These people believe that foreign powers are poised to cripple the U.S. power grid and decimate the banking system. They warn that if we fail to implement the measures which they endorse, we risk a Cyber Armageddon.

Yet this End Times narrative is a farce, and a pale one at that. These doomsday scenarios serve only to benefit the military-industrial complex. Cyberwar propaganda is an instance of threat inflation. Much like during the run-up to the disastrous global War on Terror. The message of Cyberwar is eliciting a crisis mentality. The end result is an anxious public that's susceptible to ill-conceived, but highly profitable, solutions.

Once more, while the apparatchiks sound the alarm about external threats, there are genuine threats emanating from within. America's Deep State is busy executing campaigns of espionage and sabotage in foreign networks. U.S. intelligence agencies are embroiled in covert operations at home and abroad which have been instrumental in the emergence of a sprawling underground industry that develops weaponized malware and Orwellian mass interception tools. Proponents explain that these developments are necessary to ensure our "national security." The reality is that this decidedly offensive approach is seriously undermining our collective security.

In these pages you'll see who is spreading the Cyberwar message, the nature of the game being played, the real threats that we're being distracted from, and the often unacknowledged root causes of our growing cyber-insecurity.

Preface

Media Massage

And I will utter my judgments against them touching all their wickedness …

–Jeremiah 1:16 King James Bible

I think it's wrong that – that newspaper reporters have all these documents, 50,000 or whatever they have, and are selling them and giving them out as if these – you know, it just doesn't make sense. We ought to come up with a way of stopping it. I don't know how to do that. That's more of the courts and the policymakers. But from my perspective, it's wrong, and to allow this go on is wrong.

–General Keith Alexander[1]

In an ideal world, the media would serve as a watchdog of sorts where those in power must tolerate constant, and rigorous, scrutiny by an aggressive press which reports to an engaged and knowledgeable populace. This is what's known as the *Jeffersonian model* for analyzing the role of the media. An alternative model is the *Propaganda model*, where the major news outlets distort information in a manner that defends the agendas of the people who control society.

Guardian journalist Glenn Greenwald has characterized these two models in terms of David Halberstam and Bill Keller. Halberstam was a reporter who was kicked out of the *New York Times* after persistently challenging official government narratives during the Vietnam War. Keller, the former *New York Times* editor, oversaw the publication of documents released by WikiLeaks only after receiving approval for each document from the Obama administration:

> David Halberstam viewed the measurement of good journalism as defined by how much you anger the people in power that you're covering whereas Bill Keller defines good journal-

> ism – and I think most modern establishment journalists define it this way as well – by how much you please the people in power that you're covering.[2]

In the late 1980s, Noam Chomsky and Edward Herman analytically demonstrated that the large, agenda-setting, news outlets largely adhere to the Propaganda model in their book *Manufacturing Consent*.[3] This should come as no surprise, as the major outlets, like the *Wall Street Journal*, are part of large publicly traded corporations. Being publicly traded, the agenda-setters are beholden to the desires of Wall Street, where investors measure their value as a function of the profit that they generate.

The *Wall Street Journal* sells millions of papers every day,[4] and advertisement revenue is so large that the executives who control the outlet have even considered simply giving away online content for free.[5] What this demonstrates is that major news sources like the *Wall Street Journal* have a product (their readers) that they sell to the buyers in the market (the advertisers).

As it turns out, the profit margin in this market can be pretty good. This is because papers like the *Wall Street Journal* maintain a channel to a valuable commodity: society's decision makers. In other words, many of the people who read the *Wall Street Journal* also represent America's one percent. According to ABC News, the average household income of the *Wall Street Journal*'s subscriber in 2007 was approximately $235,000.[6]

So what's going on is that you have one large corporation selling its product to other large corporations, where the product is the eyes and ears of the top tier. It only makes sense that the ideas put forth will be those that cater to the economic desires and political inclinations of the parties involved. In fact, this kind of distortion is exactly what Noam Chomsky and Edward Herman discovered while studying the nature of the mass media.

