SYNTHETIC INTELLIGENCE AND POLICE INVESTIGATIONS IN 2020
HAL 9000 PINS ON A BADGE

by

Dave Hill
Orange Police Department

September, 2012

COMMAND COLLEGE CLASS 51

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

© Copyright 2012
California Commission on Peace Officer Standards and Training

SYNTHETIC INTELLIGENCE AND POLICE INVESTIGATIONS IN 2020
HAL 9000 PINS ON A BADGE

Joe Friday meets the HAL 9000 and teams up with RoboCop for an investigative adventure straight out of “Minority Report.” Huh?! Just a little more than 2,700 days away, soon after the clock strikes midnight on January 1, 2020, a whole new era will begin in the law enforcement profession. Gone will be the days of laborious investigations. Legal research, which used to take a detective hours, will instead be accomplished in minutes—possibly seconds. Surveillance, apprehensions, and interviews of suspects which previously took an investigative team days and weeks; will instead be performed by a non-human entity, and be finalized in a much shorter time. And the tedious documentation, prosecution, and sentencing in criminal cases will take this new system less time to complete than it will take you to read this article. The common factor to the ultra-efficient success of each of these examples is the use of synthetic intelligence.

I’ll pause here for a moment to allow your head to stop spinning. Synthetic what? The term "synthetic intelligence" (SI) refers to the blending of artificial intelligence, the thinking ability of computers commonly referred to as “AI,” with human cognition. Seemingly impossible at first blush, SI is the singularity of thought involving mankind and machine, indistinguishable from purely human thought and interaction. More than just faster computer systems, the foundational basics of SI have been seen in action in the form of interactive machines like IBM's "Watson" supercomputer that beat it's human opponents on the television show "Jeopardy!" Realizing actual synthetic intelligence – let alone using it in a criminal investigation context – is so far out on the horizon that it is barely visible. And that is precisely what makes it so exciting! Is this about humans with technological additions or enhancements to their biological ability to think? Or are we talking about machines that are so advanced that they

reason and make decisions that are indistinguishable from those of a human? The answer is a resounding, "Yes!"

In the near future, the real-life "game" of cops and robbers will be more like a computer simulation ending in actual results than a television drama, which is both exciting and troubling. Practitioners, scholars, and futurists alike will have to grapple with issues inherent in the transformation to synthetic intelligence playing a major role in the criminal justice system. Let's look at four issues that consistently jump out amidst any discussion on the subject of synthetic intelligence in law enforcement investigations. The first is the question of just *what* an SI system would do. (The question of "how" is best left to the computer scientists, and tends to cloud—rather than encourage—thinking futuristically). The second issue to be explored is the legal delicacies of a machine performing tasks that touch the realm of constitutional law. Third on our list of topics is technical and legal accountability for the technology doing the work. Who is responsible for SI investigative integrity, and to whom? And finally we will look at the human element of police investigations and whether or not a computer—regardless of how powerful it is—can replace human compassion and empathy when interacting with victims, witnesses, and suspects.

More Than Just an Improved System

So what's the big deal? Systems already exist that contain multiple scores of volumes of records and data that are virtually at an investigator's fingertips. But those systems are little more than digital card files, akin to computerized Dewey decimal system records of books in a library. Sure, you can search for your information faster, but a result still depends on the *user* doing the majority of the work. With SI-based investigations, the work required of the officer or

detective is limited, but the payoff in results is substantial. Consider a simple scenario as a way to start to wrap one's mind around the whole idea.

For many years now, officers have been waving soft brushes of graphite powder over surfaces in a crime scene to try to locate and lift latent fingerprints left there by the person who committed the crime. (Readers on the west coast most often call them a "suspect" while east coast readers may more frequently use the word, "perp.") Once lifted, these prints are fed into a computer system, which searches for a match and reports that match to the investigator or technician. The investigator can then begin the process of researching the suspect's history, locating them, arresting them, interviewing them, and eventually booking them in jail. The process is then handed-off to the local prosecutor's office for the remainder of the case. But an investigation steeped in synthetic intelligence would do much more and do it faster, with fewer errors … and without any overtime.

Won't this be amazing? The SI system will read the latent print and quickly identify the person to whom it belongs. Immediate access to a cache of criminal history data allows the system to quickly provide documented arrests, convictions, acquittals, judgments, and any other legal record associated with the now-known suspect. The SI system will calculate the probability that the identified suspect committed the crime based on arrests for similar activity, similar methods of operation in those previous crimes, and by establishing the whereabouts of the suspect during the time the crime reportedly took place. This information would come from an amalgamation of financial transaction records, vehicular and cellular GPS coordinates, social networking records, and similar bits of information left behind by the individual as they travel through cyber-society.

Almost simultaneously, the system would issue a warrant for the arrest of the individual and circulate that warrant in real-time to patrol briefings and investigative meetings throughout the region. A suspect's refusal to comply with a warrant would be countered with the complete shutdown of all of their financial and online resources. Once the suspect is compelled to surrender, an interactive interview is conducted. Not simply questions and answers, SI-based interviewing systems observe and calculate heart rate, body temperature, eye movement, speech, and body language to gauge the veracity of the suspect's story. Once interviews are completed and records are digitally generated, the suspect is booked into jail, where they await trial. Although an SI-based system may very well be able to conduct the trial, consider evidence, and render a sentence, we will stick with the only the investigative scenario for now.

