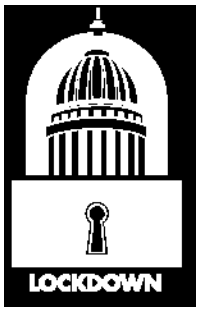

Lockdown 2010 – University of Wisconsin-Madison
Conference Proceedings

Manufactured Consent and Cyberwar

Bill Blunden
Principal Investigator
Below Gotham Labs
www.belowgotham.com

$$-K_B \sum_i P_i \log_e(P_i)$$

Abstract

Over the past year, there have been numerous pieces that have appeared in the press alluding to the dire consequences of Cyberwar and the near existential threat that it represents to the United States. While these intimations of destruction can seem alarming at first glance, closer scrutiny reveals something else. Ultimately, the gilded hyperbole of Cyberwar being peddled to the public is dangerous because it distracts us from focusing on actual threats and constructive solutions. Pay no attention to the man behind the curtain says the ball of fire named Oz. In this presentation, I'll pull back the curtain to expose the techniques being used to manipulate us and the underlying institutional dynamics that facilitate them.

Presenting the Problem

There are those who would have you believe that the United States is currently embroiled in a Cyberwar. Once more, they would assert that we're losing this war. To this end, they direct our attention to the headlines.

For example, in November of 2009 the television Program "60 Minutes" aired a piece called *Cyber War: Sabotaging the System* [1]. In one segment, the program mentioned a 2007 power outage in Brazil that affected millions of people. Reporters cited unnamed intelligence sources who claimed that the outage was the result of a cyber attack.

According to the director of Brazil's Homeland Security Information and Communication directorate, Raphael Mandarino, Brazil's electric control systems are not directly connected to the Internet [2]. Furthermore, Brazil's independent systems operator group concluded in January of 2009 that the outage resulted from soot that had accumulated on tower insulators as farmers burned their fields [3].

In a later segment of the same televised program, Jim Lewis, the director of the Center for Strategic and International Studies, described what he called "the most significant incident ever publically acknowledged by the Pentagon." Lewis was referring to an incident in November of 2008, when the *agent.btz* worm found its way into CENTCOM's classified network by way of an infected thumb drive. According to Lewis, "Some foreign power was able to get into their networks. And sit there and see everything they did. That was a major problem. And that's really had a big effect on D.O.D."

What Lewis failed to mention is that CENTCOM, being a classified network, isn't connected to the Internet. Despite the fact that the worm installs a back door on the machines it compromises, there was no way for anyone on the outside to communicate with infected machines or exfiltrate data [4].

The Dangers of a Crisis Mentality

But it's not just the smattering of actual reports that are brought to our attention. Cyberwar pundits also like to point out *potential* attack scenarios and embellish these descriptions with a litany of ominous sounding metaphors. Says one CEO, "If you're looking for a digital Pearl Harbor, we now have the Japanese ships streaming toward us on the horizon [5]."

In April of 2008, the Wall Street Journal's Siobhan Gorman wrote an article warning that "cyberspies have penetrated the U.S. electrical grid and left behind software programs that *could* be used to disrupt the system, according to current and former national-security officials [6]." As of yet there have been no corroborating details released to the public. Nevertheless, the idea of our power grid being wiped out in one fell swoop does evoke a certain visceral response.

As Bruce Schneier notes, these stories "fill our imagination vividly, in full color with rich detail. Before long, we're envisioning an entire story line, with or without Bruce Willis saving the day [7]."

The end result of all this hyperbole is that we're left with a skewed sense of risk, the hallmark of a *crisis mentality*. The general impression of an impending disaster causes us to inflate the risk that we associate with Cyberwar and at the same time disregard those risks which actually do pose a clear and present danger. It's like a baseball fan who's too scared to attend a game because they're worried that Al Qaeda might bomb the stadium, and at the same time they drive around without wearing a seatbelt.

