

# The CIA Does Vegas

## Fear and Loathing at Black Hat 2014

By Bill Blunden, July 31, 2014

One evening over drinks in Ethiopia, during his tour as a CIA officer back in the 1960s, John Stockwell expressed reservations about covert operations to a senior fellow officer named Larry Devlin. Stockwell worried that the CIA was infiltrating governments and corrupting leaders to no useful end. Devlin, well-known in spy circles for his work in the Congo, berated Stockwell<sup>1</sup>:

*"You're trying to think like the people in the NSC back in Washington who have the big picture, who know what's going on in the world, who have all the secret information, and the experience to digest it. If they decide we should have someone in Bujumbura, Burundi, and that person should be you, then you should do your job, and wait until you have more experience, and you work your way up to that point, then you will understand national security, and you can make the big decisions. Now, get to work, and stop, you know, this philosophizing."*

It's a compelling argument: trust me, I know secrets. In fact it's the same sort of argument that a federal informant named Hector Xavier Monsegur used to convince an activist named Jeremy Hammond to break into a whole slew of servers belonging to foreign governments<sup>2</sup>. Monsegur assured Hammond: "Trust me, everything I do serves a purpose." Hammond didn't realize that he was actually part of an elaborate intelligence campaign being run by the FBI. Pimped out to other American three-letter agencies as it were.

### **Trust Me: I'm an Insider**

John Stockwell was patient. He stayed on with the CIA and rose through the ranks, ultimately garnering enough clout to sit in on subcommittee meetings of the National Security Council. What he witnessed shocked him. Stockwell saw fat old men like senior ambassador Ed Mulcahy who fell asleep<sup>3</sup> and petty officials like Henry Kissinger who got into embarrassing spats when someone else sat in their chair.<sup>4</sup> All the while decisions were made that would kill people.

*Quelle surprise!* There were no wise men making difficult decisions based on dire threats to national security. Merely bureaucrats in search of enemies whose covert programs created more problems than they solved.

There's a lesson in this story that resonates very strongly. *A security clearance is by no means a guarantee of honesty or integrity.* The secrets that spies guard don't necessarily justify covert programs. Rather the veil of the government's classification system is often leveraged to marginalize the public, to exclude people from policy making, and conceal questionable activity that would lead to widespread condemnation and social unrest if it came to light.

Past decades offer an endless trail of evidence: Operation Gladio, Operation Mockingbird, Project MKUltra, Operation Wheeler/Wallowa, Watergate, Operation CHAOS, COINTELPRO, Operation Northwoods, P2OG (the Proactive, Preemptive Operations Group), Iran-Contra, etc.

Cryptome's John Young describes how this dynamic literally unwinds democracy<sup>5</sup>:

*"Those with access to secret information cannot honestly partake in public discourse due to the requirement to lie and dissimulate about what is secret information. They can only speak to one another never in public. Similarly those without access to secret information cannot fully debate the issues which affect the nation, including alleged threats promulgated by secret keepers who are forbidden by law to disclose what they know."*

### **The Parade of Lies**

In light of Ed Snowden's revelations, and the remarkably flat-footed response of our political leaders, society is witnessing a *crisis of trust*. Time after time we've been lied to by ostensibly credible government officials. Not little white lies, but big scandalous ones. Lies that bring into question the pluralistic assumptions about American democracy and suggest the existence of what political analysts from Turkey would call a "Deep State"<sup>6</sup>.

For instance, both former NSA director Keith Alexander and House Intelligence Chair Mike Rogers claimed that NSA mass interception was instrumental in disrupting over 50 terror plots, a claim that dissolved quickly upon closer scrutiny<sup>7</sup>.

Or contemplate an unnamed NSA spokesman who vehemently told the *Washington Post* that the NSA was **\*\*\*not\*\*\*** engaged in economic espionage<sup>8</sup>, only to be contradicted by leaked top-secret documents which described how the NSA broke into networks run by the Chinese telecom giant Huawei and made off with the company's crown jewels (i.e. product source code).

When President Obama scored some air time with Charlie Rose, in soothing tones he calmly explained to viewers that the NSA doesn't monitor American citizens without a warrant. It's surprising that POTUS, a man with a background in constitutional law no less, would be unaware of Section 702 of the Foreign Intelligence Surveillance Act (FISA). This legal provision contains a loophole that allows just this sort of warrantless monitoring to transpire<sup>9</sup>. Never mind Executive Order 12333, which is arguable an even greater threat<sup>10</sup>.

