Second Proposal Submission
ATTN: Gen. Starks

PYRAMID

Mass Data Collection for Analysis and Simulation
to Ensure the Safety of American Cultural,
Political, and Economic Control

Haplo Industries

James Howell, Rapporteur

SUMMARY

The recent terrorist attacks against the World Trade Center are the consequences of a rift between traditional polity and the way that individuals currently participate in civic discourse. The United States clearly must respond pre-emptively to future crises. We must prevent radicalization; we must keep our children free from destructive influences and secure their hope.

We must confront the changed means of political communication brought about by the Internet. To this end, Haplo Industries proposes partnership with the US Department of Defense to amass content and metadata from phone and computer network communications. We will provide access to our majority ownership of global wiring infrastructures, which should allow the DOD greater access to analog and digital communications alike. By 2020, the United States will have taken under its wing the technologies on which peoples domestic and foreign increasingly rely for communications of all types. We name our proposed plan toward this end PYRAMID.

PYRAMID is based on observable trends in usage of communication technologies currently being developed by private sector technology corporations (Cisco, Google, et al). Unfettered market development gives civilian corporate interests a startling amount of power. Much as a parent squanders his authority by neglecting his child and surrendering the boy to truancy, we run afoul the American public when we grant these corporations free range. They have no urgency to provide the oversight needed to prevent coordinating terrorist attacks such as those that most recently befell our great country.

Prevention requires anticipation. Anticipation requires insight into motives. Insight into motives requires intimate knowledge of each online user so we can know when dissident tendencies verge on exploding into terrorism. Government influence over these technologies will provide such relevant information to the United States. We will create profiles from "identity patterns" for each individual.

We base our understanding of identity upon current scientific and psychological trends. Identity has traditionally been regarded as an innate or essential aspect of a person (e.g. the self, psyche, or soul). We know, however, that the sum of human actions reveals behavioral patterns that grant more insight into a person's identity than any self-description can. A child says he resents his father while visibly caring for the man, thereby revealing a love that language cannot express. PYRAMID will observe the actions rather than solicit the self-testament. We will analyze metadata along with information content to build reliable models of discrete individuals, not in violation of privacy, but for the purpose of modeling collective behaviors.

The above process will lead to a radical new predictive model. Identity patterns gathered from surveillance will go into advanced computers; those systems will render simulations of entire populations. Analysts can reach out toward their cared-for populations to slim the margin of error in predicting cultural and political trends. Analysis of repeated

simulations will guide the DOD's hand decisively against the chaotic elements threatening our sovereign state.

Funding in the amount of ███████████ is requested to construct the PYRAMID facility, a sea-borne server base housing gathered surveillance information as well as the analytic machine intelligences that will parse the data.

STATEMENT OF NEED

Historically, media gatekeepers have curated truth through oversight of publication and circulation. While we note the lapses in their responsibility (as in yellow journalism), the overall pattern remains consistent: intelligent, seasoned professionals have chosen which information to project and which information to protect.

The Internet gives all ideas, regardless of truth status, the same access to an unknown audience. A cultural dilemma now appears. Individuals may either adopt positions of moral relativism, since conflicting truth claims seem may partially correct in some way; or they can adopt moral absolutism, since our truth filtering processes must harden to prevent being overwhelmed. We must regard any middling state as the potential to turn dissolute or rigid in the manners indicated.

Either state is fertile ground for breeding terrorism. We may consider these effects epistemological. Online users have no means of testing the validity of all information encountered online; therefore, they have no way to know what is true.

Unfiltered information withers the strength of moral facts. We must pre-empt the problem and prevent the need to exercise discipline on a morally shapeless populace.

Collective, niche emotions masquerade as political realities through gossip and conspiracy theories. Such intangible chatter results in the crazed beliefs that became realities in the attacks against the World Trade Center. The ambiguity of unregulated truth results in unorthodox political speech, such as flying a plane into a public building, rather than naturalizing as a citizen and voting.