Canadian scholar Marshall McLuhan once observed:

> One thing about which fish know exactly nothing is water, since they have no anti-environment which would enable them to perceive the element they live in.[7]

Because it's immersed in water every minute of its life a fish is less likely to recognize the significance of water's presence. Such is the effect of propaganda. Society is overwhelmed by spin often without being aware of it. Once more, because the Constitution of the United States includes provisions regarding the freedom of speech, ideas can compete with one another. As a result propaganda has to be more subtle and sophisticated so that people don't necessarily feel like they're being overtly influenced.

First Hand Experience

While I've read about the many filtering mechanisms of the Propaganda model and witnessed its operation from afar, I never thought that I'd encounter them directly. This changed in late 2011 when, out of the blue, I received an e-mail from a senior editor at a well-known technical publisher located South of Market in downtown San Francisco. Having viewed my slides on Cyberwar from SFSU's National Cybersecurity Awareness Event[8] the editor wanted to know if I was interested in authoring a book on the topic. Shortly after the editor's initial query I signed a contract and feverishly began the process of putting material together.

Four or five months later the editor ominously summoned your author and co-author to his office for a meeting. He announced that both he and the founder of the publishing house were very concerned about the tone of the book. The editor complained at length about the potential hazards of *push back*, particularly with regard to the coverage of former Director of National Intelligence Mike McConnell. I was sending a message that would directly challenge the narrative being spread by powerful interests, and there was a serious threat of retaliation. He also protested rather loudly that there were some things he *couldn't sell*. Then, to top off his list of complaints, he began to make pointed references to outcome of the 2012 *United States Presidential Election* with regard to the book's publication date.

It became clear that I was being asked to significantly alter, if not eliminate, material. The editor seemed to be giving me a thinly veiled ultimatum. Either I get on board and do things his way or he'd negate the contract. At one point, he even suggested that I

change the focus of the manuscript away from Cyberwar and write an entirely different book.

This is what happens when you sign on with a publishing house where the higher ups believe in "deep editing." Given the effort involved in the project, I was hesitant to walk away. Though that's exactly what I should've done; the minute that he mentioned the 2012 Presidential Election. Instead I adopted a strategy of gentle resistance, a sort of quicksand approach, where I persistently challenged the editor's comments by supplying counter-arguments and then requesting feedback. Unfortunately he decided not to engage in dialogue. As months passed the editor became unresponsive. Then, after almost a year of work, the publisher abruptly canceled the contract.

As you can see, I was eventually able to find a new publisher to work with. Indeed, I applaud TrineDay for having the courage to back this project at a time when other mainstream publishers, being confronted with a reality that made them just a bit uncomfortable, scurried back into the woodwork. Such are the risks of speaking truth to power.

The Public Relations Industry

> *The 20th century has been characterized by three developments of great political importance: The growth of democracy; the growth of corporate power; and the growth of corporate propaganda as a means of protecting corporate power against democracy.*
>
> –Alex Carey[9]

> *America has no functioning democracy.*
>
> –Former President Jimmy Carter[10]

In the lead up to World War I, President Woodrow Wilson found himself in a difficult position. By maintaining a stance of neutrality during his first term as President he won his second term with the campaign slogan "He kept us out of war." Shortly after the launch of his second term he pulled a 180-degree turn and decided that the United States needed to enter the war. How could he

convince the population to go along with him when they'd already given a mandate for continued neutrality?

To move the American public into his corner President Wilson formed the Committee on Public Information, also known as the *Creel Committee* (after its chair, journalist George Creel). The Creel Committee headed up a massive campaign to influence public opinion. For example, it amassed a division of some 75,000 "Four Minute Men," a group of volunteers who were given talking points and sent out to give speeches.[11] Their presentations tended to be about four minutes in length, somewhere in the neighborhood of the purported average attention span.