Even the simplest of investigative vignettes arouses similar questions from experienced law enforcement professionals. The most common of which has to do with how the system would navigate the guidelines and restrictions present in the U.S. Constitution. Of special concern are those facets of the 4th Amendment, that portion of the Bill of Rights, which has been examined in countless court cases since it's ratification. Would a computer resource as advanced as an SI-based system be bound by a law intended to prevent the government from performing unreasonable searches on a person's "effects"? It would stand to reason that any resource utilized by the government, including a super-intelligent computer, would be bound by the Constitution; even if that meant programming the Constitution into the system itself. (Dunn 1991) Other questions arise as well.

Could a programmer be held liable for the actions of a computer in such a case? In our litigious society, it's not the cynic who would respond in the affirmative. Liability for a system's performance would surely be the responsibility of the company producing the system as well as

the programmer doing the fine-tuning work. If the SI-based system knew every law ever passed and every case decision ever decided, and was able to bring that knowledge into an investigation, shouldn't it be able to avoid such legal missteps? This question assumes the computer system recognizes an action as a misstep. Even the machines on which we work today are programmed to perform certain actions while avoiding others, so I would expect this same ability to be inherent in a future, SI-based investigative system. And would such an advanced system be self-aware to the point that it can realize when it is approaching that line and avoid crossing it? One author and futurist says, "No." In his article, "A World Wide Mind: The Coming Collective Telempathy," Michael Chorost discusses the hyperorganism that would result from the combination of the Internet and humanity (Chorost 2012, 22-25). Such an Internet-based system, says Chorost, "has primitive ways of 'sensing' and 'reacting,' but it has no self-awareness and no ability to formulate its own goals. Nor could it ever reach such a state on its own." (Chorost 2012, 22)

Such issues and questions are as fascinating as they are frustrating. There are no easy answers because the reality is still out there a ways. But questions of the legal parameters of a synthetic intelligence system and it's application in police investigations naturally lead to questions about personal privacy, and the legal and technological accountability of the people involved in programming and running such a system.

Privacy Invasion By Government

After the attacks on the World Trade Center on September 11, 2011, the federal government passed the "Patriot Act," giving greater leeway to investigative bodies pursuing suspected terrorists. Many people with whom I interacted expressed their feeling that they were

willing to give up some of their privacy in the name of greater national security. This was true even if they could not state with any specificity what the government was doing to catch terrorists. Waiting in an extra long line at the airport—a public place—to board a plane is one thing. Allowing the government to access, synthesize, and utilize personal activity which is not necessarily intended for public consumption is something else. Some of these things are being done today in business marketing, but is society ready for the local police to have that ability? The state government? The feds?

A poll by ABC News and The Washington Post indicated that approximately 60% of Americans surveyed supported extending the authority of the Patriot Act four years after it was made law (Langer 2005). It would be plausible for society to similarly support the use of mass quantities of personal information in the interest of keeping the public safe. According to a 2005 ABC News poll, "Most Americans in the past have accepted possible privacy intrusions at times of national crisis -- but not on an unlimited or permanent basis. As the immediacy of the sense of crisis wanes, interest in privacy rights can reassert itself." (Langer 2005) With crime rates expected to increase in states like California, which are releasing an increasing number of prisoners before their terms are done, society will likely opt for more effective tools like SI in the hands of police.

The privacy concerns surrounding SI-based investigations are not necessarily a topic one brings up at parties. But it is not uncommon to hear the casual remark, "If you've got nothing to hide, then you've got nothing to worry about." Such a comment seems to diminish the importance of privacy as a foundation of American life. But if a citizen has nothing to hide because they're doing nothing wrong, then the authorities at any level may be doing more harm than good by looking into their personal affairs to begin with. Considering our latent fingerprint

example, how would an SI system have any way of knowing that a latent print was left by an innocent passer-by and not a suspect? The answer is that it wouldn't know without further inquiry. This supplemental, quality-control check could be built into the system by the entity responsible for the system's capabilities in order to prevent such a mis-identification.

Individual departments could contract with vendors competing in the free market, and that desire to increase a corporation's bottom line could result in stronger system integrity. A centralized, government-run system may be efficient and effective, but such a system has Orwellian overtones. Either example could serve as an access point to a networked SI collaborative. A scenario of such a networked world was conjured by Lee Rainie and Barry Wellman in their description of a fictional man named Will Li who began his day accessing the network. "Truthfully the computer really isn't his…[it] is really only an access point, as all his data is in the cloud, yet another thing that's owned-with all the data in it-by a big corporation." (Rainie and Wellman, 2012)

Once it is decided where in government or society such a resource will be housed, then it follows that people and organizations must be hired who would ensure best practices in both the technological and legal realms. Such responsibilities would be huge for a small team, let alone one individual. But organizations in the private or public sector are rarely found without both technological and legal experts within their organizational structure. This makes the job of identifying persons responsible for keeping things within an SI system technologically and legally sound less foreboding. Recruiting and hiring such individuals or companies would not seemingly be difficult for a LE organization to figure out. Most agencies already have an in-house expert or contract with a consultant to handle their technological and legal needs.

