Staring into the Abyss:
The Dark Side of Crime Fighting, Security, and Professional Intelligence

Notes and Comments

WHY SECURITY SUCKS

As of 2010, Frost & Sullivan estimates that there are 2.28 million information security professionals worldwide.

to which an experienced security practitioner replied**:**

“it sounds better if you make air quotes when you say information security professionals.”

THE SITUATION

We are all in this together. all hacking and all hackers are gray hat.

a black hat hacker is a hacker.
a gray hat hacker is a hacker who knows when to fudge the truth.
a white hat hacker is a hacker who put the truth down somewhere and can’t remember where he left it.

the world is gray. hacking is a subset of the world. therefore, hacking is gray.

Those who define a paradigm do not need to worry about answers, because they determine the questions that can be asked. They know the size and shape of the picture because they create the frame.

Years ago I referred to “real birds kin digital cages.” Now I would say, “real flocks of birds in digital cages.” The simulated beating wings above and below and on both sides provide an illusion of security, being part of the herd, the team, the tribe, and our own beating wings provide an illusion of the freedom of flight. But the cage slowly turns and positions us where it will.

We are all assimilated. The Borg-R-Us.

Margaret Mead , noted anthropologist, said it takes a full year to learn how to see what she learns in the first week in a new culture because she is assimilated so quickly and unconsciously into the culture. The frames of her perceptual lenses are immediately recontextualized by the cues, however exotic, in response to her statements.

In any organizational culture, we learn how to behave according to known but unwritten rules. The written rules, known only when we scan the thick book given to new hires, soon become written and unknown as they gather dust on the shelf in our cubicles.

(there are four kinds of rules: known and written, unknown and written, unknown and unwritten, and known and unwritten. The known and unwritten rules one had better learn or one won't last.

These rules define team players and whistle blowers. They define us and them. They define Team America, the tribe, our side, and all of the other ways we make a less than absolute good or value seem like an absolute good or value. We do that through agreement, reinforcement, a deeply embedded fear of consequences and reprisals, legal agreements, in short, everything that makes a seriously spiritual or religious human who takes a moral code seriously = an investigative reporter, if he or she speaks = a terrorist. Penalties escalate as The Powers categorize not the behavior, which is self-similar across those categories, but the alleged intention and allegiance of the speaker, who becomes a perp.

"The weakest link in the chain is frequently the definition of the problem, and the definition of the problem is often not what we think" – Matt Blaze

Who are we, then, really? What is the "security space" – really? What does our self-referential narrative about the "industry" include and what does it EXCLUDE? What is the rule-base of the filter and how well does it work at the perimeter?

Where have we put the truth? and what really is it?

Nothing is harder to see than things we believe so deeply we don't even see them. This is true in the "security space," in which our narratives are self-referential, bounded by mutual self-interest, and characterized by a heavy dose of group-think. It is true that, "if everyone is thinking the same thing, someone isn't thinking," and it is also true that one is not always rewarded for original far-seeing insight. In fact, the contrary.

My story: how do you change the paradigm? one way or another, you have to leave.

Timothy Leary: "You never get the truth from the company memo." Your individual identity, the boundary around it flexing and blurring, is absorbed into the corporate identity, and the more success you achieve in a particular culture, the more – when you open your mouth to speak – you articulate an instantiation of the Myth, the company line, the simple cover story many have come to believe. Think "Invasion of the Body Snatchers" when someone you think you know opens their mouth and outcomes not familiar speech but an alien ululation. That movie has been remade and remade again because it ports the truth of McCarthyism, to which it first referred, into our current context.

THE RESULT

Analysis of deeper political and economic structures reveals behaviors and beliefs in a different light which illuminates mixed motives and the fact that legitimate and illegitimate enterprises interpenetrate one another deeply, yin-yangishly, the overworld and the underworld making up one vanilla-and-chocolate swirl of pudding, one complex system, one planetary economy and society.

There is also an serious impact on security and intelligence practitioners – on psyches, relationships, lives – when work brings one constantly up against the abrasive interface of those mixed motives. Cognitive dissonance is always present and the least of our worries, unless it leads to serious emotional stress.

Twelve-step programs as a model promise regeneration of our deepest being and say, “we are only as sick as our secrets.” But life in the national security state, the security space, the intelligence “community” which permeates all meaningful communities - is founded on secrecy millions of secrets, millions of classified documents, hundreds of thousands of compartmented worlds.

“I am getting more and more cynical all the time and I still can’t keep up.” – Jane Wagner.

What does it do to a human being to live with often-frightening secrets – frightening because they confront us with the truth of ourselves and the myth of righteousness can no longer be sustained? Here is one story ... [insert story of Washington DC dinner].

THE INTENTION BEHIND THIS PRESENTATION

This analysis will hopefully make you think twice before uncritically using the buzzwords and jargon of the security profession - words like "security" itself, and "defense," and "cyberwar," and “terrorism,” and “the enemy.”

By the end of this presentation, simplistic distinctions between foreign and domestic and us and them will go liquid while the complexities of information security remain, bounded by a perimeter which has cased to be a perimeter, which is more like a moebius strip suggesting that the inside and the outside are really one thing. Niels Bohr said, “if quantum mechanics hasn’t shocked you, you haven’t understood it yet.” In a similar way, anyone doing security or intelligence work who does not experience cognitive dissonance has lost touch with the points of reference for his or her humanity – and the real big picture in which we are all actors, inside the frame.

One example:

Security Pros May Be Ready To Crack Under Growing Pressure, Study Says

Faced with securing personal devices and a growing base of threats, security pros feel overwhelmed, (ISC)2 survey reports

Feb 23, 2011

By Tim Wilson
Darkreading

Faced with an attack surface that seems to be growing at an overwhelming rate, many security professionals are beginning to wonder whether their jobs are too much for them, according to a study published last week.

Conducted by Frost & Sullivan, the 2011 (ISC)2 Global Information Security Workforce Study (GISWS) says new threats stemming from mobile devices, the cloud, social networking, and insecure applications have led to "information security professionals being stretched thin, and like a series of small leaks in a dam, the current overworked workforce may be showing signs of strain."

"In the modern organization, end users are dictating IT priorities by bringing technology to the enterprise rather than the other way around," said Robert Ayoub, global program director for network security at Frost & Sullivan. "Pressure to secure too much and the resulting skills gap are creating risk for organizations worldwide ... They are being asked to do too much, with little time left to enhance their skills to meet the latest security threats and business demands."

As of 2010, Frost & Sullivan estimates that there are 2.28 million information security professionals worldwide. Demand for professionals is expected to increase to nearly 4.2 million by 2015, with a compound annual growth rate of 13.2 percent.

Application vulnerabilities ranked as the No. 1 threat to organizations among 72 percent of respondents, while only 20 percent said they are involved in secure software development.

Nearly 70 percent of respondents reported having policies and technology in place to meet the security challenges of mobile devices, yet mobile devices were still ranked second on the list of highest concerns by respondents. The study concludes that "mobile security could be the single most dangerous threat to organizations for the foreseeable future."

Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security. More than 50 percent of respondents reported having private clouds in place, while more than 70 percent reported the need for new skills to properly secure cloud-based technologies.

Most security pros aren't ready for social media threats. Respondents reported inconsistent policies and protection for end users visiting social media sites, and nearly 30 percent had no social media security policies whatsoever.

The main drivers for the continued growth of the profession are regulatory compliance demands, greater potential for data loss via mobile devices and mobile workforce, and the potential loss of control as organizations shift data to cloud-based services, the study says.

Nearly two-thirds of respondents don't expect to see any increase in budget for information security personnel and training in 2011. Salaries showed healthy growth, with three out of five respondents reported receiving a salary increase in 2010.

When Nietzsche said, "Whoever battles monsters should take care not to become a monster too, For if you stare long enough into the Abyss, the Abyss stares also into you." (Nietzsche, Beyond Good and Evil, chapter 4, no. 146) he was warning us that becoming more fully aware has consequences. As a sign in Sandia National Lab's Physics Department says: "Do not look directly into the laser beam with your remaining eye."

So this presentation is not one of those talks that gives you 3 things to do at the office in the morning. Ideally it will echo in the weeks and months ahead when you find yourselves in situations which recall it The purpose is to reflect on who we are, not by looking at what we assert, but by observing our behavior – the same way we establish identity off and online - so we can be more effective both as practitioners of our arts and crafts and also as more fully human beings. Ideally we will think realistically about our work and lives in the context of the political and economic realities of the security profession, professional intelligence and how it permeates work and life, and global meta-national corporate structures which are the source of political decisions and economic consequences, rather than explanations rooted in paradigms of the 20th century which were shaped by prior technologies.