The Cold War Approach

You could address the allegation of an ongoing Cyberwar from a semantic level. For instance, you could argue that much of what's currently happening isn't warfare in the strict Hague Convention sense of the word (e.g. mass casualties, widespread destruction, etc.).

In an op-ed piece appearing in the Washington Post, former NSA director Mike McConnell pointed to the recent attacks on Google in reference to the Cyberwar [8]. However, based on what's been revealed it would seem that the attackers were after Google's source code. Strictly speaking this looks a whole lot more like a case of industrial espionage [9].

The same could be said for the attacks that breached the Pentagon's Joint Strike Fighter project, where intruders made off with information on the F-35 Lightning II fighter [10].

If you tried hard enough, you could probably lump these reports into some vague, arm-waving, definition of "war." But at the end of the day they're really instances of espionage.

Anyway, I'm not going to take this route because I believe that the concept of Cyberwar being promulgated is really nothing more than *a pretext* for the solutions that certain retired intelligence officials are ready to offer us. Having pushed the right buttons to whip up the requisite levels of hysteria, they spring their ideas on us while we're susceptible, while we're in the throes of a crisis mentality.

This is somewhat reminiscent of the September 18, 2008 meeting in the conference room of the House speaker, Nancy Pelosi, where Ben Bernanke admonished that unless Congressional leaders agreed to a $700 billion plan to bailout Wall Street, "we may not have an economy on Monday [11]." Faced with this looming catastrophe, lawmakers rushed in with a mass infusion of taxpayer dollars. Pay no attention to the executive bonuses or the corporate jets [12].

One "solution" that's been offered to resolve the Cyberwar "problem" draws on the military strategy that ushered the United States through the cold war: deterrence. The basic train of thought being that we prevent attacks by threatening would be attackers with massive retaliation in the event that they initiate hostilities.

Naturally, instituting a policy of massive retaliation would require us to have weaponry that's up to the task. This, in turn, would entail developing a sophisticated arsenal of hi-tech ordinance. Suffice it to say that a small army of developers, testers, and managers would need to be conscripted (preferably by beltway savvy defense

contractors) and billions in funding would need to be raised to finance the corresponding R&D [13].

The Quandary of Attribution

The thing about having a huge stockpile of military-grade offensive weaponry is that it helps if you know who to point it at. Hence, a prerequisite of massive retaliation is attribution. This is where the deterrence school of thought hits a brick wall. Experience has shown that discovering exactly who's behind a cyber attack is a losing proposition, and even when we *think* we know who's responsible we tend to overreact.

Take the recent attacks on Google. Though the actions of the company itself appear to place responsibility squarely on the shoulders of the Chinese government, there's no concrete evidence which confirms this. A report released by HBGary states that: "At this time, there is very little available in terms of attribution [14]."

On a side note, I find it odd that a company which markets its own web browser was victimized by a zero-day exploit that targets Microsoft's Internet Explorer [15].

In general, it's bad enough that we aren't able to determine who's behind an attack. What's even worse is that we may incorrectly conclude who the guilty party is and then retaliate against the wrong people. Such are the dangers of misattribution. In July of 2009, a distributed denial of service attack hit US and South Korean computer networks. Though hard evidence as to the source of the attacks was lacking [16], this didn't stop Peter Hoekstra, the lead Republican on the House Intelligence Committee, from demanding that the United States conduct a "show of force" against North Korea [17].

Researchers from Bkis Security in Hanoi discovered that the attack involved over 166,000 machines spread across 74 different countries. The master command and control server that coordinated these compromised machines was originally traced to the UK [18]. In a press release, the British company that owns this server, Global Digital Broadcast, claimed that they "quickly discounted it as coming from a North Korean Government site, as suggested and was tracked back to the source which was on a VPN circuit in Miami [19]." …Naturally, there's really no way to tell who was in control of the machine in Miami. For all we know it could have been those damn Canadians again.

