GlobalResearch
Center for Research on Globalization

9/11 and Cyberterrorism

Did the real "cyber 9/11" happen on 9/11?

By James Corbett
Global Research, July 17, 2009
The Corbett Report 17 July 2009
Theme: Intelligence, Terrorism

Government sources immediately began blaming North Korea for the recent cyberterror attacks on South Korea and the U.S., despite having no evidence to back up those claims.[1] Now, an examination of the evidence by independent computer experts show that the attack seems to have been coordinated from the UK.[2] The hysterical media coverage in the attack's wake, however, echoing the government line that it was likely the work of North Korea, has served to cement in the minds of many that this was an act of cyberwarfare.

The idea that this surprisingly unsophisticated attack[3] could have come from a well-organized, hostile state or terrorist group comes as a blessing in disguise to those groups, agencies and advisors who have been calling for greater and greater federal snooping powers in the name of stopping a "cyber 9/11" from happening.

The "cyber 9/11" meme stretches back almost to 9/11 itself. Back in 2003, Mike McConnell, the ex-director of the National Security Agency (NSA), was fearmongering over the possibility of a cyber attack "equivalent to the attack on the World Trade Center" if a new institution were not created to oversee cyber security.[4] Since then, report[5] after report[6] has continued to use the horror of 9/11 as a way of raising public hysteria over "cyber terrorism," a subject more often associated with juvenile hackers and lone misfits than radical terrorist organizations.

The real reason behind the invocation of 9/11 in the context of "cyber terror" was revealed last year by Harvard law professor Lawrence Lessig. He told a technology conference that former counterterrorism czar Richard Clarke admits there is a cyber equivalent of the constitution-destroying Patriot Act ready to be rubber stamped into law; all it requires is a "cyber 9/11" to make such legislation politically viable.[7] In effect, the cyber security establishment-the advisors, agents and experts in the newly-minted multi-billion dollar cyber security industry[8]-are waiting for a spectacular cyber terrorist attack to go ahead with plans for 'identity management' schemes like fingerprinting for internet access which would put an end to the free Internet as we have known it.[9]

What the cyber security establishment does not want you to know is that the most incredible cyber terrorist story of all time began 15 years ago. And it centers on 9/11. The establishment is interested in suppressing this story because it demonstrates that the very investigative bodies that are clamoring for more power on the pretext of the "cyber terror" hysteria are the exact same bodies that failed to investigate the documentable links between government-designated terrorists and a software company with direct access to some of the most sensitive computer systems in the United States. FBI agents whose investigation into this story were suppressed have even said that these investigations could have prevented 9/11.

It is a story of international terror and terrorist financiers. It stretches from New England to Saudi Arabia and involves businessmen, politicians and terror networks. And it begins in the most unlikely of places: the offices of an enterprise architecture software firm in Quincy, Massachusetts.

Enterprise Architecture: The God's-Eye View of Systems and Infrastructure

"Enterprise architecture software" refers to a computer program that allows someone to look at all of the data produced throughout an organization's structure in real time. This effectively gives the program user a god's-eye view of an enterprise, allowing for the mapping, visualization and analysis of all transactions, interactions, systems, processes and personnel in the entirety of a business or agency. This type of software could, for example, be used for robust business modeling, allowing for extremely detailed and accurate projections of how changes in an organization's structure or processes would effect a business' bottom line. What would happen if two departments were merged, for example, or if a business were to outsource one of its processes.

As this software began to mature in the 1990s, however, it went from a merely useful tool to something truly incredible. Sophisticated enterprise architecture software could, for example, examine all of the transactions taking place across a financial institution in real time and examine that data for possible money laundering operations or rogue traders. Such software could even have potentially detected and identified the insider trading leading up to 9/11.[10] Combined with rudimentary a.i. capabilities, such a program would not only be able to alert the appropriate personnel about such transactions, but even stop them as they are happening. If the software were sophisticated enough, it may even be able to identify the possibility of such transactions before they happen.

The utility of such software for organizations of all stripes should be obvious enough. It is unsurprising, then, that numerous government agencies and powerful corporations were hungry for this software in the 1990s. A surprising number of them, including DARPA, the FBI, the Secret Service, the White House, the Navy, the Air Force, the FAA, NATO, IBM, Booz Allen Hamilton and Price Waterhouse Coopers (amongst many others) turned to a small New England-based software firm called Ptech.[11]

Ptech: Not Your Average Software Firm

Ptech was founded in Quincy, Mass. in 1994 and by 1996 had secured a contract with DARPA to help transfer commercial software methodologies to the defense sector.[12] In 1997, it gained security clearance to bid on sensitive military contracts and bid on work for a range of other government agencies.[13] Within four years Ptech had built up a stable of clients that would make any third-party software vendor green with envy. From the inner sanctum of the White House to the headquarters of the FBI, from the basement of the FAA to the boardroom of IBM, some of the best-secured organizations in the world running on some of the most protected servers housing the most sensitive data welcomed Ptech into their midst. Ptech was given the keys to the cyber kingdom to build detailed pictures of these organizations, their weaknesses and vulnerabilities, and to show how these problems could be exploited by those of ill intent. For all of its incredible success, however, many of the firm's top investors and employees were men with backgrounds that should have been raising red flags at all levels of the government.

