ATLANTIC COUNCIL

FutureScape

Banning Garrett

STRATEGIC FORESIGHT INITIATIVE

A World Run on Algorithms?

Mostly without our awareness, algorithms now run much of our lives. In the future, they will likely be even more ubiquitous in ever more aspects of our personal and work life.[1] They will increasingly shape our choices and delineate our options. Even more pervasive but less transparent, algorithms will be used to mine and exploit data about us that is collected and stored daily in ever increasing quantities by business and government. Algorithms are also taking many of our jobs.

Mysterious Algorithms

In their simplest and oldest form, algorithms are sets of rules for processing data to produce outcomes. They are “provable, well-defined (and generally well known) solutions to a specific problem set”[2] that can be carried out using the same set of instructions each time, although the number of instructions required depends on the data input.

Algorithms have been around for most of recorded human history. Even basic math such as multiplying two numbers involves the use of an algorithm—specific steps—that will always produce the same outcome for the same two numbers. The Pythagorean Theorem from ancient Greece, still taught to every high-school student, is an algorithm. But although algorithms are not new, they were put on steroids decades ago by computers—all software is built on algorithms[3]—and they are used in every digital device in existence. Now big data, combined with nearly free and unlimited computing processing power and storage, is adding a massive boost to the power and impact of algorithms.

Emerging Technologies and Society

The Emerging Technologies and Society project is a collaboration between Singapore’s Risk Assessment Horizon Scanning Programme Office (RPO) in the National Security Coordination Secretariat (NSCS) and the Atlantic Council Brent Scowcroft Center on International Security’s Strategic Foresight Initiative (SFI). Initiated by RPO, the project focuses on the political, economic, and societal impacts of significant innovations arising from the science and technology fields. Through a series of meetings with leading researchers and private enterprises in the Silicon Valley, the project explores topics ranging from ubiquitous robotics and its impact on human capital developments, to algorithmic risk, quantum computing, and their challenges to national security.

Through horizon scanning efforts, RPO enhances policy making capabilities through engaging analysis, robust processes, and leading-edge systems. The SFI, which strives to forge greater cooperation on futures analysis among its main partners around the world, has rapidly become a hub for an expanding international community of strategic planners in government and the private sector.

RAHS PROGRAMME OFFICE
EXCITE | ENABLE | EXPERIMENT

[1] See Kevin Slavin, “How algorithms shape our world,” TED-Ed, http://ed.ted.com/lessons/kevin-slavin-how-algorithms-shape-our-world.

[2] Software engineer Jay Wettlaufer, private communication.

[3] Wettlaufer notes that “you can equate algorithms to software, although an engineer or mathematician would probably see algorithms as the shared ‘base code’ used by software programs to implement common data structures and procedures.” (Private communication)

Banning Garrett is strategic foresight senior fellow for global trends and innovation in the Atlantic Council’s Brent Scowcroft Center on International Security. The author would like to thank Peter Haynes, Jay Wettlaufer, and Paul Saffo for their invaluable assistance in preparing this report.

A World Run on Algorithms

Without algorithms, modern airplanes would not fly, cars could not be driven, and the rail and subway systems would not work. FedEx and UPS would be crippled as would the Post Office. There would be no digital TV, no cable system, and no telephony (it's been digitally switched for more than thirty years). The energy grid is dependent on algorithms for automatic fault detection and load balancing, among many other things—a dependence that will grow as countries build out "smart grids" to better manage loads and allow for "net metering" that enables consumers to upload solar or wind power they generate. In short, power plants cannot run without algorithms making thousands of decisions per second: without algorithms there would be no electric power. The Internet switching infrastructure is completely dependent on many types of algorithms, including graph theory to route packets of data.

In short, anything software-driven is part of the digital ecosystem that runs our lives, and will be running even more aspects of our lives in the future. For example, in the near future our cars will be far more "intelligent," and we will put our lives more and more in the hands of a vehicle's algorithms for collision avoidance, parking assistance, lane-departure warnings, and smart cruise control with automatic traffic spacing, among other things. Intelligent roads and inter-auto communication will follow, as will fully autonomous vehicles. The experimental self-driving Google cars are run by algorithms that process a gigabyte of data per second from a wide range of sensors, and make thousands of driving decisions per second.