Too an extent, Hoekstra's saber rattling is a predictable. A research study carried out by the psychology department at UC Berkeley demonstrated that participants who externalized blame for an attack were more likely to support a military response. While those participants more inclined towards introspection were less likely [20]. As Bruce Schneier quipped "enough of the hype and the bluster. The news isn't the attacks, but that some networks had security lousy enough to be vulnerable to them [21]."

The Issue of Collateral Damage

Another problem with the idea of massive retaliation on the Internet is the law of unintended consequences. For example,

in the months preceding the 2003 invasion of Iraq, military strategists considered attacking the networks that supported Iraq's financial institutions. They decided against this plan after determining that these networks were global, intertwined with civilian networks, and used by banks in other countries [22].

A RAND study published in 2009 arrived at similar conclusions: "Certainty in predicting the effects of cyberattacks is undermined by the same complexity that makes cyberattacks possible in the first place. Investigation may reveal that a particular system has a particular vulnerability. Predicting what an attack can do requires knowing how the system and its operators will respond to signs of dysfunction and knowing the behavior of processes and systems associated with the system being attacked [23]."

The Global Panopticon

Those who assert the existence of an ongoing Cyberwar are well aware of the shortcomings of the strategy of deterrence. In the spirit of Hegelian dialectics, they're waiting in the wings with a solution to the problem of attribution. Mike McConnell claims that "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable [24]."

This begs the question: how should we reengineer the Internet? Some experts claim that we should find ways to leverage the assets of the NSA and that "the private sector needs to be able to share network information -- on a controlled basis -- without inviting lawsuits from shareholders and others [25]."

This is a clever maneuver on their part. As Moxie Marlinspike inquired at the SOURCE 2010 conference: who do you think harvests better information on the local populace, Google or Kim Jong-Il? Why mandate surveillance when you can simply have people opt in?

The experts in our government deem that privacy and security constitute a zero-sum game. You can't enhance one without relinquishing the other. They believe that "in order for cyberspace to be policed, Internet activity will have to be closely monitored…that would mean giving government the authority to examine the content of any e-mail, file transfer, or Web search [26]."

In other words, private industry (which owns the bulk of the Internet's physical infrastructure) should invite the NSA into their networks and give them unfettered access to find out who's doing what to whom at the bit-by-bit level of granularity. Welcome to the Global Panopticon.

A Sign of Things to Come

And if it wasn't bad enough that there's a movement afoot to turn the Internet into a massive Orwellian telescreen, there's a company named Packet Forensics that's banking on where things are headed. They sell a network appliance (intended strictly for law enforcement, of course) designed to intercept SSL-encrypted HTTP sessions using forged certificates. Granted, you'd

actually have to approach a legitimate Certificate Authority like VeriSign and get them to issue you a forged certificate, perhaps by court order. But in this post-FISA Amendment era, cooperation from the private sector seems to be much more forthcoming than it used to.

The pamphlet for this appliance declares that "Your investigative staff will collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VOIP encryption [27]."

Attribution is NP Complete

Given the nature of the Internet, and the current state of the art in stealth technology (e.g. rootkits, anti-forensics, etc.), attribution simply isn't a realistic goal. In the parlance of computational complexity, it's an *NP Complete* problem.

Bytes are bytes, and a skillful attacker (think state or corporate sponsored actor) can arrange them however they wish to tell any story that they please. This includes *framing a third party for an act that they didn't commit*. It's a bitter pill to swallow but that's just how computers work. No amount of federal funding or packet shaping is going to change things. Rather than collectively bang our heads against a wall, why not work on problems where we can actually make progress?

The Best Defense…

Attacks often succeed because the intruders exploited a weakness in the system that they were targeting. Professional Black Hats don't storm the main gates with dynamite, metaphorically speaking. They quietly creep in through a concealed entryway that isn't on the floor plans and proceed to subvert essential system components from the inside out. Don't think crash and burn, think misinformation and subterfuge.

Considering the limitations of the deterrence approach to Cyberwar, perhaps we need a different game plan. As RAND pointed out, "in this medium [the Internet], the best defense is not necessarily a good offense; it is usually a good defense [28]."

Not only will stronger fortifications shield us if and when a Cyberwar ever breaks out, but they'll also help to protect us from the everyday threat of cybercrime. So even if we do the right thing for the wrong reason we can still garner a significant return on investment. The same cannot be said for deterrence.

Fortifying Our Defenses

User education to increase awareness of security issues is a start, but taken to excess this becomes a futile exercise in blaming the victim. Sure, users often click on links that they shouldn't or fail to recognize social engineering attacks, but even vigilant users can be duped. For instance, it's been well documented that a number of reputable web sites have unintentionally hosted malicious content [29].

The same can be said for instituting a disciplines security process: staying on the patch treadmill, deploying configuration controls, performing routine assessments, monitoring your networks, establish multi-layered perimeters, responding to incidents

that occur, etc. These are all important steps that are often neglected.

One thing that enabled the recent attacks on Google was that they didn't bother to secure their source code control system! According to Dmitri Alperovitch, McAfee's vice president for threat research. "No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways — much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting [30]."

This is what happens when business goals override security. Despite being entrusted with protecting resources, the primary goal of every system administrator is *availability*. Trust me; I'm a system administrator myself. Changing this to give the same level of priority to security typically entails a mandate from above. Richard Bejtlich, GE's Director of Incident Response, recommends that you approach executive officers about this by appealing to their innate desire to maintain a competitive advantage [31].

Yet, assuming that your users are security conscious, to the point of being obsessive compulsive, and your security process is meticulously followed …*you can still get rooted by zero-day exploits*. Put up all the ramparts you want, someone with a weaponized zero-day exploit will walk right through them. Heck, if it can happen to Google, it can happen to anyone. This is why I believe that, at the end of the day, *software vendors need to shoulder much of the burden* when it comes to shoring up our defenses.

The Quandary of Software Security

In criminal trials here in the United States the burden of proof is on the prosecution. In other words, you're innocent until proven guilty. Likewise, our current attitude towards software security infers that we believe software to be secure until proven otherwise.

The result of this mindset is what's known as the patching treadmill. Software is viewed as relatively secure until someone publicizes a zero-day exploit and shames (or forces) the vendor into admitting there's a flaw and releasing a patch. At this point the software is again considered to be "secure," or at least "more secure." Though, software flaws tend to be like roaches. When you find one you can bet that there are a few dozen that you don't see.

The way things work now, vendors are basically using security researchers to perform low cost quality control. For instance, in response to Google's $500 bounty on bugs in their Chrome browser, former NSA employee Charlie Miller said: "I think it's ridiculous… It's insulting. It's so low [32]." The ugly truth is that researchers with Charlie Miller's level of expertise would probably do a whole lot better, from a financial perspective, by selling their exploits on the black market.

The reactive nature of the patching treadmill isn't working. Zero-day exploits continue to plague ostensibly mature products [33]. What we need is a formally devised proactive system that recognizes the need to build in security from the ground up. One such solution discussed by Brian Snow,

a former technical director at the NSA, is the idea of *assurance* [34].

From the vantage point of the assurance school of thought, software is presumed suspect until it is shown to be otherwise. In other words, a vendor must make users (or an accreditor) sufficiently confident that their product is secure.

How does this happen? According to Snow, "We analyze the system at design time for potential problems that we then correct. We test prototype devices to see how well they perform under stress or when used in ways beyond the normal specification. Security acceptance testing not only exercises the product for its expected behavior given the expected environment and input sequences, but also tests the product with swings in the environment outside the specified bounds and with improper inputs that do not match the interface specification. We also test with proper inputs, but in an improper sequence. We anticipate malicious behavior and design to counter it, and then test the countermeasures for effectiveness.
We expect the product to behave safely, even if not properly, under any of these stresses. If it does not, we redesign it [35]."