More recently, consider Dianne Feinstein's claim back in March that the CIA had been monitoring a network used by the Senate Intelligence Committee. John Brennan, the CIA director, told her that she was full of it and sanctimoniously replied "when the facts come out on this, I think a lot of people who are claiming that there has been this tremendous sort of spying and monitoring and hacking will be proved wrong<sup>11</sup>."

Well guess what? It turns out Brennan was on the losing side of that bet. An internal investigation showed that CIA officers had indeed been watching the Senate Committee<sup>12</sup>. Stop and pause for a

moment. This disclosure is a serious warning sign. What, pray tell, do you think happens to the whole notion of checks and balances when the executive branch spies on the other two branches? Do you suppose there are implications for the balance of power?

### **Damage Control**

Faced with this ever expanding dearth of credibility, spies have worked diligently to maintain the appearance of integrity. Specifically, industry conferences like Black Hat and DEF CON have regularly catered to the needs of U.S. Intelligence by serving as platform for the Deep State and its talking points: that Cyberwar is imminent<sup>13</sup>, that cybercrime represents an existential threat<sup>14</sup>, and that mass interception is *perfectly normal and perfectly healthy*<sup>15</sup>.

*“If the tariff of security is paid, it will be paid in the coin of privacy.”<sup>16</sup>*

In these hacker venues high-profile members of the intelligence community like Cofer Black<sup>17</sup>, Shawn Henry<sup>18</sup>, Keith Alexander<sup>19</sup>, and Dan Greer<sup>20</sup> are positioned front and center in keynote slots, as if they were glamorous Hollywood celebrities. While those who value their civil liberties might opine that they should more aptly be treated like pariahs<sup>21</sup>.

### **“Time Out” Posturing**

One would hope that the gravity of Ed Snowden’s documents would have some impact. Indeed, Jeff Moss, the organizer who currently runs DEF CON and who originally founded Black Hat (and, by the way, currently sits on the Department of Homeland Security’s Advisory Council<sup>22</sup>), did attempt to make a symbolic gesture of protest in the summer of 2013. He gently requested that feds call a “time-out” and not attend DEF CON<sup>23</sup>.

To grasp the nature of this public relations maneuver is to realize that roughly 70 percent of the intelligence budget is channeled to private sector companies<sup>24</sup>. As Glenn Greenwald observed during the 2014 Polk Award ceremony, as far as the national security state is concerned there is little distinction between the private and public sector<sup>25</sup>. Anyone who has peered into the rack space of the data broker industry knows that the NSA is an appendage on a much larger corporate apparatus<sup>26</sup>.

So asking federal employees to stay away really doesn’t change much because the driving force behind the surveillance state, the defense industry and its hi-tech offshoots, will swarm Vegas in great numbers as they normally do. Twelve months after Moss calls his halfhearted “time-out” Black Hat rolls out the red carpet for the Deep State<sup>27</sup>, (while the government threatens to clamp down on attendance to conferences by foreign nationals<sup>28</sup>). This is all very telling.

**Bill Blunden** is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

## End Notes

---

- <sup>1</sup> John Stockwell, *THE SECRET WARS OF THE CIA: part I*, lecture given in October, 1987, [http://www.thirdworldtraveler.com/Stockwell/StockwellCIA87\\_1.html](http://www.thirdworldtraveler.com/Stockwell/StockwellCIA87_1.html)
- <sup>2</sup> Mark Mazzetti, "F.B.I. Informant Is Tied to Cyberattacks Abroad," *New York Times*, April 23, 2014, <http://www.nytimes.com/2014/04/24/world/fbi-informant-is-tied-to-cyberattacks-abroad.html>
- <sup>3</sup> John Stockwell, *THE SECRET WARS OF THE CIA: part I*, lecture given in October, 1987, [http://www.thirdworldtraveler.com/Stockwell/StockwellCIA87\\_1.html](http://www.thirdworldtraveler.com/Stockwell/StockwellCIA87_1.html)
- <sup>4</sup> John Stockwell, *The Praetorian Guard: The U.S. Role in the New World Order*, South End Press, July 1, 1999.
- <sup>5</sup> John Young, "Wall Street Journal Secrecy," *Cryptome*, August 22, 2014, <http://cryptome.org/0002/wsj-secrecy.htm>
- <sup>6</sup> Peter Dale Scott, "The Deep State and the Wall Street Overworld", *Asia-Pacific Journal: Japan Focus*, March 10, 2014, [http://japanfocus.org/-Peter\\_Dale-Scott/4090](http://japanfocus.org/-Peter_Dale-Scott/4090)
- <sup>7</sup> Cindy Cohn and Nadia Kayyali, "The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible," *Electronic Frontier Foundation*, June 2, 2013, <https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible>
- <sup>8</sup> Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show" *Washington Post*, August 30, 2013
- <sup>9</sup> Nadia Kayyali, "The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why," *Electronic Frontier Foundation*, May 7, 2014, <https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why>
- <sup>10</sup> John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Post*, July 18, 2014, [http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2\\_story.html](http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html)
- <sup>11</sup> Mark Mazzetti And Jonathan Weisman, "Conflict Erupts in Public Rebuke on C.I.A. Inquiry," *New York Times*, March 11, 2014, <http://www.nytimes.com/2014/03/12/us/cia-accused-of-illegally-searching-computers-used-by-senate-committee.html>
- <sup>12</sup> Mark Mazzetti, "C.I.A. Admits Penetrating Senate Intelligence Computers," *New York Times*, July 31, 2014, <http://www.nytimes.com/2014/08/01/world/senate-intelligence-committee-cia-interrogation-report.html>
- <sup>13</sup> Molly Mulrain, "Former CIA Official: 'Cyber Will Be Key Component of Any Future Conflict'", *ExecutiveBiz*, August 4, 2011, <http://blog.executivebiz.com/2011/08/former-cia-official-cyber-will-be-a-key-component-of-any-future-conflict/>
- <sup>14</sup> Gerry Smith, "Cyber-Crimes Pose 'Existential' Threat, FBI Warns," *Huffington Post*, January 12, 2012, [http://www.huffingtonpost.com/2012/01/12/cyber-threats\\_n\\_1202026.html](http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html)
- <sup>15</sup> "U.S. Cyber Command Head General Alexander To Keynote Black Hat USA 2013," *Dark Reading*, May 14, 2013, <http://www.darkreading.com/risk/us-cyber-command-head-general-alexander-to-keynote-black-hat-usa-2013/d/d-id/1139741>

