Backgrounder
Published by The Heritage Foundation

No. 2049
July 5, 2007

Future Computing and Cutting-Edge National Security

James Jay Carafano, Ph.D., and Andrew Gudgel

Data mining and cognitive computers are two emerging aspects of future computing that show promise for a large number of national security applications, from detecting terrorists to making battlefield decisions. New computational capabilities are already foreshadowing the next turn of the information revolution: an unprecedented capacity to sift through ever-increasing amounts of data on the Web and on the battlefield to detect patterns and identify which bits of information are essential to human decision-makers.

Future computing capabilities could give the United States an enormous advantage in many areas. In addition, these capabilities can be employed in manner that both respects civil liberties and enhances the protection of individual privacy.

Congress clearly has a role in advancing the use of data mining and other future computing technologies and ensuring that they are employed in an appropriate manner. Congress should establish federal guidelines for the use of data-mining technologies that promote their use for national security purposes while safeguarding the liberties of American citizens. Congress should also monitor government efforts to support research into cognitive computing, encouraging research and development into what could become a significant competitive advantage for the United States in the race for hyper-computing power in the 21st century.

History in the Making

Machines that actually manipulate data are as old as the ancient Greeks, who developed the Antikythera

Talking Points

- Hyper-computing power could give the United States a dramatic competitive advantage in key areas of national security, from detecting terrorists and increasing battlefield awareness to developing new smart weapons and unmanned combat aerial vehicles.
- The U.S. cannot afford to be complacent and assume that it will win the race to develop advanced computing systems in the 21st century.
- Congress clearly has a role in advancing the use of data mining and other future computing technologies and in establishing federal guidelines to ensure that these technologies are employed in an appropriate manner.
- To prevent abuse, accountability and oversight should be strengthened by internal policy controls, training, executive and legislative oversight, and civil and criminal penalties for abuse.
- The federal government's use of data-mining technology should be strictly limited to investigations related to national security.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/bg2049.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

mechanism, a mechanical analog computer that predicted the movements of the sun, moon, and planets.[1] In the 1820s and 1830s, Charles Babbage designed a "difference engine" and an "analytical engine," analog computers that could make complex calculations. However, they were never completed. The ENIAC, one of the first electronic, reprogrammable computers, was built by the University of Pennsylvania and used during World War II to calculate artillery firing tables.[2]

The development of the solid-state transistor and later the integrated circuit allowed the manufacture of cheaper, completely electronic digital computers. In the post–World War II era, digital computers not only served national security needs, but also were used to track bank accounts and other business transactions.

The mathematical foundations of cognitive computing (computers that operated more like human brains) were laid in the 1940s and 1950s and expanded in the 1980s.[3] Computers became increasingly more powerful while simultaneously becoming smaller in size. The development of the personal computer in the 1970s led to improved graphics, and computers went from "crunching numbers" to assistants that helped to represent information visually.

Since the 1980s, the cost of computational power has continued to decline, while the computational capacity of computers has grown exponentially. Today, computers are ubiquitous on battlefields and in boardrooms—key tools in virtually every field in national security and the commercial sector.

Until recently, computers only displayed or modified data in fixed ways that had been predetermined by humans. A computer could only do exactly what it was programmed to do, without deviation. Advances such as data mining and cognitive computing allow computers to manipulate data within general guidelines, finding associations and patterns that humans are unable to see.

Computers are becoming adaptable, capable of learning and making decisions. Applied to national security policy, this evolution of technology has large implications. In addition to being aware of this growing field, Congress should encourage its development.

Computers Rising: Data Mining and Cognitive Computing

Terms such as "data mining" and "cognitive computing" conjure up images of the HAL 9000 computer from the movie *2001: A Space Odyssey.* Data mining is nothing more than looking for patterns in data. Advertising agencies have used it for decades to determine which campaigns have the greatest draw and to identify specific target audiences. Like many other techniques originally done with pencil and paper, data mining has become faster and easier with the use of computers. Coupled with technologies that allow for better gathering of raw data—everything from laser scanners at supermarket checkouts to unmanned aerial vehicles on the battlefield—the volume of data available to decision-makers has increased dramatically.

Data mining has gone through several stages. At first, computers simply collected and stored data. Separate software was required to manipulate the data. Then the tools were built into the database software itself so that the information could be analyzed on the spot.

With the growth of large, networked databases, information had to be moved to a central "warehouse" where it could be analyzed. This centralized system is now giving way to a system in which the data stay in place and software "agents" communicate between databases, mining the data "on site." This allows for real-time analysis of ever-changing information.[4]

[1] Peter James and Nick Thorpe, *Ancient Inventions* (New York: Ballantine Books, 1994), pp. 121–123.

[2] Isaac Asimov, *Asimov's New Guide to Science* (New York: Basic Books, 1984), pp. 860 and 862.