Note the emphasis on the design phase. This is not something that get's tacked on at the end of the development cycle to appease marketing executives. Assurance work has to be a part of the process from the very beginning.

The assurance mindset also needs to be augmented by legislation. We need codified standards. Self-regulation has shown that it can't do the job. We need regulation for the same reason that we have automotive safety rules and building codes: the free market isn't capable of generating certain public goods. As Bruce Schneier noted, "Most software companies are short-term smart to ignore the cost of never-ending patching, even though it's long-term dumb [36]."

Perhaps if we hold software vendors liable for security holes they'll realize it's cheaper to get it right the first time?

Critics would argue that regulation wouldn't work because things change so quickly in hi-tech. As an engineer with over a decade of experience building software, I can tell you that this is an excuse promoted by business interests who are worried that regulation will impact their bottom line. The industry has the tools it needs; it's just a matter of using them [37].

Focusing on Immediate Risks

Despite the sound and fury generated by pundits, the risk associated with Cyberwar is dwarfed by the risks posed by cybercrime [38]. The people who warn us of Cyberwar don't like to mention this because it might diminish the urgency of their message. Cybercrime is everywhere, it happens on a routine basis. I'm talking about identity theft, credit card fraud, extortion, and espionage (just to name a few). This is the arena where we're suffering death by a thousand cuts.

The numbers aren't encouraging. The Internet Crime Complaint Center, a partnership between the FBI, Bureau of Justice Assistance, and the National White Collar Crime Center, registered 336,655 cybercrime incidents in 2009. The dollar

loss of these incidents was approximately $560 million [39].

The Defense Security Service publishes an annual report that compiles accounts of intelligence "collection attempts" and "suspicious contacts" identified by defense contractors who have access to classified information. According to the 2009 report, which covers data collected over the course of 2008, "commercial entities attempted to collect defense technology at a rate nearly double that of governmental or individual collector affiliations. This trend likely represents a purposeful attempt to make the contacts seem more innocuous, shifting focus from government collectors to commercial or non-traditional entities [40]."

Think about it, why would other countries want to destroy our information infrastructure when they can do much better by stealing our intellectual property? According to former KGB chairman Vladimir Kryuchkov, "Intelligence is probably the most profitable structure in the country. It pays its expenses with dividends. One single operation, concerning outer space, pumped 500 million dollars into our economy [41]."

The Media: An Institutional Analysis

How did we get here? What allowed all this Cyberwar fear and loathing to germinate in the first place? The best way to understand this is to study the channel through which this information gets to us: the media.

The first thing you need to realize is that news is big business. The larger media outlets, the agenda-setting organizations that have the resources to monitor events worldwide, are publicly traded mega-corporations. Take Rupert Murdoch's News Corporation, for instance. It employs 55,000 people [42] and has annual revenues on the order of $30 billion [43].

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 roughly 2 million papers every day [44] and, in 2009, its advertisement revenues were about $1.2 billion [45]. It goes without saying that the Wall Street Journal is making the bulk of its money from advertisers. 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 high-level decision makers. In other words, many of the people who read the Wall Street Journal also represent America's *political class.* According to ABC News, the average household income of the Wall Street Journal's subscriber in 2007 was approximately $235,000 [46].

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 ruling class. 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 [47].

The Fourth Branch of Government

Given their profit orientation and the demographics that they target, one way for media outlets to distinguish themselves (read: please their advertisers, and thus satisfy Wall Street investors) is to offer exclusive access to valuable information. The general tendency is for the media to turn to the government for this information. The more restricted and scarce this information is, the higher its value.

The basic mechanics of how the press accesses government secrets has been described in detail by Max Frankel, the Washington Bureau Chief of the New York Times. In 1971, when the United States Government was taking the New York Times to court over the release of the Pentagon Papers, Frankel gave a sworn deposition that clearly explained how those in power use secrecy and leaks as a form of currency when dealing with the media.

