Profiting from 9/11: The Private Company that Played a Major Role in the "War on Terror"

By Kevin Ryan

Global Research, June 05, 2014
Dig Within 4 June 2014

Region: USA
Theme: Terrorism

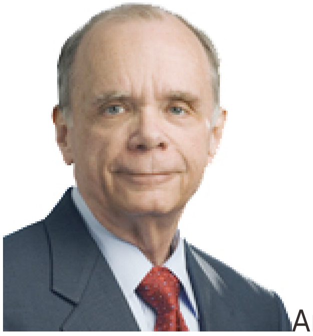
Both before and after 9/11, one private company had a greater impact on counterterrorism programs in the United States than any other. That company, Science Applications International Corporation (SAIC), also profited more from the events of 9/11 than any other. Its chief operating officer (COO), Duane Andrews, was a man who had expertise-level knowledge of the vulnerabilities that were exploited on 9/11. He also just happened to be a long-time, close colleague of Dick Cheney and Donald Rumsfeld.

SAIC business activity is related to incidence of terrorism, having won many of its record number of government contracts through the national security state that has arisen via the War on Terror. Through its numerous contracts and employee security clearances, it has become a private business that cannot be distinguished from a permanent form of government. In short, SAIC is "the fraternal twin of the intelligence establishment."[1]

With regard to 9/11, SAIC's impact cannot be overstated as the company:

- Created the national databases that tracked and identified terrorists
- Supplied U.S. airports with terrorism screening equipment
- Predicted and investigated terrorist attacks against U.S. infrastructure including national defense networks and the World Trade Center (WTC)
- Helped create the official account for what happened at the WTC both in 1993 and after 9/11
- Was a leader in research on thermitic materials like those found in the WTC dust[2]
- Employed the leader of the robotics team that scoured the pile at Ground Zero, using equipment capable of eliminating explosives
- Provided the information to capture the alleged mastermind of the attacks, Khalid Sheik Mohammed (KSM)

Furthermore, Dick Cheney's long-time protégé, Duane P. Andrews, ran SAIC's government business for thirteen years, from 1993 to 2006, and was therefore a principal actor in these activities. During this time, Andrews was also a leading corporate representative on government commissions and task forces that evaluated threats to U.S. defense and information systems.



Andrews' history with Cheney goes back decades. In the Vietnam War, he was a special operations soldier in the U.S. Air Force. He then got a position as a staff member for the U.S. House Intelligence Committee. During his time in that position, Cheney was a prominent member of the House Intelligence Committee along with Lee Hamilton, the future 9/11 Commission vice-chairman.

Later, George H.W. Bush nominated Andrews for the post of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I). This led to Andrews being personally responsible for giving Secretary of Defense Cheney his daily intelligence briefs.

Cheney and Andrews used false information to start the Gulf War. This included satellite photos allegedly showing a build-up of Iraqi troops on the Saudi Arabian border, which were later shown by *St. Petersburg Times* reporter Jean Heller to represent a false claim.[3] The false information also included the testimony of the 15-year old Kuwaiti royal, Nayirah.

Andrews left the Pentagon in 1993 to become President and COO of SAIC's federal business, which accounted for a majority of the company's revenues. Andrews personally managed SAIC's programs for the National Security Agency (NSA), and other agencies within the U.S. intelligence community, in the years leading up to 9/11 and afterward.

As the man hired to defend the U.S. against attacks on its defense information systems, Andrews became a critical part of the national security apparatus. All the while, he continued to consider Dick Cheney his personal, lifelong hero.[4]

SAIC and the road to 9/11

SAIC worked for many years in close partnership with oil-rich royals in the Middle East, particularly those that have become suspect with regard to 9/11. The first international contract that the company won was for training the Kuwaiti Defense Forces, starting in 1976. Three years later, SAIC secured its biggest and longest lasting international contract, training the Saudi Arabian navy.

In 1986, SAIC was hired by the Port Authority of New York and New Jersey (PANYNJ) "to conduct a general security review of the WTC" with respect to terrorism. SAIC's report rated the public areas of the WTC as very attractive targets for terrorism, emphasizing especially the basement levels.[5] Perhaps coincidentally, the Kuwaiti-owned security company Stratesec was hired by the PANYNJ in 1991 to provide a similar review and report.