Here is an outline:

- what we think we think
- what we really think, based on what we do
- political and economic analysis reveals a different world than the one we pretend to inhabit
-competitive intelligence and nation-state intelligence blur in this world, altering the context of security and ethical considerations of our actions which have also radically changed as a result of technologies
- the intelligence world since 1947, since 9/11, since before your birth – has exploded
- global corporate structures such as banking and financial services and how they work
- vendors and the security space
- what security professionals, chatting at the digital water cooler, really think

- real threats
- interpenetration of the intelligence community, the security world, and meta-national corporations
- clipper revisited. why clipper? who was really the worrisome threat?
- the yin/yang of official (law and order) and unofficial (criminal) enterprises
- whistle blowing, accounting, real structures of mutuality feedback and accountability
- how to build those structures in "functional networks" – thinking about AA and the like
- the real tasks and challenges of security
    - things are not always what they seem, but they are always what they are

"Reality is that which, when you stop believing in it, refuses to go away." – P. K. Dick

THINKING ABOUT SECURITY

Discussions of security and the security industry often focus on statements about "security." This duh-sounding remark suggests a condition of primary naiveté, which is like reading for example the Bible in a literalist way, as if all statements are the same kind, devoid of historical context, outside time, space, genres, and culture – outside the context that gives them meaning, in other words, particular meanings at that, which meanings include sociological, psychological, economic, political, and cultural dimensions.

Security has a context. Turning context into content, i.e. illuminating the slightly bigger box inside which we hope to find ourselves with "out of the box thinking," gives mastery over not only security, but life, the universe, everything.

Eddie Bernays and his work is a good example of how this happens. Torches of Freedom. Bookcases and books. Guatemala and the overthrow of Arbenz.

We still have beliefs, in other words, but we do not BELIEVE in our beliefs in the same way. We contextualize them differently. We understand, we hold them differently. And that does not always happens at security conferences where the rhetoric reinforces the narrative that includes sales pitches, marketing brochures, and both bunnies handing out chocolates.

Cultural studies of media, to which I will refer a little, are about beliefs, the management of perception in the mind of society. One might say that the world divides into people who believe in their beliefs in a primary naive way – and those who don't.

Security in the real world is about – what works? Why do we bow at the Zen Center? a monk asked his audience. We bow because things seem to work better when we bow

That is practical spirituality, and applies to work and life alike. What are those things, the doing of which makes things work better, when we do them?

So this is an attempt to put what we hear at conferences - like this one - into context, the social, economic, or political dimensions of security **and how those affect our behavior**

and what we say. We may still make the same claims, but ... we will not believe in them in the same way. We will hear ourselves say them and quietly critique our own blather, if only inside our heads..

There is a way to hold all of this and not get all arrogant, superior, or smarmy about it. We are all merely human. No one has the high moral ground. We all swim in the same water, as Jake Gittes said in "Chinatown. "Our real challenge is to be willing to be human, to be enthusiastically and robustly human, not less than human.

Not the Borg.

THE DARK SIDE

James Baldwin said, "The price one pays for pursuing any profession or calling is an intimate knowledge of its ugly side."

If we do not know that ugly side, we do not know the profession - or ourselves. The price we pay for self-awareness is an intimate knowledge of our ugly sides, too. So another title for this talk is: **know yourself**.

One place to look is the exploration of **deep politics, e.g.** Peter Dale Scott, " Deep Politics and the Death of JFK." There is an important "distinction between traditional conspiracy theory, conscious secret collaborations toward shared ends, and deep political analysis, the study of all those practices and arrangements, deliberate or not, which are usually repressed rather than acknowledged. In the latter, there is an open system with divergent power centers and goals, not a single objective or control point."

But more than that, a deep political system or process habitually resorts to decision-making and enforcement procedures outside as well as inside those publicly sanctioned by law and society. They are "**covert and suppressed, outside general awareness as well as outside acknowledged political processes."**

An example: criminal structures are often tolerated by police because of their usefulness for informing on lesser criminals. See e.g. the Whitey Bulger file. The same is true re: the intelligence community. In Chicago, e.g., there is a police-criminal symbiosis and the mob controls more than the police department it has corrupted. It controls civic life, its economic political and social underpinnings. Its depth and persistence creates the frame.

Next: as a result of morphing geopolitical structures into what we now call meta-national stage-managed globalism, Competitive Intelligence and "economic patriotism" are indistinguishable from state-based intelligence operations. When Jan Hering moved from the CIA to Motorola, it was a marker – first of what trans-nationals had become, then what meta-nationals would become.

.

I keynoted twice for a Microsoft Israel conference and shared the platform with Steve Ballmer. My job was to enhance his credibility when he spoke about taking security seriously, at long last, because the market and changing global conditions required it. Now, Bill Gates is no worse than Larry Ellison or Scott McNealy or Steve Jobs – to achieve the positions of any of them, you had better be a robber baron and use all means necessary to secure intellectual property from taking the property to taking the human head that knows the details, using the whole repertoire of techniques used by the IC

For one example of how low one can limbo, see recent revelations of the Murdoch caper, imagine much more, then know that you can't begin to imagine what they do. Or ... perhaps you can. If it is your work, too.

The nature of intelligence work has been changed by evolving technologies.

In my presentation for the New Paradigms in Security Workshop, **CHANGING CONTEXTS OF SECURITY AND ETHICS: YOU CAN'T HAVE ONE WITHOUT THE OTHER (NPSW 2008),** I said:

"Information security as one task, both offensive and defensive, of the intelligence community sanctions breaking foreign laws while prohibiting similar activities on American soil. But simple distinctions of "foreign" and "domestic" no longer hold. The convergence of enabling technologies of intrusion, interception, and panoptic reach, combined with a sense of urgency about the counter terror imperative and a clear mandate from our leaders to do everything possible to defeat an amorphous non-state entity defined by behaviors rather than boundaries, borders, or even a clear ideological allegiance, has created an ominous but invisible and seemingly inevitable set of conditions that undermine previous cornerstones of law, ethics, even religious traditions.

therefore: ***Security professionals exercise an implicit, de facto thought leadership because they create structures that bind and inform society and civilization.*** **Their real implicit charge is not "to defend and protect a nation" but to stabilize a world.**

The dire possibility of societal disintegration elevates the moral responsibility of the security and intelligence communities to a higher level. Linked in cooperative activity, they are responsible for maintaining social and global order at a level of understanding far beyond that formulated in the past by any one nation. These communities in the aggregate constitute a global community of practitioners who share an ethos and modalities of operation not available to ordinary citizens; they have thereby created for themselves an intrinsic vocation or calling to maintain global order *in a way that is consistent with the ethical norms and moral order articulated by the great cultural traditions even as those traditions are also transformed by diverse technologies—and even though they and we recognize that in practice that moral order and those ethical norm are often violated as a matter of practice.*

A primary goal of security and intelligence work, as it is practiced, is to tell people that the world in which they will wake up will be pretty much the world in which they fell asleep.

IOW, stability, persistence of structures even as they morph, continuity of identities (even as they morph) – the same work as that done by the human organism, in effect, as it has evolved, managing cellular changes, environmental disruptions, and genetic mutations.

Next: we do this in the context of a world within the world, a secretive world if not a secret world, which since 9/11 has grown and grown ... and grown ...

Dana Priest and William Arkin wrote in the Washington Post, 7/19/2010 – of a hidden world, growing beyond control – "**The top-secret world the government created in response to the terrorist attacks of Sept. 11, 2001, has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work.**

*** 1,271 government organizations and 1,931 private companies work on programs related to counter terrorism, homeland security and intelligence in 10,000 locations across the United States.**

*** 854,000 people, nearly 1.5 times as many people as live in Washington, D.C., hold top-secret security clearances.**

* In Washington and the surrounding area, **33 building complexes for top-secret intelligence work are under construction or have been built since September 2001**. They occupy the equivalent of three Pentagons or 22 U.S. Capitol buildings - 17 million square feet of space.

*** Many security and intelligence agencies do the same work,** creating redundancy and waste. For example, 51 federal organizations and military commands, operating in 15 U.S. cities, track the flow of money to and from terrorist networks.

Analysts who make sense of documents and conversations obtained by foreign and domestic spying publish **50,000 intelligence reports each year, a volume so large that many are routinely ignored.**

As a corollary, read my short story, *Break, Memory*, in "Mind Games," which illuminates how the masters of society manage the humplings – the 80% in the hump of the bell curve – and maintain the dregs as an example to the humplings. They do this in a world of increasing longevity by distributing memories throughout the population so all the memories are there, but only they have the algorithms and keys to the code for recovery and reassembly, thereby preventing older wiser people (silverbacks, we call ourselves) from talking to one another about relevant events and building the Big Picture.

In addition - recent US political discourse is about how much money must be cut by the government – but wars and empire and the big money for "defense" (fighting in Iraq, Iran, Afghanistan, Yemen, Somalia etc.) are seldom discussed.