According to Frankel, "practically everything that our Government does, plans, thinks, hears and contemplates in the realms of foreign policy is stamped and treated as secret -- and then unraveled by that same Government, by the Congress and by the press in one continuing round of professional and social contacts and cooperative and competitive exchanges of information [48]."

This relationship creates a covert channel that allows public figures to convey information without official responsibility. Through this back channel, officials can enhance their budget, sabotage the plans of another department, test public response to a proposed policy, or to lobby against the agenda of their superiors.

To see this in action, all you have to do is scan the news for code phrases that refer to sources without actually providing their names. Specifically, a report might cite "senior administration officials [49]," "former officials [50]," or people "familiar with the investigation [51]."

Masters of the Art: The CIA

If secrets are the coin of the realm in DC, then the MVPs of the league in Washington are the intelligence agencies. Without a doubt, these guys have the deepest rabbit holes in the meadow.

The CIA's connections with the media are part of the public record. The Church Committee Report, published in 1976, stated that the CIA maintains "a network of several hundred foreign individuals around the world who provide intelligence for the CIA and at times attempt to influence foreign opinion through the use of covert propaganda. These individuals provide the CIA with direct access to a large number of foreign newspapers and periodicals, scores of press services and news agencies, radio and television stations, commercial book publishers, and other foreign media outlets [52]."

The CIA's influence doesn't seem to be limited to foreign sources. In 1977, one of the journalists who exposed the Watergate Scandal, Carl Bernstein, published a lengthy expose which revealed

that more than 400 American journalists were secretly carrying out assignments on behalf of the CIA [53]. Bernstein claims that "In the field, journalists were used to help recruit and handle foreigners as agents; to acquire and evaluate information, and to plant false information with officials of foreign governments."

Decades after Bernstein's article, the CIA is still busy manipulating public opinion. On March 11, 2010, Wikileaks.org released a classified CIA Red Cell memo detailing various public relations strategies to bolster support for the war in Afghanistan over in France and Germany [54]. The memo refers to specially tailored "messages" aimed at altering perceptions of NATO military action. The memo doesn't go into the operational details of how these messages would be conveyed, but if the Church Committee reports are any indication of how things are done it will probably be through the agency's extensive network of media contacts.

All of this raises disturbing questions. If our intelligence agencies have influence with the press in other countries, how do we know the same thing isn't happening over here? To what extent do CIA messages find their way into the American media? Have intelligence services from other countries developed ties with reporters here in the United States? Will we ever be able to tell just how much we're being controlled and by whom?

Epilogue

So there you have it: the various Cyberwar metaphors (e.g. "Digital Pearl Harbor," "Cyber Katrina," etc.) exist because institutions within the government are competing for funding and, more importantly, control of the Internet. Furthermore, the predictions of cybergeddon are allowed to exist because they suit the economic needs of certain news outlets.

The doomsayers use their connections with the media to spread their message, with the expectation that if they're careful then maybe it won't be too obvious as to why a certain unnamed official is making vague references to impending disasters. As Max Frankel noted, "The [public] official knows, if he wishes to preserve this valuable channel and outlet, to protect his credibility and the deeper purpose that he is trying to serve."

However, sometimes it is obvious; especially when the doomsayer in question happens to present readers with solutions that benefit both their friends in the government [55] and current employer [56].

The damning part of all this is the sheer hypocrisy of it all. The large agenda-setting members of the press have long-standing arrangements with government agencies, providing the means to manufacture consent, all the while presenting themselves to the public as strictly neutral observers. Like any skilled forensic investigator, we need to question what we're told, corroborate information independently, develop alternative sources of information, and always be on the lookout for subtle telltale signs of manipulation.