After Andrews joined the company, SAIC was hired to investigate the 1993 bombing of the WTC, an event that was remarkably like the one that it had foreseen in 1986.[6] Moreover, SAIC ultimately provided input that led to producing the official account of what happened. The company boasted that — "*After the 1993 World Trade Center bombing, our blast* *analyses produced tangible results that helped identify those responsible*."[7]

In the early 1990s, SAIC was also a leader in developing technology for aviation security. At the time, SAIC had been contracted by a congressional advisory panel, led by L. Paul Bremer and Brian Michael Jenkins among others, to evaluate terrorist threats with regard to airport security.[8] By 1994, the company's explosives detection equipment was installed in major airports around the country, including in New York City, Miami, and Washington, DC.[9]

Under Andrews, SAIC was heavily focused on analyzing risks to U.S. defense information systems and led the partnership between the U.S. government and industry in that area. As the chairman of a Defense Science Board taskforce on information warfare, Andrews learned about the specific vulnerabilities of U.S. national defense systems. In early 1997, he reported to Congress that U.S. defense systems were a "target-rich environment" and that attacks on certain facilities and information systems "would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions."[10] Andrews went on to build and secure the Defense Information System Network (DISN). The secret component of the DISN, which was called SIPRnet, linked command and control systems throughout the United States.

As of March 2001, SAIC was also part of the National Coordinating Center for telecommunications (NCC). NCC provided oversight to the agency that, on the morning of 9/11 but before the attacks began, implemented a secret communications system (SRAS) for the first time. The system had been developed in conjunction with the Continuity of Government (COG) plans that Dick Cheney had worked on for nearly twenty years along with Richard Clarke, who implemented COG for the first time as the events of 9/11 proceeded.[11]

The fact that Andrews was the most knowledgeable person in terms of the vulnerabilities of information and communications networks for U.S. national security seems a worthy point for further consideration. That's because so many inexplicable problems occurred with defense communications networks on 9/11, including the following.

- There were serious problems with the National Military Command Center's conference calls that morning. Important participants could not be connected or were repeatedly dropped from the calls, including the FAA.[12]
- U.S. national security facilities were in an information void on 9/11. Agencies that should have known the most about an ongoing terrorist event were blind to the ongoing attacks.[13]
- The SIPRnet did not have any information about the attacks even as late as the afternoon of 9/11.[14]
- President Bush complained of poor communications in that he "could not reach key officials, including Rumsfeld" and "The line to the White House shelter conference room – and the Vice-President- kept cutting off."[15]

In the mid-1990s, SAIC created the U.S. systems for tracking terrorist suspects. For the FBI, SAIC developed CODIS, the national DNA database, and NCIC, the national criminal background check system.[16] To clarify, when in August 2001 Robert Fuller of the FBI went to search for Khalid Al-Mihdhar and Nawaf Al-Hazmi's alleged presence in the United States via the NCIC system, he was checking a database built by SAIC. Although Fuller found nothing, the *9/11 Commission Report* said that such checks should have unearthed driver's licenses, car registrations, and telephone listings for Al-Mihdhar and Al Hazmi, all of which were in their names.[17] This fact alone should be enough to call for the investigation of SAIC with regard to 9/11.

SAIC purchased Boeing Information Services (BIS) in 1999. BIS specialized in information systems integration, logistics, networking, and outsourcing, and dealt with management of data communications to Boeing aircraft. Its work in progress included "a five-year Defense Information Systems Network contract with the Defense Information Systems Agency", and "the Army's Reserve Component Automation System, a 12-year contract worth $1.6 billion that the company won in 1991."[18]

Andrews was a member of Donald Rumsfeld's commission on national security uses of space. This commission argued that the US should avoid international agreements that limit the deployment of weapons in space, and that, in order to avoid a "Space Pearl Harbor," the US needed to "develop the capability for power projection in, from, and through space."[19] As a result, SAIC's missile defense contracts tripled between 2001 and 2004, going from $47 million to $169 million in value.

SAIC and the WTC After 9/11

It turns out that SAIC was one of the first organizations to show up at Ground Zero. The company claimed in its 2004 shareholder report that — "Following the September 11, 2001, terrorist attacks, we responded rapidly to assist a number of customers near ground zero in New York City and in Washington, D.C."[20] In one of these instances, "SAIC technicians raced to Ground Zero within hours to install an ad hoc communications network for first responders and local financial companies."[21] Therefore, SAIC was in control of at least some of the communications at Ground Zero.