To demonize the enemy Germans were depicted as bloodthirsty Huns.[12] In particular, the Creel Committee fabricated a story about "Corpse Utilization Plants," which claimed that the Germans were taking the bodies of their own dead soldiers and boiling them down to manufacture pig food and munitions.[13] This story was bolstered by alleged eyewitness accounts appearing in other news sources, who described the gory details of the factories operations.

One member of the Creel Committee, Ed Bernays, is seen as the grandfather of modern propaganda. Bernays is credited with inventing the term *public relations* (aka PR). He did so admittedly to avoid the stigma associated with the word "propaganda."[14] More recently, members within the public relations industry have begun to call what they do as *perception management*. But these are just pleasant sounding euphemisms.

In the discipline of economics they have what's called the *efficient market hypothesis* (EMH) which is a concept used to help describe how markets work.[15] The EMH is founded on the premise that in a properly functioning market people have access to accurate information and think rationally (see Figure 1).

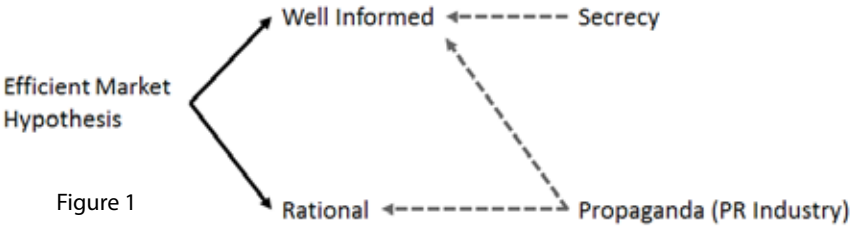


Figure 1

In economic markets, the public relations industry at times works assiduously to subvert this scenario, to prevent things from operating efficiently. Those who disseminate propaganda don't necessarily want people to have access to good information. Rather, the architects of propaganda have been known to employ tactics that appeal to people on an emotional level rather than a rational one. To see these tactics in action all you have to do is inspect a couple of cigarette commercials.

The emphasis on primal responses is no accident. Bernays, as it turns out, was the nephew of Sigmund Freud and he was heavily influenced by his Uncle's theory of the mind. Drawing from the subject of psychoanalysis, Bernays argued that people were driven by unconscious and irrational forces that, if not reined in, could tear society apart. As a result, he believed that large-scale manipulation of public opinion was not only possible, but necessary[16]:

> The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democracy society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country.

Bernays called his approach, *the engineering of consent*.[17] He applied his tools of on behalf of corporate titans like General Electric the American Tobacco Corporation. In the 1950s, as the Cold War was kicking into high gear, Bernays led a propaganda campaign at the behest of the United Fruit Corporation (UFC). UFC had land holdings in Guatemala that were threatened by nationalization. Bernays utilized the press to create the perception of a Communist threat, inciting a brutal military coup.[18]

In addition to his Uncle Sigmund, Bernays' ideas were shaped by another prominent thinker: Walter Lippmann. Lippmann was a celebrated journalist and a founder of *The New Republic* magazine. During World War I has was an advisor to President Wilson and was involved in the composition of Wilson's *Fourteen Points* speech. He was also the general secretary of a clandestine quasi-intelligence outfit called "The Inquiry" which was set up

by President Wilson for the sake of "drawing up the embryonic outlines of the postwar world."[19]

In his 1922 book entitled *Public Opinion*, Lippmann claimed that the complexities of governance were too much for normal people such that the "common interest" wasn't always obvious. Instead, the process must be managed by a "specialized class" of elite technocrats who knew what they were doing:

> The common interests very largely elude public opinion entirely, and can be managed only by a specialized class whose personal interests reach beyond the locality.