"For the 2010 fiscal year, the president's base budget of the Department of Defense rose to $533.8 billion. Adding spending on "overseas contingency operations" brings the sum to $663.8 billion. When the budget was signed into law on October 28, 2009, the final size of the DoD's budget was $680 billion, $16 billion more than President Obama had requested. Defense-related expenditures outside DoD constitute $216 billion - $361 billion in additional spending, bringing **total defense spending to $880 billion - $1.03 trillion** in fiscal 2010

The U.S. DoD budget accounted in fiscal 2010 for 19% of the US federal budgeted expenditures and 28% of estimated tax revenues. Including non-DOD expenditures, defense spending was **approximately 25–29% of budgeted expenditures and 38–44% of estimated tax revenues.** According to the Congressional Budget Office. defense spending grew 9% annually on average from fiscal year 2000–2009."

A friend recalled a conversation with the late great **Bob Abbot.** My friend said: "Ahhh... I get it, you're a spy." Abbot corrected me and said, "**no, spies *work* for me**...".

THE LESSON YOU CAN NOT SEPARATE SECURITY FROM THE VAST DARK CAVE IN WHICH IS TAKES PLACE, THE WORLD OF BLACK AND GRAY OPERATIONS, MILITARY AND INTELLIGENCE WORK, A WORLD WITHIN THE WORLD, WITH MASSIVE ENGINES OF FUNDING AND THEREFORE DIRECTION OF THE MILITARY-INDUSTRIAL-ENTERTAINMENT-MEDIA-EDUCATIONAL COMPLEX.

In this context, let's discuss INFORMATION SECURITY.

First, "vendor-space." (all of these quotes and subsequent quotes are from friends chatting about their work. They are anonymized to protect the innocent and guilty. They are spontaneous and based on long experience, and you can recognize I hope that they are "what's so."

What is the security business? It is what it is.

An example from vendorspace:

We deal with vendors every day. The vendor is brought to us by an enterprise that is licensing code from the vendor either to deploy internally, use in software they are building, or bundle. We analyze their code. There is typically resistance from the vendor to send their code to us that ranges from, "this is a pain in the ass but I guess I have to make my sale" to "I am going to complain and drag my feet, threaten things but give in with some small concessions" to "no way, I am the big cheese, I am not going to let you have a 3rd party assessment". Where a vendor falls along this spectrum parallels the

economic leverage the enterprise customer has over the vendor. If the enterprise is the size of a Barclays or a Dell and the vendor is small, the vendor capitulates quickly. If the vendor and customer are the same size (think midsize bank and big Indian outsourcer) then there is more hemming and hawing but the vendor eventually gives in. If the vendor is huge and the customer is smaller than the US govt the vendor says no since they have market power. This is sort of like the US not going along with international treaties. **They don't go along because they can get away with it.**

Let's port a metaphor from the world of cyber security to the social political world:

"You do not know what assumptions the system is making,." says a security expert retired from CIA. "**What assumptions are implicit in the architecture of the system?** You can not query the system about assumptions, hence you can't query it to reveal its flaws (or back doors.). The system is not self-aware. What does the system think it knows that it may not know? People who build systems do not understand that principle."

OR THEY DO UNDERSTAND IT AND MAKE USE OF IT

"The environment in which the logic is running is simply an unknown from a security standpoint. This means the environment needs to be audited too. It is not a good idea to use new environments for security critical code. When PHP came out people rushed to it because it was easy to use but look at all the problems that came down the road."

W**e're talking about nested levels of unconscious assumptions about the security industry, the security enterprise .... security, period, as a "mind space" that is leveraged for economic, political, and social advantage.**

The internet was built on an "US" model. It was built for trust and ease of access. The context of security is predicated on an us/them model – us is good, them is bad. Us is safety, them is threat. But as Pogo said, we have met the enemy and it is **us.**

In this context, what does the word "security" really mean?

A security expert with decades of experience surveyed that vendor expo floor out there – vendorspace - a couple of years ago and said: **"every single one is selling something that can't do what they claim, which is protect the enterprise."**

An editor of a national publication replied, when I suggested a particular application was built on smoke and mirrors: "Our entire industry is based on smoke and mirrors."

Ten years ago Neal Stephenson made this point at CFP about code: Without a sociopolitical context, cryptography is not going to protect you. R**elying on an encryption scheme is like trying to protect your house with a fence consisting of a single, very tall picket**. (his slide shows a lone picket rising into the sky, a bird considering it with bulging eyes.)

We identify the threats that we can fight, not the threats we cannot fight.
"cryptography is the opiate of the naive."

A noted cryptographer told Peter Neumann that the crypto built into a particular voting machine was solid. Neumann acknowledged that but pointed out that the voting machine in question was compromised: the system was broken. That's not my problem, said the cryptographer, turning it into what economists call "an externality," i.e. kicking the consequences down the road..

Another colleague said: "Security vendors sell "solutions" that address our fears, real or imaginary, and tools that can do what they can do and not what they can't do. AV does not stop at least 20%. Once you are owned you are owned. Making security powerful and invisible to the user is not the first imperative.″

And another said: I remember X laughing at the ATM and other embedded device code he was looking at because it was so simple and easy to exploit, in my non-expert opinion I would say that the cell phone stuff is even easier."

To which another said: "Mobile device security implementations currently suck more ass than the abomination that we call mainstream software."

AND THIS IS ALL HAPPENING INSIDE THE DARK CAVE

Where the intelligence community, security-world, and meta-national corporations cooperate in behaviors mandated by definitions of success (political, economic, social) in which they have become complicit. But what does it have to do with ... "security?"

As one noted: if warrantless tapping of the phone system and internet is OK and can be secret, what assurances can Google give us that they aren't the NSA's largest database. Why bother with SSL to connect to gmail and google apps when the backend can be queried by NSA?

And warrantless wiretapping of Americans IS ok, according to Gen. Michael Hayden. When asked if there might be ethical or legal issues around intercepting the communications of Americans without court warrants, Hayden said, no, because **"we have the power."**

Building the information systems we have built is permission for using them to do whatever they can be used to do, by anyone and everyone, regardless of the intention of the builders. Attribution of an attack in cyberspace is child's play compared to attribution of moral and legal responsibility for building a system so complex that no one can possibly understand it (see the financial system for another example). If everybody does it, then nobody does it. Collusion between Murdochians, politicians and police was not a problem until ANOTHER POINT OF REFERENCE EMERGED that challenged their collusion.

Identifying that point of reference is one theme of this presentation.

Dan Geer: The financial world has proven by demonstration that we humans are abundantly capable of building systems we can neither then understand nor control. The digital world is insisting on a second round of proof. Just as the greatest enemy of our personal health is ubiquitous cheap food, the greatest enemy of our national health is ubiquitous cheap interconnectivity.

A senior information practitioner said, after a long discussion years ago with a ranking FBI gent:

Your choice is not Big Brother or no Big Brother. Your choice is one Big Brother or many Little Brothers.
Think carefully before you choose.

Clipper chip was motivated for some as much by a fear of the FBI as it was a means to enable panoptic surveillance. And for a reason: COINTELPRO 2.0 is currently in full swing.

Report Prepared by the Electronic Frontier Foundation - January 2011

EXECUTIVE SUMMARY

In a review of nearly 2,500 pages of documents released by the Federal Bureau of Investigation as a result of litigation under the Freedom of Information Act, EFF uncovered alarming trends in the Bureau's intelligence investigation practices. The documents consist of reports made by the FBI to the Intelligence Oversight Board of violations committed during intelligence investigations from 2001 to 2008. The documents suggest that FBI intelligence investigations have compromised the civil liberties of American citizens far more frequently, and to a greater extent, than was previously assumed. In particular, EFF's analysis provides new insight into
:

Number of Violations Committed by the FBI

• From 2001 to 2008, the FBI reported to the IOB approximately 800 violations of laws, Executive Orders, or other regulations governing intelligence investigations, although this number likely significantly under-represents the number of

violations that actually occurred.

• From 2001 to 2008, the FBI investigated, at minimum, 7000 potential violations of laws, Executive Orders, or other regulations governing intelligence investigations.

• Based on the proportion of violations reported to the IOB and the FBI's own statements regarding the number of NSL violations that occurred, the actual number of possible violations that may have occurred in the nine years since 9/11 could approach 40,000 violations of law, Executive Order, or other regulations governing intelligence investigations

Substantial Delays in the Intelligence Oversight Process

• From 2001 to 2008, both FBI and IOB oversight of intelligence activities was delayed and likely ineffectual; on average, 2.5 years elapsed between a violation's occurrence and its eventual reporting to the IOB.

Type and Frequency of FBI Intelligence Violations

• From 2001 to 2008, of the nearly 800 violations reported to the IOB:
o over one-third involved FBI violation of rules governing internal oversight of intelligence investigations.
o nearly one-third involved FBI abuse, misuse, or careless use of the Bureau's National Security Letter authority.
o almost one-fifth involved an FBI violation of the Constitution, the Foreign Intelligence Surveillance Act, or other laws governing criminal investigations or intelligence gathering activities.

• From 2001 to 2008, in nearly half of all NSL violations, third-parties to whom NSLs were issued — phone companies, internet service providers, financial institutions, and credit agencies —contributed in some way to the FBI's unauthorized receipt of personal information.

• From 2001 to 2008, the FBI engaged in a number of flagrant legal violations, including:
o submitting false or inaccurate declarations to courts.
o using improper evidence to obtain federal grand jury subpoenas.
o accessing password protected documents without a warrant.

For further information, contact Mark Rumold, mark@eff.org, or Jennifer Lynch, jen@eff.org.

WE ARE NOT ALONE IN FINDING OURSELVES IN THIS KETTLE OF FISH:

The overworld and the underworld ARE the yin yang of reality. The sociologist Emile **Durkheim**'s views on crime were a departure from conventional notions. He believed that **crime is "bound up with the fundamental conditions of all social life and serves a social function.** He stated that crime implies, "not only that the way remains open to necessary change, but that in certain cases it directly proposes these changes... crime [can thus be] a useful prelude to reforms." In this sense he saw crime as being able to release certain social tensions and so have a cleansing or purging effect in society. **... To make progress, individual originality must be able to express itself...[even] the originality of the criminal...** " (1895).

Durkheim recognized deviance as important to the well-being of society and proposed that challenges to established moral and legal laws (deviance and crime, respectively) acted to unify the law-abiding. Recognition and punishment of crimes is, in effect, the very reaffirmation of the laws and moral boundaries of a society. The existence of laws and the strength thereof are upheld by members of a society when violations are recognized, discussed, and dealt with either by legal punishment (jail, fines, execution) or by social punishment (shame, exile).

Crime actually produces social solidarity, rather than weakens it. Durkheim also proposed that crime and deviance brought people in a society together. When a law is violated, especially within small communities, everyone talks about it. Meetings are sometimes held, articles are written for local news publications, and in general, a social community bristles with activity when a norm is broken. As is most often the case, a violation incites the non-violators (society as a whole) to cling together in opposition to the violation, reaffirming that society's bond and its adherence to certain norms.

A third idea Durkheim held was that deviance and crime also help to promote social change. While most violations of norms are greeted with opposition by the masses, others are sometimes not, and those violations that gain support often are re-examined by that society. Often, those activities that once were considered deviant, are reconsidered and become part of the norms, simply because they gained support by a large portion of the society. In sum, deviance can help a society to rethink its boundaries, and move toward social change, hopefully for the greater benefit of the group.

Durkheim on Crime

"There is no society that is not confronted with the problem of criminality. Its form changes; the acts thus characterized are not the same everywhere; but, everywhere and always, there have been men who have behaved in such a way as to draw upon themselves penal repression. There is, then, no phenomenon that represents more indisputably all the symptoms of normality, since it appears closely connected with the conditions of all collective life."
(1963, p. 62 [excerpt from *The Rules of the Sociological Method*])

"...We must not say that an action shocks the *conscience collective* because it is criminal,

but rather that it is criminal because it shocks the *conscience collective*. We do not condemn it because it is a crime, but it is a crime because we condemn it."
(1972, p. 123-124 [excerpt from *The Division of Labor in Society*])]

"Contrary to current ideas, the criminal no longer seems a totally unsociable being, a sort of parasitic element, a strange and inassimilable body, introduced into the midst of society. On the contrary, he plays a definite role in social life. Crime, for its part, must no longer be conceived as an evil that cannot be too much suppressed."
(1963, p. 63 [excerpt from *The Rules of the Sociological Method*])

You see THE IMPLICATION: WE are in collusion with criminals on behalf of the FUNCTIONING of society as is, as it will.

Example: extortion is a cost of doing business – but don't kill the cow or no one can get milk. That is the danger of asymmetric power: nation states might not accept the consequences a small cadre of bad actors are willing to accept, including their own deaths, in order to attack the most wired/wireless society on earth.

Growing up in Chicago helped me understand this. Working for an alderman through my college years, I was never once asked to do something that was legal on his behalf.

Example:: FBI taking a hacker and having him hack, recording it, telling him he broke the law (although on their behalf) and now they own him: CONTROL

They do not call someone who runs agents a control for no reason. LBJ said, trust is when you've got him by the balls.

The web is extensive, dark, and pervasive:

Example: **price fixing and air cargo companies**: WSJ Nov 8 2010: Air France-KLM Face EUR150M-EUR250M Cargo Price Fixing Fine

PARIS (Dow Jones)--**Franco-Dutch airline Air France KLM (AF.FR) faces a new EUR150 million to EUR250 million fine Tuesday when the European Commission releases its verdict on an alleged air cargo cartel, French daily Les Echos Monday reports without citing its sources.**

Air France-KLM, which provisioned EUR530 million for the case in 2007-2008, has already paid EUR258.7 million in fines in the U.S., Canada and Australia for the same affair, Les Echos said.

Tuesday, it could be fined another EUR150 million to EUR250 million, the newspaper reported, without citing sources.

Air France-KLM and several other airlines have been accused of fixing prices since 2000, by making deals among themselves over surcharges they imposed to offset increases in fuel costs, and in the cost of additional anti terrorism measures, as well as extra war-risk insurance premiums following the outbreak of war in Iraq in 2003.

The commission can penalize companies as much as 10% of their annual global sales if they find evidence of price-fixing.

Air France-KLM denied to comment on the report Monday. "Brussels has not yet taken a decision," a spokeswoman told Dow Jones Newswires, without even confirming a decision is due Tuesday.

The interpenetration of the overworld and underworld is most obvious in practices of **money laundering and banking.**

Which enterprises are cited as being in the forefront of information security? Financial institutions. They are therefore identified with SECURITY. but ... if they are fostering conditions of radical insecurity in the world ... then we are in the position of, for example, the Army counter-intelligence agent sent to Haiti in the 90s to interdict drugs, who found out ... he told me ... that a presidential colleague was coming down to make sure the route remained OPEN**.** [CIA agent Michel-Joseph Francois, a Haitian police chief, indicted for smuggling 33 tons of heroin and cocaine. “Haiti’s corrupt officials protected about 50 tons of cocaine/year that transited to the US in the early 1990s.” (“Cocaine Politics” by Peter Dale Scott and Jonathan Marshall)]

US Bank Money Laundering -
Enormous By Any Measure
By James Petras
Professor of Sociology, Binghamton University

There is a consensus among U.S. Congressional Investigators, former bankers and international banking experts that **U.S. and European banks launder between $500 billion and $1 trillion of dirty money each year, half of which is laundered by U.S. banks alone. As Senator Carl Levin summarizes the record: "Estimates are that $500 billion to $1 trillion of international criminal proceeds are moved internationally and deposited into bank accounts annually. It is estimated that half of that money comes to the United States".**

Over a decade then, **between $2.5 and $5 trillion criminal proceeds have been laundered by U.S. banks and circulated in the U.S. financial circuits**. Senator Levin's statement however, only covers criminal proceeds, according to U.S. laws. It does not include illegal transfers and capital flows from corrupt political leaders, or tax evasion by overseas businesses. **A leading U.S. scholar who is an expert on international finance associated with the prestigious Brookings Institute estimates "the flow of corrupt money out of developing (Third World) and transitional (ex-Communist) economies**

into Western coffers at $20 to $40 billion a year and the flow stemming from mis-priced trade at $80 billion a year or more. My lowest estimate is $100 billion per year by these two means by which we facilitated a trillion dollars in the decade, at least half to the United States. Including the other elements of illegal flight capital would produce much higher figures. The Brookings expert also did not include illegal shifts of real estate and securities titles, wire fraud, etc.

In other words, **an incomplete figure of dirty money (laundered criminal and corrupt money) flowing into U.S. coffers during the 1990s amounted to $3-$5.5 trillion. This is not the complete picture but it gives us a basis to estimate the significance of the "dirty money factor" in evaluating the U.S. economy.** In the first place, it is clear that the combined laundered and dirty money flows cover part of the U.S. deficit in its balance of merchandise trade which ranges in the hundreds of billions annually. As it stands, the U.S. trade deficit is close to $300 billion. **Without the "dirty money" the U.S. economy external accounts would be totally unsustainable, living standards would plummet, the dollar would weaken, the available investment and loan capital would shrink and Washington would not be able to sustain its global empire.** And the importance of laundered money is forecast to increase. Former private banker Antonio Geraldi, in testimony before the Senate Subcommittee projects significant growth in U.S. bank laundering. "The forecasters also predict the amounts laundered in the trillions of dollars and growing disproportionately to legitimate funds." The $500 billion of criminal and dirty money flowing into and through the major U.S. banks far exceeds the net revenues of all the IT companies in the U.S., not to speak of their profits. These yearly inflows surpass all the net transfers by the major U.S. oil producers, military industries and airplane manufacturers. The biggest U.S. banks, particularly Citibank, derive a high percentage of their banking profits from serving these criminal and dirty money accounts. The big U.S. banks and key institutions sustain U.S. global power via their money laundering and managing of illegally obtained overseas funds.

U.S. Banks and The Dirty Money Empire

Washington and the mass media have portrayed the U.S. as being in the forefront of the struggle against narco trafficking, drug laundering and political corruption: the image is of clean white hands fighting dirty money. The truth is exactly the opposite. U.S. banks have developed a highly elaborate set of policies for transferring illicit funds to the U.S., investing those funds in legitimate businesses or U.S. government bonds and legitimating them. The U.S. Congress has held numerous hearings, provided detailed exposés of the illicit practices of the banks, passed several laws and called for stiffer enforcement by any number of public regulators and private bankers. Yet the biggest banks continue their practices, the sum of dirty money grows exponentially, because both the State and the banks have neither the will nor the interest to put an end to the practices that provide high profits and buttress an otherwise fragile empire.

First thing to note about the money laundering business, whether criminal or corrupt, is that it is carried out by the most important banks in the USA. Secondly,

the practices of bank officials involved in money laundering have the backing and encouragement of the highest levels of the banking institutions - these are not isolated cases by loose cannons. This is clear in the case of Citibank's laundering of Raul Salinas (brother of Mexico's ex-President) $200 million account. When Salinas was arrested and his large scale theft of government funds was exposed, his private bank manager at Citibank, Amy Elliott told her colleagues that "this goes in the very, very top of the corporation, this was known...on the very top. We are little pawns in this whole thing" (p.35).

Citibank, the biggest money launderer, is the biggest bank in the U.S., with 180,000 employees world-wide operating in 100 countries, with $700 billion in known assets and over $100 billion in client assets in private bank (secret accounts) operating private banking offices in 30 countries, which is the largest global presence of any U.S. private bank. It is important to clarify what is meant by "private bank."

Private Banking is a sector of a bank which caters to extremely wealthy clients ($1 million deposits and up). The big banks charge customers a fee for managing their assets and for providing the specialized services of the private banks. Private Bank services go beyond the routine banking services and include investment guidance, estate planning, tax assistance, off-shore accounts, and complicated schemes designed to secure the confidentiality of financial transactions. The attractiveness of the "Private Banks" (PB) for money laundering is that they sell secrecy to the dirty money clients. There are two methods that big Banks use to launder money: via private banks and via correspondent banking. PB routinely use code names for accounts, concentration accounts (concentration accounts co-mingles bank funds with client funds which cut off paper trails for billions of dollars of wire transfers) that disguise the movement of client funds, and offshore private investment corporations (PIC) located in countries with strict secrecy laws (Cayman Island, Bahamas, etc.)

For example, in the case of **Raul Salinas, PB personnel at Citibank helped Salinas transfer $90 to $100 million out of Mexico in a manner that effectively disguised the funds' sources and destination thus breaking the funds' paper trail. In routine fashion, Citibank set up a dummy offshore corporation, provided Salinas with a secret code name, provided an alias for a third party intermediary who deposited the money in a Citibank account in Mexico and transferred the money in a concentration account to New York where it was then moved to Switzerland and London.** The PICs are designed by the big banks for the purpose of holding and hiding a person's assets. The nominal officers, trustees and shareholder of these shell corporations are themselves shell corporations controlled by the PB. The PIC then becomes the holder of the various bank and investment accounts and the ownership of the private bank clients is buried in the records of so-called jurisdiction such as the Cayman Islands. Private bankers of the big banks like Citibank keep pre-packaged PICs on the shelf awaiting activation when a private bank client wants one. The system works like Russian Matryoshka dolls, shells within shells within shells, which in the end can be impenetrable to a legal process.

The complicity of the state in big bank money laundering is evident when one reviews the historic record. Big bank money laundering has been investigated, audited, criticized and subject to legislation; the banks have written procedures to comply. Yet banks like Citibank and the other big ten banks ignore the procedures and laws and the government ignores the non-compliance. {e.g. Anti-Money Laundering

But Bank of America states in public: they have implemented an enterprise-wide Anti-Money Laundering (AML) compliance program, which covers all of its subsidiaries and affiliates, and is reasonably designed to comply with applicable laws and regulations.

Bank of America Anti-Money Laundering (AML) and Counter-Terrorist Financing Policy Statement

Crime has a destructive and devastating effect on the communities in which we operate. Safeguarding the global financial system is critically important for the economic and national security of the jurisdictions in which we operate. Accordingly, it is the policy of Bank of America to take all reasonable and appropriate steps to prevent persons engaged in money laundering, fraud, or other financial crime, including the financing of terrorists or terrorist operations, (hereinafter collectively referred to as “money laundering”) from utilizing Bank of America products and services. Compliance with both the letter and the spirit of the anti-money laundering regulatory regimes in the countries and jurisdictions in which Bank of America operates is one way the Bank works to achieve this policy.

IN FACT:

Over the last 20 years, big bank laundering of criminal funds and looted funds has increased geometrically, dwarfing in size and rates of profit the activities in the formal economy. Estimates by experts place the rate of return in the PB market between 20-25% annually. **Congressional investigations revealed that Citibank provided "services" for 4 political swindlers moving $380 million: Raul Salinas - $80-$100 million, Asif Ali Zardari (husband of former Prime Minister of Pakistan) in excess of $40 million, El Hadj Omar Bongo (dictator of Gabon since 1967) in excess of $130 million, the Abacha sons of General Abacha ex-dictator of Nigeria - in excess of $110 million. In all cases Citibank violated all of its own procedures and government guidelines:** there was no client profile (review of client background), determination of the source of the funds, nor of any violations of country laws from which the money accrued. On the contrary, the bank facilitated the outflow in its prepackaged format: shell corporations were established, code names were provided, funds were moved through concentration accounts, the funds were invested in legitimate businesses or in U.S. bonds, etc. In none of these cases - or thousands of others - was due diligence practiced by the banks (under due diligence a private bank is obligated by law to take steps to ensure that it does not facilitate money laundering). In none of these cases were the top banking officials brought to court and tried. Even after arrest of their clients, Citibank continued to provide services, including the movement of funds to secret accounts and the provision of loans.

Correspondent Banks: The Second Track

The second and related route which the big banks use to launder hundreds of billions of dirty money is through "correspondent banking" (CB). CB is the provision of banking services by one bank to another bank. It is a highly profitable and significant sector of big banking. It enables overseas banks to conduct business and provide services for their customers - including drug dealers and others engaged in criminal activity - in jurisdictions like the U.S. where the banks have no physical presence. A bank that is licensed in a foreign country and has no office in the United States for its customers attracts and retains wealthy criminal clients interested in laundering money in the U.S. Instead of exposing itself to U.S. controls and incurring the high costs of locating in the U.S., the bank will open a correspondent account with an existing U.S. bank. By establishing such a relationship, the foreign bank (called a respondent) and through it, its criminal customers, receive many or all of the services offered by the U.S. big banks called the correspondent.

Today, all the big U.S. banks have established multiple correspondent relationships throughout the world so they may engage in international financial transactions for themselves and their clients in places where they do have a physical presence. Many of the largest U.S. and European banks located in the financial centers of the world serve as correspondents for thousands of other banks. Most of the offshore banks laundering billions for criminal clients have accounts in the U.S. All the big banks specializing in international fund transfer are called money center banks, some of the biggest process up to $1 trillion in wire transfers a day. For the billionaire criminals an important feature of correspondent relationships is that they provide access to international transfer systems - that facilitate the rapid transfer of funds across international boundaries and within countries. The most recent estimates (1998) are that 60 offshore jurisdictions around the world licensed about 4,000 offshore banks which control approximately $5 trillion in assets.

U.S. Banks Help Cartels Launder Illegal Drug Money
Monday, July 05, 2010

Wachovia bank recently reached an agreement with federal prosecutors to settle charges that it allowed drug cartels to launder more than $378 billion through exchange houses it owned in Mexico from 2004 to 2007. Wachovia, now owned by Wells Fargo, was found to have committed the largest violation of the Bank Secrecy Act in U.S. history.

Wells Fargo has agreed to pay $160 million in fines and penalties, which represents less than 2% of its 2009 profits. If Wells Fargo does pay the amount agreed upon, the Justice Department **will drop all related charges** next March. According to Bloomberg News, "**No big U.S. bank--Wells Fargo included--has ever been indicted**

for violating the Bank Secrecy Act or any other federal law. Instead, the Justice Department settles criminal charges by using deferred-prosecution agreements, in which a bank pays a fine and promises not to break the law again."

Some of the laundered drug money was used to buy DC-9 planes to smuggle drugs into Mexico. But Wachovia wasn't the only bank to allow illicit funds to move through its accounts. **The aircraft purchases also relied on monies that moved through Bank of America. And American Express Bank International in Miami has twice been fined for failing to detect drug money filtering through its accounts.**

Not just banks have profited from drug cartel money. In February, **Western Union**, which transfers money by wire, agreed to pay $94 million to settle investigations by Arizona's attorney general.

They were laundering money equal to one third of the GDP of Mexico yet claimed that no one noticed.

Privacy? Gone and get over it. As a security professional wrote:

DOJ sends order to Twitter for Wikileaks-related account info
http://news.cnet.com/8301-31921_3-20027893-281.html

"I guess my DMs [to Jacob Applebaum] are now part of the evidence in this investigation. Not that there is anything interesting there. Of course **when I sent the DMs I assumed that since they were in the clear with no anonymization they were already being hoovered up by the illegal NSA/AT&T internet tap in SF. They already had all this data. This court order lets them now use that evidence in a trial as it was legally obtained."**

Not just American banks of course:

Jyske Bank fined for laundering
Monday, 17 May 2010
Danish bank

Possible conflicts in banking regulations between Gibraltar and Spain have led to a considerable fine for Jyske Bank, according to bank management

Spanish financial authorities have issued Jyske Bank a 1.7 million euro fine for violating the country's money laundering regulations, reports Jyllands-Posten newspaper.

Activities at Jyske Bank's division in the British overseas territory of Gibraltar are at issue in the case, where the Spanish authorities assert they have been denied access to vital information.

In the decision to fine the bank, the violations were described as ‘very serious’ and Jyske Bank in Gibraltar was cited for failure to properly report, unwillingness to investigate certain transactions, and having inadequate control procedures.

It is the first time a Danish bank has been fined for violations of another country’s money laundering rules.

Unmasking the Vatican's bank

Jan 25 2011

ROME, Italy — When Pope Benedict XVI makes lofty statements about the role ethics plays in the economy, he speaks from experience.

Within the Vatican is the only branch of the Instituto per le Opere di Religione (IOR), otherwise known as the Vatican bank. Its ATM uses Latin.

Only Vatican employees and religious institutions are allowed to open accounts in the bank — which you’d think would make it the most moral bank in the world.

So why is its chief, economist Ettore Gotti Tedeschi, under investigation for money laundering?

Italy's Central Bank flagged a 23 million euro transfer from an IOR account in an Italian bank, the Credito Artigiano, to two other accounts as lacking some information now compulsory under EU-mandated anti-money laundering laws. So prosecutors seized the money, froze the IOR account, and opened an investigation.

This embarrassing “misunderstanding” — as the Vatican called it in a note published in its newspaper, l'Osservatore Romano — managed to turn the spotlight again on an institution that has been involved in many murky affairs.

“The IOR is not a bank in the normal definition of the term,” wrote Vatican spokesman Federico Lombardi in a recent letter to the Financial Times. In fact, it doesn't lend money or act as a consultant to businesses.

“It is more a fund deposit and transfer institution than a bank,” said Carlo Marroni, a Vatican expert with Il Sole 24 Ore, Italy's financial daily. IOR doesn't invest in the stock market, he thinks, “though they operate on the currency or bond market, or buy gold.” To trade in world markets it must go through other banks, such as the Credito Artigiano.

It is hard to pin down the value of IOR’s holdings. “It doesn't publish a budget or an annual report,” Marroni said. “It is usually held that it has 5 billion euros in deposits, but I don't know how exact this figure is.”

Another often reported figure is that accounts turn a 13 percent yearly interest — tax-free, like the Vatican itself.

But, “I think it's much less than that,” said Marroni. A leaked document from 1987 published in a recent book that made headlines here, “Vaticano Spa” — Spa being the acronym for publicly traded companies in Italian — showed that an IOR account yielded a 9 percent net interest.

IOR's biggest asset, anyway, is its secrecy — all its accounts are identified only by number. This secrecy has been used for unholy goals.

Some of them have been documented in full. The author of “Vaticano Spa,” Gianluigi Nuzzi, gained access to the archive left by the late Monsignor Renato Dardozzi, a key player at IOR from 1974 to the late 1990s. He used it to investigate the bank's involvement in money-laundering for Italian politicians and even mafia bosses. In a letter published by Nuzzi, **the previous president of the Vatican Bank, Angelo Caloia, confessed worriedly to cardinal Angelo Sodano, John Paul II's “prime minister,” that IOR had served to “clean” bribes and that it held ciphered accounts for Catholic politicians, such as seven-time prime minister Giulio Andreotti.**

When Banco Ambrosiano head Roberto Calvi, know as “God's Banker,” died under Blackfriars Bridge in London in 1982, the Vatican Bank was then the main shareholder of the Banco.

The American head of IOR at the time, Illinois-born cardinal Paul Casimir Marcinkus, a former body guard to Pope Paul VI, resorted to Vatican immunity to avoid prosecution by Italian judges. He died in 2006 and has often been blamed for the scandals that plagued the bank in the 1980s.

Wolfsberg Group

UBS remains strongly committed to promoting the development and implementation of anti-money laundering (AML) standards for the financial industry as a whole, thereby contributing to wider efforts against money laundering. As an example of this, UBS was one of the driving forces behind the launch of the Wolfsberg Group, which issued its first global AML principles in 2000.

UBS banker arrested over money laundering

Brazilian authorities launch investigation into Swiss banks UBS and Credit Suisse and US insurer AIG
Michael Herman and AP

A banker from UBS' wealth management group was one of 19 people arrested by Brazilian police last night in connection with an anti-money laundering investigation that is also targeting the rival Swiss bank Credit Suisse and AIG, the US insurer.

UBS confirmed that a Swiss employee in its wealth management and business banking division had been detained.

It said that the bank was looking into the matter but declined to name the banker concerned or comment further.

The arrest was made during an investigation into an alleged scheme that allowed Brazilian companies to avoid taxes by laundering money through Swiss banks and the US insurance group, a detective from Brazil's federal police said.

Clariden Leu, a private banking subsidiary of Credit Suisse, confirmed that one of its employees had also been detained. Credit Suisse decline to comment.

In a statement, a federal judge named UBS, Credit Suisse and AIG as the financial institutions under investigation.

AIG said that it was "not aware of any wrongdoing by any AIG employee".

OR

Barclays, UBS, HSBC, Royal Bank of Scotland Involved in Money Laundering for Corrupt Nigerian Politicians

October 13, 2010

Barclays, HSBC, UBS, others 'fuel corruption in Nigeria'

> **Barclays, HSBC, NatWest, Royal Bank of Scotland and UBS – have been linked to money laundering scam over which some corrupt Nigerian politicians were indicted.**
>
> A report entitled 'International Thief' from Global Witness, a Non-Governmental Organisation (NGO) that exposes the corrupt exploitation of natural resources and international trade systems, drives campaigns to end impunity, resource-linked conflict, and human rights and environmental abuses, accused the banks of fueling corruption in the world's most-populous black nation.
>
> In a 40-page report published yesterday in www.globalwitness.org, Global Witness said that the five banks had taken millions of pounds between 1999 and 2005 from two former governors accused of corruption (Diepreye Alamieyeseigha of Bayelsa State and Joshua Dariye of Plateau

State), but had failed sufficiently to investigate the customers or the source of their funds.

WHISTLE-BLOWERS AND TEAM-PLAYERS (see excerpts from my column on the subject below)

Either one counts on a CONTEXT that supports "truth-telling" or one has to build a context in which one can find trusted colleagues and tell the truth in a small group and develop strategies based on that truth and commitment. PRIVACY IS NOT AN ISSUE FOR THE INDIVIDUAL. THAT FOCUS IS RED HERRING. SECURE COMMUNICATIONS AMONG TRUSTED COLLEAGUES IS THE ISSUE. (See: Tunisia, Iran, Egypt, Syria for recent examples.)

In my last conversation with Gary Webb, I asked if his work on "Dark Alliance" was worth it. He said:

Was it worth it? Yes. The CIA admitted it. I know it was the truth, and that's what kept me going. I knew I was right.

My eyes were wide open. I knew what I was getting into. The kids suffered. I had the paper behind me – I thought. Support came from all sorts of places. Especially African Americans. My wife was OK with it. She was used to me getting death threats.

You get one chance in a lifetime to do the right thing. If you don't do it, you surrender, and then they win. These are the worst people on earth that you're dealing with – they lie, plant stories, discredit and worse for a living and have the resources and the experience. But somebody's got to do it. Otherwise they win.

When he killed himself, I thought of this late-night conversation. Who in fact won?

Since 9/11 the Media Complex has hammered at the loss of under 3000 lives as a criminal act justifying a global response that included torture as a standard methodology, numerous wars and special forces activities, and the hoovering of American comms without warrants. The cartel wars have cost more than 35,000 lives and some of the banks named above are complicit in their murders. That you can read it here is an example of how free speech functions as a bleeder valve, so long as it does not lead to action. If it leads to action – e.g. MLK Junior, Malcolm X, Fred Hampton, etc. – it is not tolerated so easily.

[Casa de Cambios, NAFTA, 22,000 Dead by Kathleen Miller - August 4th 2010

Law enforcement officials often suggest money laundering is too complex a process for the average person to understand. Factor in an understandable concern

that interfering, even from afar, in the business of big banking could always affect one's own bottom-line, and you can see why reports of financial crimes do not receive the same attention, in the press, from the public or the government, as say, Lindsay Lohan's sentencing for too many DUIs.

W**hat we need perhaps is a simpler view of how the US-Mexico banking relationship supports transnational crime and how that relationship is nourished and sustained by NAFTA.** We also need to understand what part the wire transmitting operations know as "Casa de Cambios" (CDCs) play, and why, in the case of Wachovia's laundering of millions in dirty dollars, these CDCs have been so critical to success.

NAFTA, which created a unified trade bloc, also created a transnational financial bloc. During the last two decades, foreign institutions have been binging on a menu of mergers and acquisitions, acquiring significant interest and, in some cases, outright control of banks and other financial services providers in Mexico.

Large, powerful US banks like Wachovia, Bank of America, American Express, Citigroup, Spain's BBVA and London-based HSBC have been setting up shop in a nation burdened by a $39 billion per annum illegal drug industry, a history of corruption in both the private and public sectors, and ongoing civil unrest spawned by the quest for criminal control of Mexico's drug trade.

One important result is an opportunity for cash to move unimpeded from Mexico's casa de cambios to their accounts in Mexican banks, and then to correspondent accounts in US banks. Drugs move from Mexico into the U.S., and drug money then moves south, through Mexico, and back to the U.S. or wherever the trafficker wants his 'clean' money to land.]

February 7, 2009 (LPAC) **In the mid-1990s, George Soros reportedly gave a $50 million personal loan to the Colombia financiers, the brothers Gilinski -- Jaime and Isaac Gilinski, to support their takeover of the Banco de Colombia, which had been privatized.** Soros reportedly gained about a 9% interest in that bank. The Gilinskis were majority owners of Banco de Colombia for about three years, then sold it, but may have retained a minority interest. **Soros may have invested more in the bank after the Galinskis moved out of control.**

On October 4, 2000, PBS interviewer Juan Williams spoke with **Carlos Toro, a childhood friend of Colombian drug cartel leader Carlos Lehder. Toro was an informant for the Drug Enforcement Agency** who helped put Lehder and others in jail, and then went into the Witness Protection Program.

"MR. TORO: The Colombian banking industry and also Colombian banks that had subsidiaries in Miami and Panama working very closely with us.

"In those days...we had Colombian banks, Banco De Colombia, Banco [unintelligible], Banco Cafetero [ph], Eagle National Bank of Miami. We were allies. In those days--and maybe Steve knows how Eagle National Bank was a powerful aid for us between 1980 and 1984.

"MR. WILLIAMS: But the cartel did not own the bank. It was simply allied with the cartel.

"MR. TORO: The cartel didn't own the bank in front of FDIC, but we own the bank...."

In 2003, the Lubavitcher organization at Harvard University held a ceremony honoring the same Jaime Gilinski of Cali, Colombia, because he gave the money to build their headquarters; Alan Dershowitz spoke at the same or another ceremony honoring Gilinski, saying Gilinski's action would work against anti-semitism at Harvard. The Lubavitcher introducing Gilinski called him "the leader of Jewish communities throughout Latin America."

On March 31, 2005, the Federal Reserve issued a cease and desist order to the Eagle National Holding Co. Of Miami, Florida, owner of Eagle National Bank of Miami, banning transactions between the company and other financial organizations controlled by the holding company's chairman, Jaime Gilinski; the Galinski companies are controlled by a trust owned by the Gilinski family.

WHAT IS THE IMPACT ON SERIOUS WELL-INTENTIONED SECURITY PROFESSIONALS?

SEE: "Northward into the Night" in Mind Games

One security professional noted after Def Con 2010, "there are a lot of neat stories out of DefCon/BH this year. But they all seemed to revolve around:

- Attacks are sexy
- The sky is continuing to fall

I saw **very few defensive technologies and techniques** being presented. I don't recall reading about _anything_ defensive in the press. some stats about attacks, but that just paints a picture of how bad things are. GSM attacks, ATM attacks, social media attacks, etc all got many write-ups. Honestly, I can't recall reading anything about defense.

I'm pretty frustrated with the state of the industry right now. Finding a single vuln will get you on national news. Selling the same defensive tech for 20 years makes you a ton

of money. **Finding ways to actually deal with the fact that orgs are getting 0wned every day by ppl who are clearly targeting specific access is met with a test pattern.**

Another said the seemingly obvious:

“The attack is sexy. Publicizing the attack is sexy and can perpetuate the FUD cycle as well. :(

IMHO the focus is still on "stuff" to be placed on top of a flawed underlying foundation. Ergo we never can really get to 'acceptable' levels of infosec unless either we a) rip out the networks and start from scratch again, or b) change the competence of corporate/govt infosec folks to not tolerate mediocrity and empower them with the authority, resources, and support to do what it takes to "do it right." Otherwise we're just throwing good money after bad and perpetuating the status quo. It's why I no longer do pen tests or red teams, because folks don't really learn from our findings, they just want to check-the-box each year. So for me, why bother? I'm not making a tangible difference anymore, so if clients don't care, apart from maybe making a nice profit on a gig to offer recommendations that I know will be ignored, why should I?

There are some pretty good papers discussing the economic incentives of keeping the state of infosec just as-is, because it's beneficial to vendors / consultants. You know, like how the pharmaceutical industry likes it when folks stay sick so they can sell more drugs. Nobody wants a "cure" -- the "vendors" don't, and the "patients" just chalk incidents up as the price of doing business in cyberspace and look for a palliative, rather than a curative.

Another said: **the problem is that to tell the truth, one has to 1) not be a vendor and 2) be willing to spill the beans on getting owned. There are very few people that are willing to get up and say "I work security, my job is to prevent intrusions, we get owned a lot (so I kind of fail at my job), sometimes it is really bad, and here is how we deal with it."**

Telling someone how you have to reverse engineer 0day attacks and unravel complex malware *as fast as possible* can be very sexy, and using real world examples to back it up really helps bring the message home.

In airing the dirty laundry you reveal defensive techniques you have adapted that in many cases actually work at stopping the bad guys (or at least some of them for a while). But by speaking about these techniques publicly you are telling your enemies how to adapt, so you have yet another sexy aspect of defense you can discuss**.**

Another: **even when we do our jobs correctly, we're all still going to get owned. The real challenge is getting business leaders to accept that reality and allow us to redirect funding to programs that help companies deal with that reality**.

And another: Attacks can be simple, silver bullet, and developed by one guy. This makes them easy to describe. Defenses are mulitlayered and have timelines of years and take teams of people to implement. defense is boring because we already know what to do. It is not a technology problem but a business problem. That is why one of my focuses is to make application security as cheap and consumable by the masses as possible.

And another: After working mostly in red teaming and pen-testing, I took a job running security for a hedge fund for a few years. Working defense is distinctly more challenging than offense for unexpected reasons, and this is how I saw it as being different:

1. You are held back by people and processes, not technical challenges
2. Success is the result of thoroughness, not cleverness
3. Success is gradual and continual, not sporadic and elusive

On offense (pen-testing or research), you find yourself thinking, "If only I could figure out how to do X". On defense, I found myself thinking mostly, "If only I could get so-and-so/everyone to do X". The solutions and improvements were largely nothing magical, but more like eating your vegetables. You know that you should do it, you just have to do it consistently and thoroughly over many years to obtain the benefits. And let's face it, eating your vegetables isn't exactly new or "sexy", but the results of doing so over many years may be.

WHISTLEBLOWERS AND TEAM PLAYERS – revisited

It was only after whistleblowers came out of the closet during the Great Economic Deflation that Time Magazine honored the practice of what team players call “ratting out your pals.” Conservative magazines like Time may give lip service to whistle blowing in the abstract but never champion whistle blowers until after they have sung. Instead they support the conditions and practices which make whistleblowers a threat in the first place.

Whistleblowers are a reminder that ethics must be embodied in real flesh-and-blood human beings who put themselves on the line. Unless our deeper beliefs and values become flesh, they are words words words designed to make us feel better, rationalize misdeeds, and send distracting pangs of conscience straight into space.

If you have never known a real flesh-and-blood whistleblower, **see** the film “The Insider” for a good portrait. The film confirms the conclusion of a Washington law firm specializing in whistleblower cases that lists motivations for whistle blowing – money, anger and resentment, revenge, justice – and eliminates all but one as sufficient to carry a whistleblower through the abuse they will face. Only acting from a pained conscience will sustain a whistleblower through the ordeal.

During a recent speech for accountants about ethics, our Q&A moved quickly into the gray areas where accountants spend much of their time. Outsiders think accountants live in a black and white grid with simple answers but in fact they wade through a swamp of maybe this or maybe that.

Accountants are paid whistleblowers. Accountants are intended to be in the corporate culture but not of it, to use company books like mirrors to reveal the truth and consequences of choices. That's why it is so difficult to do the job right.

The tension comes from the fact that only an individual can have a conscience. An institution or organization can develop a culture that supports doing the right thing only when a leader pursues that objective with single-minded intensity. Left to themselves, all cultures are based on survival, not telling the truth. Cultures reward team players, not whistleblowers. In all my years as a teacher, priest, speaker and consultant, I have never seen a culture with a conscience.

A cop friend reminds me that the first time a rookie cop sees his partners beat someone up in an alley or notices that money or cocaine doesn't always get back to the station, he is closely watched. The word goes out quickly that "he's OK" or "watch out for him." Those that are OK move up. The cop is a practicing Roman Catholic and noted that recent scandals in the church are symptoms of the same dynamics.

Institutions usually encourage disclosure only when it no longer matters. Operation Northwoods – the desire by the Joint Chiefs of Staff in 1962 to eliminate Fidel Castro by sinking refugee boats from Cuba, attacking our own base at Guantanamo, and planting terror bombs in American cities – was revealed by James Bamford in his book "Body of Secrets," but nary a peep of outrage greeted revelation of the treasonous scheme. When the Church apologized to Galileo for torturing him four hundred years after the fact, it raised the question of how an institution had so lost its moorings that someone might think an absurd gesture like that had meaning.

Why are so many of your heroes, I was asked, people who were assassinated? Why do names like Jesus, Lincoln, Gandhi, and Martin Luther King, Jr. keep showing up in your conversation?

I think it's because they embody what it takes to make a stand on behalf of the truth. They were all human but found the courage to blow the whistle on the cultures of death our institutions create. Their reward was getting whacked.

Make no mistake, those who articulate or embody an upward call always inspire ambivalence. A disciple of Gandhi said that even those who loved him most were secretly relieved when he was murdered because for the moment the pressure was off. Jesus as icon is malleable in the hands of his institutional custodians whereas Jesus the Jew in the street was a real pain.

In an era characterized by increasing secrecy by the government and the gradual but progressive surrender of our rights, it's only a matter of time until some malevolent design ripens and bursts into the sunlight because some whistleblower just can't stand it another minute. Some team player, their motives mixed but their conscience pricked,

will tell the truth. That's the only way to have accountability when those with power and privilege remove transparency from the processes of government and business.

When a mainstream Midwest woman asks how she will tell her grandchildren what America was like before the Great Change, how she will explain openness and disclosure, the Freedom of Information Act, guarantees in the Bill of Rights … then I know that we don't need a weatherman to know the direction of the wind and see the firestorm on the horizon. Signs of the times grow on trees like low-hanging fruit, ripe for the picking.

We are all team players, all of us some of the time, some of us all of the time, but we each have our own particular crossroads where we must decide if our words will become flesh. It is never easy and there are always consequences. Only integrity will see us through to the bitter end and none of us really know if we have it until it is tested.

Again, what is the real state of the craft?

"A lot of people - and particularly non-technical leaders - aren't willing to ask the next round of hard questions because they haven't come to the realization that what we've currently got is fundamentally broken. There are folks out there still trying to perfect AV and IDS mouse traps. I suggest that no "big data" solution is going to magically solve the problem of the "I have to see it first in order to detect it later" brokenness that represents the foundation of the vast majority of our controls.

Why raise this as an important step? Because I wonder if one can initiate honest dialog about fundamental change without acknowledging the need for that dialog. (i.e. This shit doesn't work, now lets start the hard conversation about real change)

Risk and accountability. our inability to accurately identify and convey technology risks kills us. What is the cost of Adobe Reader vulns when they are used to steal your CAD diagrams that result in knock-off parts being manufactured in China? That's an extreme example, but this conversation needs to occur AT EXECUTIVE LEVELS.
if we don't start the dialog with honest assessments and realistic assumptions we have zero hope of moving forward. And I think that starts with "give up on x technologies - they are at the end of their lives."

a lot of the "shocking" public realizations that have transpired the last 12-24 months (Zeus, wikileaks, stuxnet, the HBG fiasco) are the formalized and weaponized materializations of what we knew was possible all along.

Software security problems in all sorts of goods and services? Check. Greater societal dependence on this technology? Check.

Greater complexity? Check.
People selling 0day to god knows who, for money? Check.
Professional development of digital weaponry? Check.
Black market economy? Check.
Industrial espionage? Check. (Although this is not exactly new...)
Leaked information? Targeted information? Traded information? Check.
Intelligence agencies outside of the USG that have growing capabilities? Check.
Real world ramifications to all of the above? CHECK.

and another:

I guess it basically comes down to handling risk. You assume the worse risk scenarios possible, and proceed to develop trust models that usually don't fully mitigate all risks. You simply are mitigating your fear. It isn't "how much security do I need until I have no risk" it is "how much security do I need until I can live comfortably with the various risks I feel I am facing".

REPRISE: ENDING WHERE WE BEGAN

"The price one pays for pursuing any profession or calling is an intimate knowledge of its ugly side." – James Baldwin

**"Whoever battles monsters should take care not to become a monster too,
For if you stare long enough into the Abyss, the Abyss stares also into you."
- Nietzsche, Beyond Good and Evil, chapter 4, no. 146**

THE BIGGEST LESSON:

THINGS ARE NOT WHAT THEY SEEM
e.g. making jihadist web sites more robust.
In Mind Games, read at least the introduction to "Zero Day Roswell."

security is more than implementation of software & hardware. it's creation of a geopolitical structure than enables us to believe tomorrow will be like today. It is the amelioration of the anxieties of life, often using fictitious narratives as a way to say "there there" as we tuck in society for the night with a kiss.

e.g. we recontextualize anomalies as known events, so they won't be feared:
a terror attack degrades the mind of society. an accident does not.

assassins – always said to be an anomalous lone gunman. As Dulles, former CIA Director, told the Warren Commission, when asked about the plot to kill Lincoln and a simultaneous plot to kill Andrew Johnson – "that proves my point."

In short, we live in a bat-shit crazy-making world.

How can we use the word “security” as if we mean ... security? what is it, then? as wise guys say, it is what it is.

try to find out what’s going on? That’s a full time job, and most people are distracted by work, family, amusements.
Jonathan Moreno – author of Mind Wars. How hard it was to explore that subject, despite credentials.
Steve Miles – torture including physicians which means experimentation. George Bush saying we used water boarding 3 times. Complete bullshit. Oops death and the Uzbeks. Oh yeah? You ever work with the Turks?

Water boarding is a distraction. It’s nothing compared to what we do.

What does it do to us? secondary trauma: going over the line:

Multiple sources of accountability when a videotape shows interrogator as well as the interrogated That’s a metaphor for complexifying the situation with too much information, confusing information, multiplying sources of information, disinformation, and misinformation.

It is not just the “stupid user” problem – it is the human condition. Sometimes tech people speak to security issues as if they are not subject to the human condition. But specialized knowledge can be a trap if it is not contextualized in a wider understanding.

The cutting edge is no longer just information technology but cross-disciplinary knowledge, biology (markers: 2004 new president at MIT from biology, Gates saying he would be in biology today, DIYbio, biohacking)

what can we do? Victor Frankl as an example.

WE, not they. Understand our real role in the body politic. Work to moderate the worst threats to stability and ensure robust societies and economies in which we can be more fully human.

Remember what the undercover cop in the film said: I don’t know if I am a cop pretending to be a criminal or a criminal pretending to be a cop. Until we look into the mirror and see that, we are in danger of believing in our beliefs. We need to take ourselves seriously but not too seriously, just seriously enough**: be mindful and vigilant.**

And all shall be well, and all manner of thing shall be well.