The firm was founded on $20 million of startup money, $5 million of which was provided by

Yassin al-Qadi[14], a wealthy and well-connected Saudi businessman who liked to brag about his acquaintance with Dick Cheney.[15] He also had connections to various Muslim charities suspected of funding international terrorism.[16] In the wake of 9/11 he was officially declared a Specially Designated Global Terrorist by the U.S. government and his assets were frozen.[17] At the time, Ptech's owners and senior management denied that al-Qadi had any involvement with the company other than his initial investment, but the FBI now maintains they were lying and that in fact al-Qadi continued investing millions of dollars in the company through various fronts and investment vehicles. [18] Company insiders told FBI officials that they were flown to Saudi Arabia to meet Ptech's investors in 1999 and that al-Qadi was introduced as one of the owners.[19] It has also been reported that Hussein Ibrahim, Ptech's chief scientist, was al-Qadi's representative at Ptech[20] and al-Qadi's lawyers have admitted that al-Qadi's representative may have continued to sit on Ptech's board even after 9/11.[21]

Ibrahim himself was a former president of BMI, a New Jersey-based real estate investment firm that was also one of the initial investors in Ptech and provided financing for Ptech's founding loan. Ptech leased office space and computer equipment from BMI[22] and BMI shared office space in New Jersey with Kadi International, owned and operated by none other than Ptech's sweetheart investor and Specially Designated Global Terrorist, Yassin al-Qadi.[23] In 2003, counterterrorism czar Richard Clarke said: "BMI held itself out publicly as a financial services provider for Muslims in the United States, its investor list suggests the possibility this facade was just a cover to conceal terrorist support." [24]

Suheil Laheir was Ptech's chief architect. When he wasn't writing the software that would provide Ptech with detailed operational blueprints of the most sensitive agencies in the U.S. government, he was writing articles in praise of Islamic holy war. He was also fond of quoting Abdullah Azzam, Osama Bin Laden's mentor and the head of Maktab al-Khidamat, which was the precursor to Al-Qaeda.[25]

That such an unlikely cast of characters were given access to some of the most sensitive agencies in the U.S. federal government is startling enough. That they were operating software that allowed them to map, analyze and access every process and operation within these agencies for the purpose of finding systemic weak points is equally startling. Most disturbing of all, though, is the connection between Ptech and the very agencies that so remarkably failed in their duty to protect the American public on September 11, 2001.

Ptech on 9/11: The Basement of the FAA

For two years prior to 9/11, Ptech was working to identify potential problems or weaknesses in the FAA's response plans to events like a terrorist hijacking of a plane over U.S. airspace. According to their own business plan for their contract with the FAA, Ptech was given access to every process and system in the FAA dealing with their crisis response protocols. This included examining key systems and infrastructure to analyze the FAA's "network management, network security, configuration management, fault management, performance management, application administration, network management and user desk help operations." [26] In short, Ptech had free reign to examine every FAA system and process for dealing with the exact type of event that was to occur on 9/11. Even more incredible, researcher Indira Singh points out that Ptech was specifically analyzing the potential interoperability problems between the FAA, NORAD and the Pentagon in the event of an emergency over U.S. airspace.[27]

Ptech also presumably had operational information about the systems that the FAA, NORAD and others employed during crisis response exercises like Vigilant Guardian[28], the NORAD exercise that was taking place on 9/11 and included simulations of hijacked jets being flown into New York[29] and hijacked jets being flown into government buildings.[30] This is significant because there is every indication that just such drills were confusing NORAD's response to the real hijackings that were taking place that day. As researcher Michael Ruppert points out, a rogue agent with access to a Ptech backdoor into the FAA's systems could have been deliberately inserting fake blips onto the FAA's radars on 9/11[31]. That scenario would explain the source of the phantom Flight 11 that the FAA reported to NORAD at 9:24 a.m. (well after Flight 11 had already hit the World Trade Center)[32], a report whose source the 9/11 Commission claims they were unable to find.[33]

In short, Ptech's software was running on the critical systems responding to the attacks of 9/11 on 9/11 itself. The software was designed for the express purpose of giving its users a complete overview of all the data flowing through an organization in real time. The father of enterprise architecture himself, John Zachman, explained that with Ptech-type software installed on a sensitive server "You would know where the access points are, you'd know how to get in, you would know where the weaknesses are, you'd know how to destroy it."[34]

Stifled Investigations

In the late 1990s, Robert Wright-an FBI special agent in the Chicago field office-was running an investigation into terrorist financing called Vulgar Betrayal.[35] From the very start, the investigation was hampered by higher-ups; the investigation was not even allocated adequate computers to carry out its work.[36] Through Wright's foresight and perseverance, however, the investigation managed to score some victories, including seizing $1.4 million in U.S. funds that traced back to Yassin al-Qadi.[37] Wright was pleased when a senior agent was assigned to help investigate "the founder and the financier of Ptech", but the agent did no work and merely pushed papers during his entire time on the case.[38]

Shortly after the 1998 African embassy bombings, Vulgar Betrayal began to uncover a money trail linking al-Qadi to the attack.[39] According to Wright, when he proposed a criminal investigation into the links, his supervisor flew into a rage, saying "'You will not open criminal investigations. I forbid any of you. You will not open criminal investigations against any of these intelligence subjects." Wright was taken off the Vulgar Betrayal investigation one year later and the investigation itself was shut down the following year.

In the aftermath of 9/11, Indira Singh-a risk management conultant for JP Morgan-was looking for enterprise architecture software to implement the next generation of risk management at the financial juggernaut. Impressed by their client list, Singh invited Ptech to demonstrate their software. It wasn't long before she began discovering the connections between Ptech and international terrorist financing. She worked exhaustively to document and uncover these links in an effort to persuade the FBI in Boston to open their own investigation into Ptech, but she was told by one agent that she was in a better position to investigate this than someone inside the FBI.[40] Despite the persistent efforts of Singh and the testimony of company insiders, the FBI did not inform any of the agencies contracting with Ptech that there were concerns about the company or its software.

In late 2002, Operation Green Quest-a Customs Department-led multi-agency investigation into terrorist financing-raided Ptech's offices due to its ties to al-Qadi and others.[41] The

very same day of the raid White House Press Secretary Ari Fleischer declared the company and its software safe.[42] Mainstream news articles defending Ptech after the story broke, however, blithely admit that the company was informed of the raid weeks in advance, hoping perhaps that readers will not notice that his completely defeats the purpose of such a raid or calls into question its results.[43] Eventually, Michael Chertoff led an effort to give the FBI total control over Greenquest, leading to Customs officials accusing him of sabotaging the investigation.[44] No indictments were laid in the immediate aftermath of the Ptech raid against al-Qadi or anyone else related to the company. Chertoff went on to become the head of Homeland Security.

The 9/11 Commission Report, obviously, does not mention Ptech. Given the incredible information about this company and its links to Specially Designated Global Terrorist Yassin al-Qadi, this is perhaps surprising. This startling omission becomes more ominous however, when it is understood that the 9/11 Commission co-chair, Thomas Kean, made $24 million dollars off a land deal with al-Qadi linked organization BMI.[45]

For over a decade, investigations into Ptech, its employees and its investors have been stifled, suppressed or derailed by people in key positions. But all of that finally changed this week.

A Break in the Case

On Wednesday, the Boston Field Office of the FBI unsealed a 2007 indictment of Oussama Ziade, Ptech's former CEO, and Buford George Peterson, the former CFO and COO.[46] The indictment charges that the pair knowingly lied to investigators about the extent of al-Qadi's investments and ties with Ptech. Another unsealed indictment, this one from 2005, alleges Ziade attempted to engage in transactions involving al-Qadi's property, a federal offence as al-Qadi was a Specially Designated Global Terrorist at the time. If the pair are convicted on the charges, they face 30 years in prison and a $1 million fine.

Whether this represents a significant breakthrough in the case and the beginning of the official unraveling of the Ptech story will likely depend on whether political pressure is brought to bear by an informed public who are concerned with this story. Given that the public has been whipped into cyber-hysteria over the North Korean figments of the government's imagination, it will require the media to stop parroting the government's talking points and begin informing the public about the very real, documentable links between terrorist financiers and the technological capability to override key emergency response systems on 9/11.