Lippmann's worldview was later echoed by American political scientist Harold Lasswell:

> The modern propagandist, like the modern psychologist, recognizes that men are often poor judges of their own interests, flitting from one alternative to the next without solid reason.
>
> Democracy in America has compelled a whole new technique of control, largely through propaganda because of the ignorance and superstition of the masses.[20]

Lippmann believed that this specialized class, having identified policies that benefited the common interest, could then generate support for their decisions by *manufacturing consent* (Bernays' idea of engineering consent is derived from this concept). In a nutshell, Lippmann advocated that the specialized class make decisions and then convinced society to go along after the fact using propaganda.

Looking at these formative years, it's clear that the foundations of modern propaganda were established by people who believed that society generally wasn't capable of governing itself. They postulated that people couldn't be trusted to make good decisions and that they would be better off leaving the work to government to technocrats who then generated support for their decisions using the tools of public relations. This scheme for democracy was embraced and propaganda has become the primary means through which the elite communicate with the rest of society.[21]

Historically the American elite have been known to shun democracy in matters of global dominion. Such that public opinion is a mere peripheral issue. For example, speaking to Richard Nixon on the need to depose Chilean President Salvador Allende, Henry Kissinger advised Nixon:

> Allende is now president. The State Department thinks we can coexist with him, but I want you to make sure you tell everybody in the U.S. government that we cannot, that we cannot let him succeed, because he has legitimacy. He is democratically elected. And suppose other governments decide to follow in his footstep, like a government like Italy? What are we going to do then? What are we going to say when other countries start to democratically elect other Salvador Allendes? We will – the world balance of power will change …[22]

Here's another instance where an elite spokesman lets the truth slip out. In August of 2013, at the American Legislative Exchange Council (ALEC) conference in Chicago, one right wing think tank fellow made the following statement about the necessary ingredients required to amend the Constitution[23]:

> Oh, well, you really don't need people to do this. You just need control over the legislature and you need money, and we have both.

In democratic forms of governance, where the population is supposed to participate in decision making, citizens need access to good information in order to properly exercise sound judgment. This is in line with Karl Popper's concept of an *open society*. Given the capacity of PR to obfuscate facts and rely on emotionally potent appeals, it can be a powerful means to subvert democracy (see Figure 2). Financial columnist Igor Greenwald comments:

> Corporations lie more convincingly than individuals. They have the resources to hire experts and lobbyists. They can buy any overt advertising they might require from wholly-owned media subsidiaries.[24]

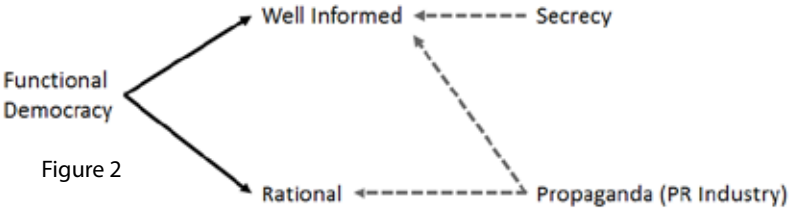


Figure 2

Secrecy can likewise play a similar role in terms of undermining the decision making process, even in presumably democratic political systems. In this regard national security is a near universal pretext that leaders turn to when they want to keep the public in the dark.[25]

Both of these tools, propaganda and secrecy, will be on display in this book.

Behold a Pale Farce

And I looked, and behold a pale horse: and his name that sat on him was Death, and Hell followed with him.

–Revelations 6:8 King James Bible

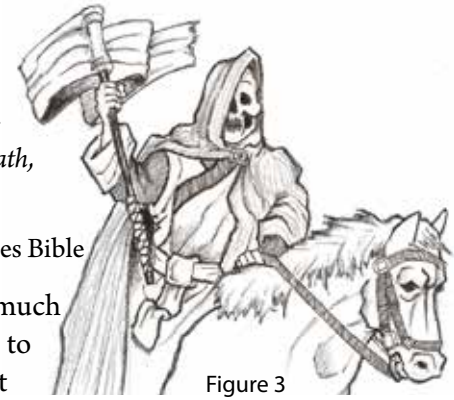


Figure 3

The reason why I've devoted so much bandwidth in this preface to propaganda and media studies is that the people promoting the concept of Cyberwar rely heavily on tactics honed by the PR industry. As I'll demonstrate, the notion of Cyberwar is accompanied by a slew of doomsday scenarios; altogether farcical tales of the end times. I personally doubt very much that these vivid worst-case scenarios are intended to encourage logical thought, hence this book's title.