[3] Neural Network Solutions, "Introduction to Neural Networks: History and Development of Neural Networks," at *www.neuralnetworksolutions.com/nn/intro2.php* (November 27, 2006).

[4] Jesus Mena, speaking at program on "Future Computing: Shaping National Security Policy from the Inside Out," The Heritage Foundation, Washington, D.C., November 6, 2006, at *www.heritage.org/Press/Events/ev110606a.cfm*.

Other uses of data mining include bioinformatics, which sifts through large volumes of information from biological experiments. Earlier this year, researchers at Stanford and Harvard Universities used data-mining techniques to identify gene correlations across a number of different experiments by sifting through results that had been submitted to scientific journals.[5] GlaxoSmithKline, a pharmaceutical company, is developing a similar database and techniques to conduct drug discovery research.[6] Data-mining techniques are also used extensively in detecting computer intrusions and for terrorist screening.[7]

Cognitive computing promises a new generation of computers that mimic the functions of human brains. Unlike today's computers, cognitive computers operate autonomously, using learning and reasoning to derive new knowledge. The Department of Defense has explored the use of cognitive computing for autopilots and has already tested self-piloting craft that adapt to changing conditions. Cognitive computing promises to reduce the time needed to develop new smart weapons and unmanned combat aerial vehicles.[8]

Cognitive computing is also being used to translate spoken language in real time, creating an "instant translator." The technology has already been used to demonstrate simultaneously translation between spoken English and Spanish and between English and Mandarin Chinese.[9]

Potential National Security Applications

While current computing technology continues to expand the ability of the intelligence community and Department of Homeland Security to "connect the dots," the most dramatic unclassified developments in future computing are happening within the Department of Defense.

As the number of sensor systems on the battlefield increases dramatically, so does the volume of raw information flowing to military commanders and decision-makers. Picking the handful of essential facts out of this ocean of information will become increasingly more difficult.

To this end, the U.S. Army Research Laboratory has established a research program to investigate the use of data mining to ensure that soldiers and commanders are not overburdened with data.[10] In June 2006, the U.S. Air Force Research Laboratory awarded a contract to conduct research on developing filter and data-mining technologies to provide information to aid intelligence analysts in making decisions.[11]

Advances in sensors, as well as in computer hardware and software, could lead to integrated sensor-processor suites that take in raw information on the battlefield, determine which data are valuable, process them, and forward decision-ready intelligence to the human that receives the sensor's output. Other integrated sensor-processor packages

[5] Press release, "Stanford/Packard Scientist's Data-Mining Technique Strikes Genetic Gold," American Association for the Advancement of Science *EurekAlert!*, January 10, 2006, at *www.eurekalert.org/pub_releases/2006-01/sumc-ssd011006.php* (November 27, 2006).

[6] Press release, "Output of e-Science Project Helps GSK Speed Up Drug Discovery," American Association for the Advancement of Science *EurekAlert!*, September 21, 2005, at *www.eurekalert.org/pub_releases/2005-09/eaps-ooe091905.php* (November 27, 2006).

[7] Varun Chandola, Eric Eilertson, Levent Ertoz, Gyorgy Simon, and Vipin Kumar, "MINDS: Architecture & Design," University of Minnesota, Minneapolis, July 14, 2006, at *http://handle.dtic.mil/100.2/ADA455153* (June 29, 2007), and Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," Congressional Research Service *Report for Congress*, updated January 27, 2006, at *http://handle.dtic.mil/100.2/ADA450426* (June 29, 2007).

[8] Jeff Pleinis, "Advanced Adaptive Autopilot," U.S. Air Force Research Laboratory, Munitions Directorate, at *www.afrlhorizons.com/Briefs/Jun03/MN0213.html* (November 20, 2006).

[9] U.S. Air Force Research Laboratory, "Automatic Spoken Language Translation," at *www.rl.af.mil/div/IFB/techtrans/datasheets/ASLT.html* (November 20, 2006; unavailable June 29, 2007).

[10] U.S. Army Research Laboratory, "ARO Computing and Information Sciences 11.0," at *www.arl.army.mil/main/Main/default.cfm?Action=29&Page=205* (November 27, 2006; unavailable June 29, 2007).

[11] Francis Crumb, "AFRL Awards Small Business Contract to Utica Firm," June 23, 2006, at *www.if.afrl.af.mil/div/IFO/IFOI/IFOIPA/press_history/pr-06/pr-06-61.html* (November 27, 2006; unavailable June 29, 2007).

could allow weapons systems to identify and reprioritize targets on the fly.