Two questions remain to be answered: Did the real "cyber 9/11" happen on 9/11? And will the public care enough to demand the answer to that question? If the answer to either question is 'yes,' concerned readers are advised to download the mp3 file of Episode 045 of The Corbett Report podcast, "Ptech and the 9/11 software," and begin distributing it to others to bring awareness to this incredible story.[47]

Notes

[1] http://antifascist-calling.blogspot.com/2009/07/behind-cyberattacks-on-america-and.html
[2] http://blog.bkis.com/?p=718
[3] http://www.wired.com/threatlevel/2009/07/mydoom/
[4]

http://www.smh.com.au/cgi-bin/common/popupPrintArticle.pl?path=/articles/2003/04/21/1050777200225.html
[5]
http://www.nationalterroralert.com/updates/2008/04/10/michael-chertoff-cyber-terror-threats-on-par-with-911/
[6]
http://voices.washingtonpost.com/securityfix/2009/04/digital_pearl_harbor_cyber_911.html
[7] http://www.infowars.net/articles/august2008/050808i911.htm
[8] http://www.nytimes.com/2009/05/31/us/31cyber.html?_r=1
[9] http://www.csmonitor.com/2005/0602/p01s04-ussc.htm
[10] http://www.business.uiuc.edu/poteshma/research/poteshman2006.pdf
[11] http://en.wikipedia.org/wiki/Ptech
[12] http://www.govexec.com/archdoc/rrg96/0996rrg5.htm
[13] http://www.islamicsupremecouncil.org/CMS/Topics/insideUS/1218159502002.htm
[14] http://www.boston.com/news/daily/03/ptech.htm
[15] http://www.saudia-online.com/newsoct01/news30.shtml
[16] http://www.historycommons.org/context.jsp?item=a91qlimoney#a91qlimoney
[17] http://ustreas.gov/press/releases/po689.htm
[18] http://boston.fbi.gov/dojpressrel/pressrel09/bs071509.htm
[19] http://www.historycommons.org/context.jsp?item=a99alqadiptech#a99alqadiptech
[20] http://www.historycommons.org/context.jsp?item=a94ptechbmi#a94ptechbmi
[21] http://www.historycommons.org/context.jsp?item=a99alqadiptech#a99alqadiptech
[22] http://www.boston.com/news/daily/03/ptech.htm
[23] http://www.investigativeproject.org/documents/case_docs/81.pdf
[24] http://www.investigativeproject.org/documents/testimony/77.pdf
[25] http://www.frontpagemag.com/readArticle.aspx?ARTID=8245
[26] http://www.fromthewilderness.com/free/ww3/012705_ptech_pt2.shtml
[27] ibid.
[28] http://www.911readingroom.org/whole_document.php?article_id=278
[2 9]
http://hcgroups.wordpress.com/2009/06/14/two-days-before-911-military-exercise-simulated-suicide-hijack-targeting-new-york/
[3 0]
http://www.boston.com/news/packages/sept11/anniversary/wire_stories/0903_plane_exercise.htm
[31] http://www.fromthewilderness.com/free/ww3/012705_ptech_pt2.shtml
[32] http://www.911blogger.com/node/19181
[33] http://www.msnbc.msn.com/id/5233007
[34] http://www.nationalcorruptionindex.org/pages/profile.php?profile_id=6
[35] http://www.laweekly.com/2004-08-26/news/a-vulgar-betrayal
[36] http://www.foxnews.com/story/0,2933,54070,00.html
[37] http://www.apfn.org/apfn/Wtc_whistleblower3.htm
[38] http://www.historycommons.org/context.jsp?item=a0498nowork#a0498nowork
[3 9]
http://web.archive.org/web/20021220054102/http://www.abcnews.go.com/sections/primetime/DailyNews/FBI_whistleblowers021219.html
[40] http://www.911blogger.com/2005/07/indira-singh-ptech-researcher.html
[41] http://archives.cnn.com/2002/US/Northeast/12/06/ptech.raid/
[42] http://www.forbes.com/2002/12/06/cx_ah_1206raid.html
[43] http://www.boston.com/news/daily/03/ptech.htm

[44] http://www.newsweek.com/id/58250/output/print
[45] http://www.insider-magazine.com/911Kean.pdf
[46] http://boston.fbi.gov/dojpressrel/pressrel09/bs071509.htm
[47] http://www.corbettreport.com/index.php?ii=88&i=Documentation

---

Articles by: **James Corbett**

About the author:

James Corbett is a Film Director and Producer based in Okayama, Japan. He started The Corbett Report (www.corbettreport.com) website in 2007 as an outlet for independent critical analysis of politics, society, history, and economics. It operates on the principle of open source intelligence and provides podcasts, interviews, articles and videos about breaking news and important issues from 9/11 Truth and false flag terror to the Big Brother police state, eugenics, geopolitics, the central banking fraud and more.