Technology's Promise and the Future

Scholars such as William Halal, author of the book, Technology's Promise: Expert Knowledge on the Transformation of Business and Society, believe that the distinction between the intelligence of man and machine will be blurred, if not completely rubbed out, by the year 2020. A cursory review of his virtual think tank website, "techcast.org," reveals opinion pieces and forecasting papers strongly stating how powerful artificial intelligence, the precursor of synthetic intelligence, will be, and that it may be just around the corner. Halal asserts that "At about 2020, the very time when the planet is likely to teeter between calamity and salvation, routine human thought should be automated by far more sophisticated IT networks, a second generation of more powerful computers, and good AI." (Halal 2008, xxiii)

The question of whether or not a machine can think as well as a human, and all the social, moral, ethical, and technological debates that attach, are all material for numerous other articles down the line. Synthetic intelligence may be able to optimally perform tasks, even make an infinite number of accurate, split-second decisions, with data and processes; but can it interact with a suspect and tell whether the suspect is lying or telling the truth? Would a system, which applies super-human data-gathering, be successful sitting across from a victim and conveying empathy and compassion when confirming details of their story? Renowned futurist and Singularity University co-founder Ray Kurzweil seems to imply that it would. "Within a quarter-century, nonbiological intelligence will match the range and *subtlety* of human intelligence. It will then soar past it." (Reynolds, 2009) (Italics added.) The idea of the subtlety of human intelligence is what goes beyond binary coding and rote calculations, and into the realm of interaction. Technology authority Steven M. Shaker adds a perceptual facet to this idea. "An approach to AI called embodiment…maintains that intelligent behavior occurs out of the

interplay among the brain, the body, and the world. Ideas, thoughts, concepts, and reasoning are shaped by our…ability to perceive, move, and interact with our world." (Shaker 2009, 23) Even if such communicative interaction is not precisely the same as with a human, it does not mean that possibilities should not be explored and the results applied to police investigations.

Could a system entrusted with protecting society through the identification and apprehension of criminals be allowed to work through these virtual conundrums by simple trial and error, or does the security of the public demand a flawless system before it is instituted? Some scientists are already skeptical of just how successful AI has been, which may result in a collective foot-dragging to bring an SI-based investigative system into use. But the safety, security, and the confidence of the public we serve as law enforcement professionals demands that a system as powerful as the one discussed be instituted only after it has been nearly perfected.

We will soon leave the era where technological resources are tools in the hands of human criminal investigators, and embark on an age in which they are the actual investigators themselves. In fact, the first boarding call for that flight into the future has already been announced. In Santa Cruz and Los Angeles, for example, police officers are utilizing software that was originally used for predicting earthquakes, and they are using it to predict crime. The system, made by a company called PredPol, "calculates its forecasts based on times and locations of previous crimes, combined with sociological information and patterns." (Kelly, 2012) The approximately 2,700 days left until the year 2020 will include the development of systems which are able to handle scores of investigative tasks with aplomb. These systems will be internally programmed to respect the Constitution and its application to police work while effectively

walking the fine line of technological and legal integrity and accountability to the citizens who both pay for and are served by such a system.

In those situations where human intelligence and interaction are preferred to artificial intelligence, such as interviews and interrogations, the human police professional will still be available to bring their unique abilities to the task. For the human to take the lead, and the machine to act as wingman, is the ideal example of the blended, synergistic essence of synthetic intelligence. Such a combination will be so effective that it will usher in an era in which a plot akin to “Minority Report” is quaintly obsolete, and investigations conducted through synthetic intelligence applications are commonplace and successful.

Works Cited

Chorost, Michael. 2012. A world wide mind: the coming collective telempathy. *The Futurist* March-April 2012: 22.

Dunn, Theodore. 1995. Exploring the possibility of using intelligent computers to judge criminal offenders. http://www.fdle.state.fl.us/Content/getdoc/814750b4-4546-49f0-9be2-90fe772257f7/Dunn.aspx (accessed July 16, 2012).

Halal, William. 2008. Technology's promise: expert knowledge on the transformation of business and society. New York, NY: Palgrave MacMillan.

Kelly, Heather. 2012. Police embracing tech that predicts crimes. http://www.cnn.com/2012/07/09/tech/innovation/police-tech/index.html?iref=allsearch (accessed July 10, 2012).

Langer, Gary. 2005. Poll: support seen for patriot act. http://abcnews.go.com/US/PollVault/story?id=833703#.UASYxUad44Q (accessed July 16, 2012).

Rainie, Lee, and Barry Wellman. 2012. The individual in a networked world: two scenarios. *The Futurist* July-August 2012: 26.

Reynolds, Glenn. 2009. The singularity is coming-now what? http://www.popularmechanics.com/technology/engineering/robots/4337160?click=main_sr (accessed July 16, 2012).

Shaker, Steven. 2011. The coming robot evolution race. *The Futurist* September-October 2011: 23.