Sensors and data mining are not only useful in making targeting decisions. Weather can profoundly affect military operations and communications, and wind patterns are important in tracking clouds of chemical or biological agents. The U.S. Army Research Laboratory has established a research project that hopes to use networks of sensors and computers to turn weather data into real-time weather intelligence and decision aids for commanders.[12]

Cognitive computers, which could learn and relearn, would be capable of not only working around battle damage, but also improving the speed and accuracy of their calculations, essentially gaining experience.[13] The U.S. Office of Naval Research is examining the feasibility of creating large-scale neural networks (structures that mimic brain functions) that would do more than simple pattern matching and enter into the realm of cognitive skills that can make human-like decisions.[14]

Cognitive computers could also perform mundane tasks such as preventive maintenance. The U.S. Air Force Research Laboratory is conducting research on creating an advanced aircraft engine that would both adapt to changing flight conditions and self-identify maintenance problems and needed repairs.[15]

Besides weapons systems, cognitive computers could be used to simulate possible scenarios and indicate courses of action for battlefield decision-makers. The Air Force Research Laboratory is looking at ways to create systems that would run multiple, branching simulations within a computer and use "intelligent" adversaries that would adapt their responses to changing conditions and human-made choices.[16] A similar system is being developed to run command-and-control-type exercises.[17]

What Congress Should Do

Data mining and cognitive computing show promise in many important applications. Improved data mining and cognitive computing techniques will increase the number of potential uses and push the actual manipulation of raw data "down the chain" toward sensors and other input devices. Congress can best help to exploit these emerging technologies by setting rules and investing in future computing.

Setting the Rules. Congress clearly has a role in advancing the use of data mining and other information technologies for national security purposes and in ensuring that they are employed in an appropriate manner. Establishing federal guidelines for the use of these technologies is one way to address the issue.

Such guidelines would begin by defining what programs should come under the scope of data-mining programs. They should also include the following elements:

- Every deployment of federal data-mining technology should require authorization by Congress.
- Agencies should institute internal guidelines for using data analysis technologies, and all systems

[12] U.S. Army Research Laboratory, "C4I: Battlefield Weather for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)," modified August 11, 2005, at *www.arl.army.mil/main/Main/default.cfm?Action=18&Page=69* (November 20, 2006).

[13] U.S. Defense Advanced Research Projects Agency, "Self-Regenerative Systems: Mission," at *www.darpa.mil/ipto/programs/srs/index.htm* (November 15, 2006).

[14] U.S. Office of Naval Research, "Neural Engineering & Biorobotics: Neural Computation," at *www.onr.navy.mil/sci_tech/34/341/ne_comp.asp* (November 15, 2006).

[15] Tim Lewis, "Future Aircraft Jet Engines Will Think for Themselves," U.S. Air Force Research Laboratory, Propulsion Directorate, at *www.afrlhorizons.com/Briefs/Dec01/PR0105.html* (November 20, 2006).

[16] Duane A. Gilmour, James P. Hanna, Walter A. Koziarz, William E. McKeever, and Martin J. Walter, "High-Performance Computing for Command and Control Real-Time Decision Support," U.S. Air Force Research Laboratory, Information Directorate, at *www.afrlhorizons.com/Briefs/Feb05/IF0407.html* (November 20, 2006).

[17] Michael J. Young, "Agent-Based Modeling and Behavioral Representation," U.S. Air Force Research Laboratory, Human Effectiveness Directorate, at *www.afrlhorizons.com/Briefs/0006/HE0009.html* (November 20, 2006).

should be structured to meet existing legal limitations on access to third-party data.

- A Senate-confirmed official should authorize any use of data-mining technology to examine terrorist patterns. The system used should allow only for the initial query of government databases and disaggregate personally identifying information from the pattern analysis results.
- To protect individual privacy, any disclosure of a person's identity should require a judge's approval.
- A statute or regulation should require that the only consequence of being identified through pattern analysis is further investigation.
- A robust legal mechanism should be created to correct false positive identifications.
- To prevent abuse, accountability and oversight should be strengthened by internal policy controls, training, executive and legislative oversight, and civil and criminal penalties for abuse.
- The federal government's use of data-mining technology should be strictly limited to investigations related to national security.

Investing in Future Computing. Congress should encourage government research into exploiting cognitive computing for national security applications. These technologies could meet a wide range of homeland security and defense needs, from information systems that draw on retained information to identify links between terrorists to weapons with instantaneous target acquisition that also provide real-time information to battlefield decision-makers. The Department of Homeland Security and the Department of Defense should continue to fund and develop cognitive computing.

The Way Forward

Data mining and cognitive computers are powerful tools that could greatly improve the identification, analysis, and decision-making capabilities in homeland security and defense. Congress not only should be aware of these computing technologies, but also should encourage their development by creating policy that establishes clear guidelines for responsible use within constitutional limits without impeding future development.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. Andrew Gudgel is a freelance science writer currently residing in Maryland. Oliver Horn, Defense Research Assistant at The Heritage Foundation, contributed to this report.