References

[1] http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[2] Marcelo Soares, “Brazilian Blackout Traced to Sooty Insulators, Not Hackers,” *Wired*, November 9, 2009, http://www.wired.com/threatlevel/2009/11/brazil_blackout/

[3] http://www.aneel.gov.br/cedoc/adsp2009278_1.pdf

[4] Kevin Poulsen, “Urban Legend Watch: Cyberwar Attack on U.S. Central Command,” *Wired*, March 31, 2010, http://www.wired.com/threatlevel/2010/03/urban-legend/

[5] John Markoff, “Do We Need a New Internet?” *New York Times*, February 15, 2009, http://www.nytimes.com/2009/02/15/weekinreview/15markoff.html

[6] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html

[7] Bruce Schneier, “New York and the Moscow Subway Bombing,” Schneier on Security, April 7, 2010, http://www.schneier.com/blog/archives/2010/04/new_york_and_th.html

[8] Mike McConnell, “Mike McConnell on how to win the cyber-war we're losing,” *Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[9] John Letzing, “Google Still Chasing Source Of Recent Cyberattacks,” *Wall Street Journal*, March 24, 2010, http://online.wsj.com/article/BT-CO-20100324-711806.html

[10] Siobhan Gorman, August Cole, And Yochi Dreazen, “Computer Spies Breach Fighter-Jet Project,” *Wall Street Journal*, April 23, 2009 http://online.wsj.com/article/SB124027491029837401.html

[11] Joe Nocera, “As Credit Crisis Spiraled, Alarm Led to Action,” *The New York Times*, October 1, 2008, http://www.nytimes.com/2008/10/02/business/02crisis.html

[12] Sheryl Gay Stolberg and Stephen Labaton, “Obama Calls Wall Street Bonuses ‘Shameful’,” The New York Times, January 30, 2009, http://www.nytimes.com/2009/01/30/business/30obama.html

[13] Christopher Drew and John Markoff, "Contractors Vie for Plum Work, Hacking for U.S.," *The New York Times*, May 3, 2009,
http://www.nytimes.com/2009/05/31/us/31cyber.html?_r=1

[14] *HB Gary Threat Report: Operation Aurora*, February 10, 2010
http://www.hbgary.com/wp-content/themes/blackhat/images/hbgthreatreport_aurora.pdf

[15] *Protecting Your Critical Assets: Lessons Learned from "Operation Aurora,"* McAfee Labs and McAfee Foundstone Professional Services,
http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

[16] Siobhan Gorman and Evan Ramstad, "Cyber Blitz Hits U.S., Korea," *Wall Street Journal*, July 9, 2009,
http://online.wsj.com/article/SB124701806176209691.html

[17] Kim Zetter, "Lawmaker Wants 'Show of Force' Against North Korea for Website Attacks," *Wired*, July 10, 2009,
http://www.wired.com/threatlevel/2009/07/show-of-force/

[18] http://blog.bkis.com/en/korea-and-us-ddos-attacks-the-attacking-source-located-in-united-kingdom/

[19] http://www.globaldigitalbroadcast.com/newspage.php?newsId=123

[20] Violet Cheung-Blunden, "Paving the Road to War with Group Membership, Appraisal Antecedents, and Anger," *Aggressive Behavior*, Volume 34 Issue 2, Pages 175 - 189

[21] Bruce Schneier, "So-Called Cyberattack was Overblown," *MPR News*, July 13, 2009,
http://minnesota.publicradio.org/display/web/2009/07/10/schneier/

[22] Shane Harris, "The Cyberwar Plan," *National Journal*, November 14, 2009,
http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php

[23] Martin C. LibiCki, *Cyberdeterrenceand Cyberwar*, RAND Corporation, 2009,
http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

[24] Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," *The Washington Post*, February 28, 2010,
http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[25] Ibid.

[26] Lawrence Wright, "The Spymaster: Can Mike McConnell fix America's intelligence community?" *The New Yorker*, January 21, 2008,
http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?printable=true

[27] Ryan Singel, "Law Enforcement Appliance Subverts SSL," *Wired*, March 24, 2010
http://www.wired.com/threatlevel/2010/03/packet-forensics/

[28] Martin C. LibiCki, *Cyberdeterrenceand Cyberwar*, RAND Corporation, 2009, page 176,
http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

[29] Elinor Mills, "Malware Delivered by Yahoo, Fox, Google Ads," *CNET News*, March 22, 2010,
http://news.cnet.com/8301-27080_3-20000898-245.html

[30] Kim Zetter, "'Google' Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010,
http://www.wired.com/threatlevel/2010/03/source-code-hacks/

[31] Richard Bejtlich, "Forget ROI and Risk. Consider Competitive Advantage," March 21, 2010,
http://taosecurity.blogspot.com/2010/03/forget-roi-and-risk-consider.html

[32] Elinor Mills, "Microsoft, Google split over browser bug bounty," *CNET News*, February 9, 2010,
http://news.cnet.com/8301-27080_3-10449661-245.html?tag=mncol;title

[33] Elinor Mills, "iPhone, Safari, IE 8, Firefox hacked in CanSecWest contest," *CNET News*, March 24, 2010,
http://news.cnet.com/8301-27080_3-20001126-245.html?tag=mncol;title

[34] Brian Snow, "We Need Assurance!" 2005 Annual Computer Security Applications Conference
http://www.acsac.org/2005/papers/Snow.pdf

[35] Ibid.

[36] Bruce Schneier, "E-Voting Certification Gets Security Completely Backward," *Wired*, August 9, 2007
http://www.wired.com/politics/security/commentary/securitymatters/2007/08/securitymatters_0809

[37] John Viega and Gary McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way*, Addison Wesley, 2001, ISBN-10: 020172152X

[38] John Mueller and Mark G. Stewart, "Hardly Existential," Foreign Affairs, April 2, 2010,
http://www.foreignaffairs.com/print/66156?page=show

[39] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

[40] http://dssa.dss.mil/counterintel/2009/index.html

[41] Robert Eringer, *Ruse: Undercover with FBI Counterintelligence*, Potomac Books, 2008, ISBN-10: 1597971898

[42] http://www.google.com/finance?q=NWS

[43] http://www.sec.gov/Archives/edgar/data/1308161/000119312509172310/d10k.htm

[44] http://www.accessabc.com/products/freereports.htm

[45] Trefis, "What the Wall Street Journal Is Worth to News Corp.," *Forbes.com*, April 14, 2010, http://blogs.forbes.com/greatspeculations/author/trefis/

[46] Scott Mayerowitz, "What Do the Rich and Powerful Read?" *ABC News*, July 28, 2007

[47] Edward Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, Pantheon, 2002, ISBN-10: 0375714499

[48] http://www.pbs.org/wgbh/pages/frontline/newswar/part1/frankel.html

[49] Robert Novak, "Mission To Niger," *The Washington Post*, July 14, 2003, http://www.washingtonpost.com/wp-dyn/content/article/2005/10/20/AR2005102000874.html

[50] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005

[51] Siobhan Gorman and Jessica Vascellaro, "Google Attack Linked to Asian Hackers," *The Wall Street Journal*, February 23, 2010, http://online.wsj.com/article/SB10001424052748704751304575080362745174130.html

[52] Select Committee to Study Government Operations with Respect to Intelligence Activities, *Book I: Foreign and Military Intelligence*, U.S. Government Printing Office, 1976, page 192 http://www.aarclibrary.org/publib/church/reports/book1/html/ChurchB1_0100b.htm

[53] Carl Bernstein, "The CIA and the Media," *Rolling Stone*, October 20, 1977, http://www.carlbernstein.com/magazine_cia_and_media.php

[54] http://file.wikileaks.org/file/cia-afghanistan.pdf

[55] Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," *The Washington Post*, February 28, 2010,

http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[56] Ryan Singel, "Cyberwar Doomsayer Lands $34 Million in Government Cyberwar Contracts," *Wired*, April 13, 2010,
http://www.wired.com/threatlevel/2010/04/booz-allen/