James A. Baker III Institute for Public Policy
Rice University

Open Source, Policy Informatics and Python: Understanding the Mumbai Attacks Through Information Technology

By

Christopher Bronk, Ph.D.

Fellow in Technology, Society and Public Policy
James A. Baker III Institute for Public Policy
Rice University

and

Derek Ruths, M.S.

Department of Computer Science, Rice University

December 18, 2008

These papers were written by a researcher (or researchers) who participated in a Baker Institute research project. Wherever feasible, these papers are reviewed by outside experts before they are released. However, the research and views expressed in these papers are those of the individual researcher(s), and do not necessarily represent the views of the James A. Baker III Institute for Public Policy.

Open Source, Policy Informatics and Python: Understanding the Mumbai Attacks Through Information Technology

The recent terror attacks in Mumbai are attracting immense international attention as India and the world seek justice. Officials in New Delhi and elsewhere are pointing blame in the direction of Pakistan, citing mounting evidence. We at the Baker Institute are watching closely, too, hoping to make our own contribution to the war against transnational terrorism with the aid of sophisticated computer-analysis software.

For the past 18 months, a group of Rice University professors and students have applied methodologies from computer science in the areas of artificial intelligence and bioinformatics to the issue of terrorism. Collaborating with colleagues at the Institute for the Study of Violent Groups (ISVG), which collects and encodes news stories into a massive "open source" database available to all researchers, our team has developed computing applications to rapidly query and process this data. Our group has written software in the highly flexible Python programming language that allows us to ask who might be the responsible party for a terrorist incident using a certain set of parameters, such as weaponry employed, choice of target and tactics. Every time there is a major terrorist attack, we are able to test our models, refine our methods and incorporate new functions into our system.

For us, Mumbai represents the latest test case for a project that is aimed at understanding deeper theory of transnational terrorism. A part-time diversion from day jobs in our respective disciplines, the project has moved forward, with papers presented at Harvard's Kennedy School and at the annual academic summit of INSA — the Intelligence and National Security Alliance, the organization charged with connecting outside experts to the U.S. intelligence community. Though a tragedy of great magnitude, Mumbai has allowed us to further refine our system by seeing how well we can assign attribution for a major terrorist attack by querying against the ISVG database with minimal information.

On Thanksgiving Day, as the attacks unfolded, our undergraduate program assistant ran a series of such queries on the Mumbai attacks based on the information reported by the TV networks. By entering the weapons used (machine guns, grenades and explosives), the target (public structures) and tactics (raid, direct fire and ambush), and without respect to any geographic or ideological bent, he essentially asked, "Who in the world has done this sort of thing before?" The answers were the expected ones, with al-Qaida at the top of a list that also included the Liberation Tigers of Tamil Eelam (LTTE), the Palestinian militant group Hamas, a Chechen independence group and the India-based United Liberation Front of Assam. This query provided a simple answer as to who might be able to pull off such an attack, irrespective of geography.

In our next passes, we focused in on groups known to be active in South Asia. Even keeping the query open to territory beyond India, including Afghanistan and Sri Lanka, we generated a list of names including Pakistan-based Lashkar-e-Tayyiba (LeT), the Bangladeshi Jamaat-ul-Mujahideen and Al-Mansoorian, a group active in Kashmir. By running extremely simple queries against the large, detailed ISVG database that had no new content added in the immediate period before the Mumbai attacks, we came up with the same groups mentioned as likely suspects in Indian, U.S. and other international media. The software we had crafted to better assign attribution in terror attacks appears to have worked — allowing us to match signatures and say, with some confidence, what groups had the requisite experience, resources and coordinating factors to pull off the Mumbai attacks.

Our experience hints at the possibility for more fully utilizing computing technology to better understand our complex contemporary foreign affairs environment. The U.S. intelligence community and foreign intelligence agencies no doubt make good use of sophisticated computing tools in sifting through the massive amount of information available on the terrorism issue, but a problem remains in the human capacity to absorb all of that information. Even the best-funded intelligence operation cannot watch everything all of the time. What we have demonstrated is that information technology can help determine where to look. From that, we can then direct the human effort to more deeply understand transnational terrorism and other topics.

The challenge now is how to deploy information technology to better serve diplomacy, law enforcement and intelligence. In the interest of combating transnational violence, academia, industry and government must develop new tools for coping with this information overload. This will require interdisciplinary effort crossing multiple academic concentrations, from the social sciences to engineering. The practice of foreign affairs is an information intensive activity, and those who have the most powerful information tools are likely to prevail.