Perhaps the most interesting SAIC connection to the cleanup was John Blitch, a lieutenant colonel in the U.S. Army's Special Forces, who was said to have retired from the Army just the day before 9/11. It was reported that Blitch was "filling out the paperwork in an out-processing office of the Pentagon on the morning of September 10, 2001," and that after "three years at the helm of the Defense Department's Tactical Mobile Robots Program," he was "leaving to direct the Center for Intelligent Robotics and Unmanned Systems at the Science Applications International Corporation."[22]

Instead of traveling to his SAIC office in Colorado on 9/11, as he had planned, "Blitch scrapped the trip…and headed for New York. On the road, Blitch donned his fatigues, dug out his military ID, and worked his cell phone, summoning colleagues from Florida to Boston to pack up their finest tactical robots and rendezvous at Ground Zero." And "Over the next 11 days, the group's 17 robots squeezed into spaces too narrow for humans, dug through heaps of scalding rubble, and found seven bodies trapped beneath the mountains of twisted steel and shattered concrete."[23]

Blitch was experienced at such search missions, and had done "ground-breaking research in robot assisted search and rescue conducted during the Oklahoma City Bombing response".[24] By May 2001, laser technology was being used by Blitch's robot program. It was reported that — "Robots are performing quite successfully in the field of explosive ordnance disposal (EOD)"… and "EOD units [include] a laser weapon for ordnance neutralization…[used to] burn unexploded ordnance."[25]

Therefore, SAIC had the means and opportunity to neutralize any unwanted explosives that might have been buried in the pile at Ground Zero. That's interesting in that SAIC supplied the largest contingent of non-governmental investigators to the NIST WTC investigation after 9/11. That investigation went to great lengths in order to avoid consideration of explosives.

Manufacturing and Profiting From War

SAIC went on to play an integral role in the "War on Terror", and was even responsible for capturing Khalid Sheikh Mohammed. It was SAIC staff and technology that "tease[ed] out crucial clues about Mohammed's activities from intercepted text messages that he sent to his al Qaeda operatives using as many as 20 different cell phones."[26]

After 9/11, SAIC was hired to fix the problems it had created with terrorist tracking systems. Duane Andrews was personally in charge of the project called Trailblazer, which was originally launched in 1999 but ostensibly was not tested for operational use by the U.S. government until six years later. The system was meant to translate all NSA intercepts, including telephone, email and other electronic information, into actionable intelligence.

An oft-cited example of the failures that Trailblazer was meant to avoid was the reported incident in which messages stating "tomorrow is zero hour" and "the match begins tomorrow" were intercepted by the NSA on September 10, 2001 but not translated until September 12th. The Trailblazer system was not the answer to those problems, however, and was ultimately a total failure. After 6 years and $1.2 billion spent, the NSA cancelled the project in 2005.

Another huge failure led by SAIC was with the FBI system called Virtual Case File (VCF), which was intended to solve the supposed information sharing problem that prevented the FBI from tracking terrorists like Al-Mihdhar and Al-Hazmi, who lived for years with an FBI informant. VCF was meant to provide a centralized database of terrorism related information that all FBI agents could utilize. However, after three years and hundreds of millions in costs, VCF was written off as "the most highly publicized software failure in history."[27]

SAIC's 9/11 profiteering didn't stop there. While helping NIST to determine the causes of the WTC destruction, "SAIC personnel were instrumental in pressing the case that weapons of mass destruction existed in Iraq under Saddam Hussein, and that war was the only way to get rid of them."[28] The company helped supply the faulty intelligence that said Saddam had WMDs and then profited from the invasion by generating Iraq contracts worth billions of dollars. In 2003 alone, SAIC pulled in $5.4 billion in government revenue.

With the help of SAIC, John Poindexter of Iran-Contra fame was able to convince the U.S. government to hire him to ensure "Total Information Awareness" as a result of the 9/11 attacks. Through related programs, SAIC won major contracts for management of huge IT systems that involved spying on Americans and running the Joint Intelligence Operations Centers (JIOCs).[29]

Considering the incredible growth in contracts that SAIC realized from the events of 9/11, any independent investigation into those events should carefully consider the role played by that company and its leadership. Andrews and his company were integral to the counterterrorism programs of the United States in the years prior to 9/11. The company's role included creating the national databases that tracked and identified terrorists, supplying airport screening equipment, predicting and investigating terrorist attacks against the WTC, helping to create the official account for what happened at the WTC after 9/11, and providing the information to capture KSM. Undoubtedly, SAIC's impact on the counterterrorism programs of the United States prior to 9/11 was unique and pervasive.

Duane Andrews should be a person of specific interest because he had expert knowledge of the vulnerabilities of the U.S. defense and information systems at a time when many of those systems failed catastrophically. If anyone knew how to exploit weaknesses in the telecommunications and electronic systems of the U.S. defense department, it was Duane Andrews. His history of being closely aligned with the activities of Dick Cheney and Donald Rumsfeld, for the twenty years prior to 9/11, provides additional reason to suspect him.