In addition to confusion of cultural truth, the Internet provides new opportunities for mobilizing unorthodox political speech. Reliance upon traditional media (print, wire, television, etc) has hitherto paced the rhythm of political discourse. People kept in touch at the speed of thoughtful reflection. The Internet has increased the speed of communications and decreased the time required to think about the ideas we communicate. The same tool that reports baseball scores facilitates faster communication between dissidents, hastening the process of radicalization and improving organizational mobility.

As recent events illustrate, we see a breakdown in our work with Middle Eastern countries in particular. Dissidents abroad can more easily communicate with radicalized Americans. Whereas geographical barriers previously would have slowed such correspondence, digital communications allow terrorists unfettered access to susceptible recruits. We may assume that such tools will likewise result in civil rifts, requiring police rather than military response.

361 million people currently use the Internet for professional, financial, educational, and personal needs. The userbase stands to grow to 200 million people by 2010, including Americans and foreign internationals. America has much to protect: its political heritage, its cultural medley, and its research in such crucial areas as environmental science and cancer medicine.

We must repair this divide.

PROGRAM DESCRIPTION

PYRAMID is a multi-front strategy for collecting and storing online communications. Analysis of stored data will proceed under supervision of programs ancillary to PYRAMID. In sum, we propose the use of machine rather than human intelligence to organize data and search for patterns therein, pending the DOD's adoption of PYRAMID.

We propose the construction of a sea-borne data storage facility given legal protections under maritime law. It will, in effect, be a semi-sovereign colony of the United States. Please see the modified version of Japan's prospective Shimizu Mega-City Pyramid as our proposed ideal structure.

PYRAMID will grow in phases. Each successive strategy will complement the strategies that came before. We will begin by manipulating software, and we will push toward the ultimate goal of controlling network infrastructures directly. Software invasion will begin the process of culling information from systems; infrastructure dominance will make us the system.

Our first strategies are collectively called Computer Network Exploitation. Government- and Haplo-designed malware will leach data from outbound and inbound digital communications. We can break encryption protocols that protect banking and medical records (documents that give context to archived chatter) and consumer-facing encryption. The initial step has a weakness. Wired intranets that do not exchange data outside their networks will be inaccessible. Infrastructural dominance will help to crack closed intranets.

Infrastructure control must have global ambitions. International competitors such as China and Russian require complex strategies adjacent to (but beyond the scope of) this proposal. PYRAMID's infrastructural goals target Second World countries.

We must ensure that American routers and switches become the basic Second World standard. Second World governments are eager to rise into the first world, and they cannot engineer technology compatible with First World networks. China and Russia will no doubt race to dominate that market with their network hardwares. We must eclipse their ambitions.

We can bug exported technology that enables us to intercept their internal communications and, importantly, their external communications with our First World competitors. Even knowing that a Second World country communicates with China at all (informed by metadata) will help our understanding of potential terrorist developments abroad.

Domestic targets will include individuals whose ideologies become volatile when sympathetic, like-minded people organize. Dissidents, economic reformers, social radicals, and unprincipled labor organizers are examples. Past riots associated with their endeavors prove the instability of their reform methods. We must prevent their breaking away from our societal union.

We must also anticipate the public's awareness of PYRAMID. We must assume that a whistleblower will alert the press at some unknown time, and we can use media messaging to soften that blow. Cracking banking, medical, and consumer networks will weaken the overall security of encrypted information, allowing isolated hackers into those networks. We can deflect attention toward individual, comparatively disorganized hackers as "cyberterrorist" threats. We can also make private corporations (considered responsible for their own network security) take public scorn, thereby deflecting attention away from PYRAMID.

When parts of the program enter public knowledge, we can use the court system to dominate media attention before PYRAMID comes to light. Consider this "justice theater." Make court cases, symbols, and individuals more important than debate surrounding our activities. When that fails, use public debate itself as another layer of attention. Generate as much debate about the debate as possible to disorient and exhaust the public whose interests we serve.

Ideally, we will be able to cultivate a mass-surveillance culture. This is the goal of every good father: to raise children whose moral compass polices them in the father's absence. Categories such as "innocent" and "suspect" will become flexible, and the population themselves will enforce their plasticity. These global HUMINT priorities will be more detailed in proposals to come.