The primary outcome of the Cyberwar campaign is mass anxiety, where people so apprehensive and uneasy that they'll accept any solution to feel safe again. This is convenient because the solutions being proposed by the Cyberwar crowd harken back to the Cold War. There's a heavy emphasis on massive retaliation and Orwellian surveillance schemes, neither of which are constructive approaches. These supposed remedies would only channel vast

sums of money to the defense industry and further infringe on our civil liberties by enhancing government control.

There's a very real effort afoot to create the perception of an imminent and grave threat. A public that feels panicky which will pay dearly to make the anxiety go away, much to the benefit the same people stoking the coals of alarm. What society needs to do is to collectively step back, take a deep breath, and approach the topic from a more rational frame of mind.

As far as the domain of politics is concerned, propaganda and secrecy will always exist as means to sabotage decision making. In countries like the United States, however, which have provisions for freedom of speech there are opportunities to shed light on complicated topics.

In a nutshell: that's what this book is all about.

Organization

This book is divided into four parts. In the first part I present a sampling of Cyberwar hyperbole that's received media coverage, identify a couple of the more prominent actors, and follow the policies that have been enacted. Next, we'll take a closer look at China to provide some context against which assertions in the first chapter can be judged. Finally, I set up the second part of the book by developing a cataloguing scheme for cyber incidents. To treat an ailment you first need an accurate diagnosis. My goal is to establish precise definitions so that I can cultivate an accurate picture of what's actually going on.

In the second part of the book I survey a number of high-profile cyber incidents and classify them according to definitions established at the end of the first part. What I discovered was an overwhelming preponderance of crime and espionage. I didn't, however, encounter any cyber incidents that could be interpreted as Cyberwar. Yet Cyberwar has been portrayed as an impending threat, one which is certain to transpire. Hence, at the end of part two I introduce the concept of *threat inflation* to expose the underlying dynamics at work.

In the third part of the book I examine solutions that have been offered to protect the United States from the threat of Cyberwar.

Specifically, the Cold War strategy of deterrence is explored at length and, in lieu of its failings, I wade into the details of the rising surveillance state. Neither of these options is attractive or even feasible. Yet they would both waste vast amounts of money and sacrifice our liberty on the altar of national security. This leads to part four of the book.

In part four of the book I mull over the factors that actually allow cyber-attacks to succeed and steps that can be taken to mitigate them. When it comes to security breaches there are a number of factors working together on various levels. But all factors aren't equal and some factors are actually used by the software industry to obscure more central ones. In light of this I focus primarily on the crisis of poor software design and the market forces that drive it. I also recommend re-orienting our national security strategy towards developing truly resilient software and deploying it at a grass-roots level.

Acknowledgments

We have an executive, a Department of Justice, that's unwilling to prosecute high officials who lied to Congress and the country on camera, but they'll stop at nothing to persecute someone who told them the truth.

–Edward Snowden[26]

This book was composed over what could be characterized as a long forced march. Despite the obstacles, dead ends, ambushes, constant frustration, and hostile environment that beset the project, we stubbornly pressed onward. As in any demanding situation persistence and optimism were the keys to success.

The stakes are high. Society is being deluged with a perception of threat, a misdiagnosis that has been inflated well beyond what it deserves, in an effort to promote solutions which will undermine our collective security. I have faith that by presenting people with evidence-based conclusions, by appealing to reason, the debate can be shifted away from hyperbole and towards effective broad-based security measures.

There have been many people who offered their assistance during the writing process. In particular I'd like to express my grat-

itude to George Ledin at UC Sonoma for his support and encouragement. George is one of the very few professors who openly lecture on malware design in the United States and his willingness to charge headlong into this nascent field of study is commendable.

Norm Matloff is a professor at UC Davis who works tirelessly to counteract the growing trend of outsourcing (i.e. global labor arbitrage). It's a topic, very much like Cyberwar, were corporate-funded propaganda has taken root and holds a disproportionate amount of sway. Norm's activism in this area, to expose the lies and fabrications of corporate spin masters, does a great service to computer scientists all over the country.

I'd also like thank George Smith, a Senior Fellow at GlobalSecurity.org who coined the phrase *Cult of Cyberwar*. George has been tracking this topic for years and his thoughts on Cyberwar have been vital.

That goes double for John Young and Deborah Natsios, who manage the leaks site *Cryptome*. They have consistently offered the world their uncensored view of the security industry. For years John skeptically claimed that the intelligence services had systematically compromised technology across the board. Some people have dismissed his observations as the ranting of a paranoid geezer, "art as evidence" they say. It turns out the grouchy old cynic was right on the money.

Canadian filmmaker Scott Noble also deserves credit for directing a series of powerful, well-researched, documentaries that were a significant source of inspiration for this book. Scott's work covers topics like public relations, government secrecy, clandestine operations, and other insidious tools of social control. His films provide a backdrop for what you'll read herein and can be viewed online for free.[27] It's time very well spent, nay transformative.

Three cheers for Noam Chomsky over on the East Coast, the ideological epicenter of the progressive movement. Noam is a voice of conscience who asks that in the realm of foreign policy we apply to ourselves the same standards that we apply to others. It's this aspect of his analysis that fundamentally shaped this book's stance.

On the other side of the country, nigh the hills of Berkeley, poet and scholar Peter Dale Scott writes voluminously on how sources

of wealth and violence outside of government –organized crime, NGOs, transnational corporations, lobbyists, big oil, drug cartels, arms manufacturers, and global financiers– use their influence to exercise state policy. That is, Peter deftly reveals the nature and dealings of the *Deep State*. It's a term that resonates with me as I see our formal institutions as being driven primarily by subtle currents that typically flow beneath the surface of ordinary political discourse.

I'd like to tip my hat to Glenn Greenwald at the *Guardian*. When I discovered that Glenn had been targeted by a goon squad (known as *Team Themis*: HBGary Federal, Palantir, and Berico) on behalf of a major financial institution, I knew it was a sure sign that his journalism had merit. Though, in an effort to inoculate against reflexive ovation, I've begun haunting a blog known as *The Rancid Honeytrap.*[28]

A number of whistleblowers have sacrificed both their careers and their well-being to publicize government programs that pose an enormous threat to our Constitutional liberties. They've also revealed our government officials as a collection of pathological liars. In particular, I'm referring to patriots like Philip Agee, Daniel Ellsberg, Chris Pyle, John Stockwell, Ray McGovern, Thomas Tamm, Mark Klein, Thomas Drake, William Binney, Russell Tice, Chelsea Manning, John Kiriakou and Edward Snowden. This book owes these whistleblowers a tremendous debt of gratitude. By virtue of their disclosures they provided direct, and often damning, evidence to back conclusions that otherwise could only be alluded to with circumstantial evidence.

Then there are publishers like *WikiLeaks* who channel this information to the public. Julian Assange has done the world a service by demonstrating just how subservient the mainstream media outlets have become. The various interests promoting the idea of Cyberwar have been able to propagate their message in part because of their connections with the press. Such are the hazards of organizations that monetize information under the rubric of public service. What this shows is that Cyberwar propaganda isn't just late night geek fodder, it's says something significant about the current state of journalism.

Make no mistake about it, the aggressive prosecution of whistleblowers and efforts to hobble journalists ultimately translate into a fundamental attack on democracy.[29] While heads of government may publicly intimate[30] that harsher measures will be taken if newspapers fail to show the necessary "social responsibility," the spies aren't anywhere near as coy[31]:

> You've had your fun. Now we want the stuff back.

Finally, I'd like to show some love to all of the professionals at TrineDay who dutifully applied their expertise to make this book happen. Kris Millegan has devoted his life to exposing the intrigues of a relatively small group of plutocrats who relentlessly purchase influence on behalf of their own narrow financial interests. After reading the foreword which he wrote to Daniel Estulin's *Shadow Masters* I knew that Kris wouldn't back down as the original publisher did. There's a term for this sort of thing: most people call it *integrity*. A vicious class war is raging in the United States and the Devil takes the hindmost.[32] While our social fabric crumbles, society needs this kind of integrity more than ever.

$\Theta(e^x)$,
Bill Blunden

Endnotes

1) Glenn Greenwald, "As Europe erupts over US spying, NSA chief says government must stop media," *Guardian*, October 25, 2013, http://www.theguardian.com/commentisfree/2013/oct/25/europe-erupts-nsa-spying-chief-government.

2) Kevin Gosztola, "Glenn Greenwald's Speech to the Socialism Conference [with Transcript]," *FireDogLake*, June 29, 2013, http://dissenter.firedoglake.com/2013/06/29/glenn-greenwalds-speech-to-the-socialism-conference-with-transcript/.

3) Edward Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, Pantheon Books, 1988.

4) US Newspaper Circulation Averages for the Six Months ended: 9/30/2011, Audit Bureau of Circulations, http://abcas3.accessabc.com/ecirc/newstitlesearchus.asp.

5) Catherine Holahan, "The Case for Freeing the WSJ Online," *BusinessWeek*, August 10, 2007, http://www.businessweek.com/technology/content/aug2007/tc20070810_305348.htm.

6) Scott Mayerowitz, "What Do the Rich and Powerful Read?" ABC News, July 28, 2007, http://abcnews.go.com/Business/IndustryInfo/story?id=3421988&page=1.

7) Marshall McLuhan and Quentin Fiore, *War and Peace In the Global Village: An Inventory of Some of the Current Spastic Situations That Could Be Eliminated by More Feedforward*, Hardwired, 1997.

8) *Cyberwar: Hyperbole and Reality*, SFSU's National Cybersecurity Awareness Event, 2010, http://www.belowgotham.com/SFSU-2010-Blunden-Slides.pdf.

9) Alex Carey, *Taking the Risk out of Democracy*, University of Illinois Press, 1997, chapter 2, page 18.

10) Alberto Riva, "Jimmy Carter: US 'has no functioning democracy'," *Salon*, July 18, 2013, http://www.salon.com/2013/07/18/jimmy_carter_us_has_no_functioning_democracy_partner/.

11)United States. The White House. *Committee on Public Information. Purpose and Plan of Four Minute Men*. Washington D.C.: Government Printing Office, 1917, http://libcudl.colorado.edu/wwi/pdf/i7178116x.pdf.

12) Thomas Fleming, *The Illusion of Victory: America in World War I*. New York: Basic Books, 2003; pg. 247.

13) Randall Martin, *The Art of Faking Credentials*, MercatorNet, March 26, 2008, http://www.mercatornet.com/articles/view/the_art_of_faking_credentials.

14) *Century of the Self*, directed by Adam Curtis, BBC Four, 2002, http://video.google.com/videoplay?docid=9167657690296627941.

15) Eugene Fama, *Efficient Capital Markets: A Review of Theory and Empirical Work*, The Journal of Finance, Volume 25, Number 2, May 1970, pages 383-417.

16) Edward Bernays, *Propaganda*, Ig Publishing, September 2004. ISBN 0970312598.

17) Edward L. Bernays (1947), *The Engineering of Consent*, The Annals of the American Academy of Political and Social Science, 250 p. 113.

18)Larry Type, *The Father of Spin: Edward L. Bernays and The Birth of Public Relations*, Picador, 2002, ISBN-13: 978-0805067897.

19) Ronald Steel, *Walter Lippmann and the American Century*, Transaction Publishers, 2008, p. 128.

20) Harold Lasswell, "Propaganda," *Encyclopedia of the Social Sciences*, Macmillan, 1954.

21) *Psywar*, Directed by Scott Noble, Metanoia Films, Canada, 2010, http://metanoia-films.org/psywar/.

22) "'Make the Economy Scream': Secret Documents Show Nixon, Kissinger Role Backing 1973 Chile Coup," *Democracy Now!*, September 10, 2013, http://www.democracynow.org/2013/9/10/40_years_after_chiles_9_11#.

23) Theresa Riley, "Inside the 'ALEC Universe'," *Bill Moyers and Company*, August 15, 2013, http://billmoyers.com/category/what-matters-today/the-united-states-of-alec/.

24) Igor Greenwald, "Is Capitalism Dying?" *Forbes*, January 7, 2013, http://www.forbes.com/sites/igorgreenwald/2013/01/07/is-capitalism-dying/print/.

25) Alan Cowell, "Cameron Criticizes The *Guardian* for Publishing Secrets," *New York Times*, October 17, 2013, http://www.nytimes.com/2013/10/17/world/europe/cameron-criticizes-the-guardian-for-publishing-secrets.html.

26) "Edward Snowden Speaks Out Against NSA 'Dragnet Mass Surveillance,'" *Democracy Now!* October 14, 2013, http://www.democracynow.org/2013/10/14/edward_snowden_speaks_out_against_nsa#.

27) http://metanoia-films.org/films/.

28) http://ohtarzie.wordpress.com/.

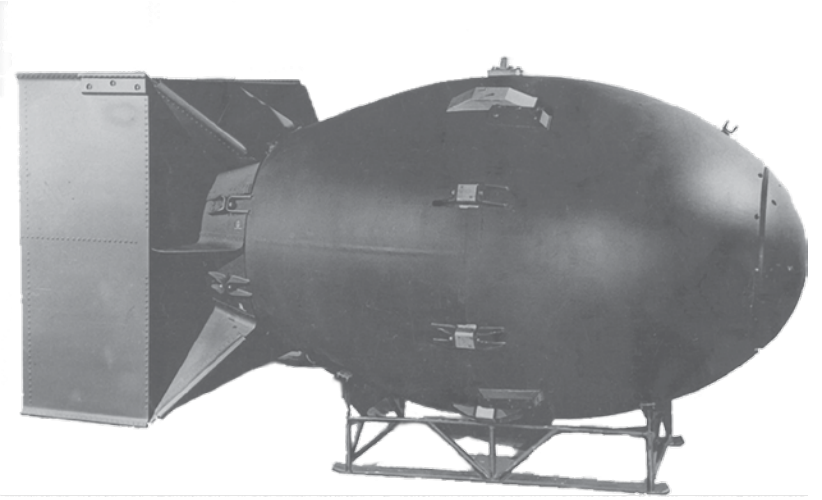
29) Committee to Protect Journalists, *The Obama Administration and the Press: Leak investigations and surveillance in post-9/11 America*, October 10, 2013, http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.

30) Nicholas Watt, "David Cameron makes veiled threat to media over NSA and GCHQ leaks," *Guardian*, October 28, 2013, http://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden/print.

31) Alan Rusbridger, "David Miranda, schedule 7 and the danger that all reporters now face," *Guardian*, August 19, 2013, http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters.

32) Jacob S. Hacker and Paul Pierson, *Winner-Take-All Politics: How Washington Made the Rich Richer – and Turned Its Back on the Middle Class*, Simon & Schuster, March 15, 2011, ISBN-13: 978-1416588702.

Part I – Rampant Hyperbole



Chapter 1

A Backdrop of Metaphors

Chapter 2

Our Frenemy in Asia

Chapter 3

Cyberwar as a Misdiagnosis