Notes

[1] Donald L. Barlett and James B. Steele, Washington's $8 Billion Shadow, Vanity Fair, March 2007, http://www.vanityfair.com/politics/features/2007/03/spyagency200703

[2] Kevin R. Ryan, The Top Ten Connections Between NIST and Nanothermites, Journal of 9/11 Studies, July 2008

[3] Morris Berman, Dark Ages America: The Final Phase of Empire, W. W. Norton & Company, 2011

[4] Laura Rozen, The First Contract, The American Prospect, March 30, 2007,http://www.prospect.org/cs/articles?articleId=12612

[5] New York County Supreme Court, Matter of World Trade Ctr. Bombing Litig, 2004 NY Slip Op 24030 [3 Misc 3d 440], January 20, 2004

[6] New York State Law Reporting Bureau, In The Matter of World Trade Center Bombing Litigation, 2004 NY Slip Op 24030 [3 Misc 3d 440], January 20, 2004, http://www.courts.state.ny.us/reporter/3dseries/2004/2004_24030.htm

[7] Science Applications International Corporation, Annual Report 2004http://www.saic.com/news/pdf/Annual-Report2004.pdf

[8] U.S. Congress, Office of Technology Assessment, Technology Against Terrorism: The Federal Effort, OTA-ISC-481, Washington, DC: U.S. Government Printing Office, July 1991.

[9] A. Maureen Rouhi, Government, Industry Efforts Yield Array Of Tools To Combat Terrorism, Chemical & Engineering News, July 24, 1995

[10] Statement by Duane P. Andrews, Chairman, Defense Science Board Task Force on Information Warfare & Defense,https://www.fas.org/irp/congress/1997_hr/h970320a.htm

[11] Matthew Everett, Backup Communications System Was 'Miraculously' Switched on for 'Exercise Mode' and Ready for Use on 9/11, Shoestring 9/11, January 10, 2011,http://shoestring911.blogspot.com/2011/01/backup-communications-system-was.html

[12] Matthew Everett, The Repeatedly Delayed Responses of the Pentagon Command Center on 9/11, Shoestring 9/11, November 7, 2010

[13] Matthew Everett, Why Were U.S. Intelligence Facilities in an 'Information Void' During the 9/11 Attacks?, Shoestring 9/11, August 19, 2012

[14] Ibid

[15] The 9/11 Commission Report, p 40. Note that these communication failures helped ensure that the President was out of the loop for a longer period of time.

[16] Science Applications International Corporation, Press Release, August 24, 1994

[17] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, 2004, p 539

[18] Nick Wakeman, Boeing Information Services Sale Has Industry Abuzz, Washington Technology, Jan 21, 1999

[19] Report of the Commission to Assess United States National Security Space Management and Organization

[20] SAIC shareholder report, 2004,http://files.shareholder.com/downloads/SAIC/0x0x208149/64117BC7-5895-497E-A8EB-158A6E57012C/AR_2004.pdf

[21] William Launder, Homeland Security Goes Public, Forbes.com, 08.03.06,http://www.forbes.com/2006/08/02/saic-homeland-security-ipo-cx_wl_0803saic.html

[22] Michael Behar, The New Mobile Infantry: Battle-ready robots are rolling out of the research lab and into harm's way, Wired, Issue 10.05 | May 2002,http://www.wired.com/wired/archive/10.05/robots.html

[23] Ibid

[24] American Android Corp webpage, About Us,http://www.americanandroid.com/about.jb.html

[25] Sandra I. Erwin, Battlefield Robots: Not Just 'Entertainment', National Defense, May 2001,http://www.nationaldefensemagazine.org/archive/2001/May/Pages/Battlefield_Robots4252.aspx

[26] Paul Kaihla, US: In The Company Of Spies, CorpWatch, May 1st, 2003,http://www.corpwatch.org/article.php?id=7892

[27] Harry Goldstein, Who Killed the Virtual Case File?: How the FBI blew more than $100 million on case-management software it will never use, IEEE Spectrum, September 2005

[28] Charlie Cray, "Science Applications International Corporation," CorpWatch,http://www.corpwatch.org/section.php?id=17 ; cf. Barlett and Steele, "Washington's $8 Billion Shadow."

[29] Tim Shorrock, QinetiQ Goes Kinetic: Top Rumsfeld Aide Wins Contracts from Spy Office He Set Up, CorpWatch, January 15, 2008

The contents of this article as well as the view expressed are of sole responsibility of the author. The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article.

The original source of this article is Dig Within

Articles by: **Kevin Ryan**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca