Date: Mon, 16 Nov 2009 16:22:01 -0500
To: "Dr. Baruch Fischhoff - Chair, National Academy study on improving intelligence" <baruch@cmu.edu>
From: Lloyd Etheredge <lloyd.etheredge@policyscience.net>

Subject: 29. Strong, Embedded Barriers: Civic Guarantees

Cc: "Dr. Philip Tetlock" <tetlock@haas.berkeley.edu>, bruce.buenodemesquita@nyu.edu, edward.kaplan@yale.edu, tom.fingar@stanford.edu, tinsleyc@georgetown.edu, zegart@ucla.edu, arkes.1@osu.edu, stevekoz@msu.edu, gary.mcclelland@colorado.edu, kskinner@andrew.cmu.edu, bwanchisen@nas.edu, "Dr. Reid Hastie - NAS Project on Improving Intelligence" <reid.hastie@chicagobooth.edu>, "Dr. Robert Keohane - National Academy of Sciences"<rkeohane@princeton.edu>, "Amb. John Negroponte" <chutt@maglobal.com>, "Dr. Richard Atkinson - Chair - NRC/DBASSE" <rcatkinson@ucsd.edu>

Dear Dr. Fischhoff and Study Group Members:

Unexpectedly, the digital age (and the early 9/11 and anthrax attacks in the US) has secured for the US, NATO, and other governments a global surveillance system with linked databases (including surveillance cameras) that would have been beyond the dreams of even the most totalitarian governments in history. It is timely to assure that the designs of all databases and analysis capabilities deeply embed - i.e., in their physical design and software code - barriers to illegitimate use.

The DNI and all 200,000+ US employees are legally obligated to honor and guarantee civil liberties standards. However Bamford's The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping of America (2008) ends with a cautionary chapter and report that, public assurances not withstanding, the guarantees by Executive branch personnel are verbal and are not embedded at the level of software code and physical hardware (pp. 344-354).

US Nuclear Weapons Control as a Model

US control systems for arming and launching nuclear weapons illustrate the range of options and safeguards that I believe your Report should discuss and, based on social science research, recommend.

- These include (i*nter alia*) automatic, real-time transmission of alarms about unauthorized data, access of databases, and analysis that computers send directly to distant, independent, monitoring officials - e.g., the DNI, to Congressional Committees and to oversight courts.

- The launching of ICBMs required authenticated codes that changed daily and simultaneous and independent concurrence and physical actions (keys to be turned) by two officers, each equipped with firearms and with the duty to kill the other officer rather than permit an unauthorized/unauthenticated launch. The requirement for daily-changed authentication codes and independent physical actions - for example by an employee of the Executive branch and a court oversight official - would be straightforward to design.

- We are not designing safeguards for the Obama Administration and the most high-minded and trusted officials. The National Academy should be designing a resilient database/analysis system for a range of challenges. Even in America in recent decades - beginning with Nixon - we have seen how an Executive Branch can get its way and the pressures on government employees who lack independent standing (e.g., John Dean). The review of J. Edgar Hoover's secret files was alarming and they included a memorandum, by the young liberal White House aide Bill Moyers, requiring Hoover to provide LBJ with names of all members of Congress and their aides who were known to engage, or suspected of engaging, in homosexual activity. LBJ wanted the information not for a legitimate purpose but because one of his own senior, long-time aides had been caught in such behavior and LBJ wanted ammunition, if needed, to inhibit Republican political use of the scandal. (Moyers was quoted by the judge, who reviewed Hoover's files, as pleading "I was young" - which was true, but the case illustrates that a system that relies upon human beings alone can be pushed.) The Federalist Papers was right about the necessity of independent concurrence by people with different power/political constituencies.

- We also need to embed barriers to global access to US data and analysis systems (e.g., via NATO or Israeli intelligence-sharing); to spying on US citizens in linked databases that are not developed by the DNI; and for access to DNI data-gathering in India (corporate back office operations in Hyderabad) and other locations where illegitimate access to corporate financial data and financial transactions might secure enormous financial

benefits. (It is not simply individual privacy that is involved, and the DNI/NSA have the kinds of attractive corporate financial data that could send profit-oriented people on Wall Street to jail.)

The DNI Should Request These Embedded Safeguards

I hope that it is legitimate to include these legality & design questions within your purview - and, if there is doubt, I hope that the National Academy of Sciences will ask for clarification/permission. Admiral Blair is obligated to organize and manage databases and analyses to meet legal standards and I think your Panel should reflect the advice of social/behavioral science of how - if governments are to keep these extraordinary desktop capabilities - to do this in reality while meeting other responsibilities. And in reality, with an astonishing N=200,000 employees and the linked databases that resulted from the post 9/11 mandates, I doubt that even the DNI or head of NSA can be confident in their current level of monitoring and controls.

Lloyd Etheredge

Dr. Lloyd S. Etheredge - Fellow, World Academy of Art & Science
Policy Sciences Center Inc.
127 Wall St., Room 322 - Box 208215
New Haven, CT 06520-8215
URL: www.policyscience.net
301-365-5241 (v); lloyd.etheredge@policyscience.net (email)