---

<sup>16</sup> Daniel E. Geer, "Cybersecurity and National Policy," *Harvard Law School National Security Journal*, Volume 1 – April 7, 2010, <http://harvardnsj.org/2011/01/cybersecurity-and-national-policy/>

<sup>17</sup> <https://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html#Black>

<sup>18</sup> <https://www.blackhat.com/html/bh-us-12/speakers/Shawn-Henry.html>

<sup>19</sup> Jim Finkle, "Defcon 2012 Conference: Hackers To Meet With U.S. Spy Agency Chief," *Reuters*, July 20, 2012, [http://www.huffingtonpost.com/2012/07/20/defcon-2012\\_n\\_1691246.html](http://www.huffingtonpost.com/2012/07/20/defcon-2012_n_1691246.html)

<sup>20</sup> Spencer Ackerman, "NSA keeps low profile at hacker conventions despite past appearances," *Guardian*, July 31, 2014, <http://www.theguardian.com/world/2014/jul/31/nsa-hacker-conventions-recruit-def-con-black-hat/print>

<sup>21</sup> George Smith, "Computer Security for the 1 Percent Day," *Escape From WhiteManistan*, May 19, 2014, <http://dickdestiny.com/blog1/?p=18011>

<sup>22</sup> <http://www.dhs.gov/homeland-security-advisory-council-members>

<sup>23</sup> Dan Goodin, "For first time ever, feds asked to sit out DefCon hacker conference," *Ars Technica*, July 11, 2013, <http://arstechnica.com/security/2013/07/for-first-time-ever-feds-asked-to-sit-out-defcon-hacker-conference/>

<sup>24</sup> Tim Shorrock, "Put the Spies Back Under One Roof," *New York Times*, June 17, 2013, <http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html>

<sup>25</sup> "'We Won't Succumb to Threats': Journalists Return to U.S. for First Time Since Revealing NSA Spying," *Democracy Now!* April 14, 2014, [http://www.democracynow.org/2014/4/14/we\\_wont\\_succumb\\_to\\_threats\\_journalists#](http://www.democracynow.org/2014/4/14/we_wont_succumb_to_threats_journalists#)

<sup>26</sup> "Inside the Web's \$156 Billion Invisible Industry," *Motherboard*, December 18, 2013, <http://motherboard.vice.com/blog/inside-the-webs-156-billion-invisible-industry>

<sup>27</sup> Spencer Ackerman, "NSA keeps low profile at hacker conventions despite past appearances," *Guardian*, July 31, 2014, <http://www.theguardian.com/world/2014/jul/31/nsa-hacker-conventions-recruit-def-con-black-hat/print>

<sup>28</sup> Andrea Shalal and Jim Finkle, "U.S. may act to keep Chinese hackers out of Def Con hacker event," *Reuters*, May 24, 2014, <http://www.reuters.com/article/2014/05/24/us-cybercrime-usa-china-idUSBREA4N07D20140524>