Algorithms to Run Even More of Our Lives

While for many years algorithms have influenced decisions in our personal lives such as guided "matches" on dating web sites, in the future our work lives may also be increasingly run by algorithms. Data scientists are examining work relationships, identifying patterns, and building algorithms to help improve employee collaboration and management of sales relationships, and enabling employees to see how their performance compares with that of their colleagues. A Palo Alto startup called RelateIQ is looking into this. Cofounder Adam Evans recently told the *Wall Street Journal*, "We wanted to build an algorithm that could do what a highly-trained relationship manager, with twenty years of experience, could do."[4]

Improvement in algorithms receives much less public attention than increases in microprocessor performance. The pace of algorithm advancement, however, has far outstripped Moore's Law, which accurately predicted forty years ago that the power of microprocessors would double every eighteen months to two years. An assessment of the speed with which a standard optimization problem could be solved by computers between 1988 to 2003 documented a *43 million*-fold improvement, which was broken down into two factors: faster processors and better algorithms embedded in software.[5] While processor speeds improved by a factor of 1,000, algorithm performance improved by an astounding 43,000-fold over that same period.

Big Data Powered by Algorithms

These vastly improved algorithms have been a key factor powering the age of "big data," a concept with no official definition but which refers to huge volumes of data that are created and captured but cannot be processed by a single computer—instead requiring the resources of multiple machines or even the cloud to store, manage, and parse.[6] This size of "big" data is in excess of a petabyte, or one million gigabytes. Big data includes "images and videos on mobile phones uploaded to YouTube, digital movies populating the pixels of our high-definition TVs, banking data swiped in an ATM, security footage at airports and major events such as the Olympic Games, subatomic collisions recorded by the Large Hadron Collider at CERN, transponders recording highway tolls, voice calls zipping through digital phone lines, and texting as a widespread means of communications."[7] It also comprises billions

[4] "Your New Secretary: An Algorithm," *Wall Street Journal*, June 13, 2013, http://convergence.bna.com/ContentDelivery/ContentItem/Article/23867 0228000000271/386400?Highlight=false.

[5] Erik Brynjolfsson and Andrew McAfee, *Race Against the Machine* (Digital Frontier Press: Lexington, MA, 2011), p. 18.

[6] James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/insights/business_ technology/big_data_the_next_frontier_for_innovation?p=1.

[7] John Gantz and David Reinsel, "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East," IDC Iview, sponsored by EMC Corporation, December 2012, http://www.emc.com/ collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.

of daily search-engine queries, tweets, and Facebook posts. While the amount of information individuals create themselves—writing documents, taking pictures, downloading music, making searches, posting tweets and "likes," etc.—is huge, it remains far less than the amount of information being created *about them* in the digital universe, often without their knowledge or consent.[8]

Algorithms are a critical factor enabling the era of big data, which also has been made possible by virtually unlimited computer processing power and storage, both of which are trending toward "free." Algorithms determine which data is valuable enough to be saved and analyzed and which should be discarded, although increasingly nearly all data is being stored since its future unknown uses cannot be predicted and the costs of storage have declined to virtually nothing. In analyzing the data, algorithms often derive unexpected but important correlations of seemingly unrelated factors, and then determine what actions should be taken, be they with or without direct human intervention.

We see the results of algorithms and big data almost everywhere we turn. All of our Internet searches are based on algorithms. Netflix uses algorithms to assess our previous downloads and suggest other movies we might want to order—and 60 percent of downloads are based on these recommendations. Similarly, Amazon uses data collected about our previous purchases to suggest books we might want to order, again with surprising accuracy. "If you're keeping track, algorithms already have control of your money market funds, your stocks, and your retirement accounts," Christopher Steiner notes, adding "they'll soon decide who you talk to on phone calls; they will control the music that reaches your radio; they will decide your chances of getting lifesaving organ transplants; and for millions of people, algorithms will make perhaps the largest decision in their life: choosing a spouse."[9]

Helping Watson Win *Jeopardy!* and the NSA Mine Data

Some algorithms have their roots in artificial intelligence (AI) and can evolve. "They observe, experiment, and learn—all independently of their human creators," according to Christopher Steiner, author of the bestselling *Automate This*. "Using advanced computer science techniques such as machine learning and neural networking, algorithms can even create new and improved algorithms based on observed results. Algorithms have already written symphonies as moving as those composed by Beethoven, picked through legalese with the deftness of a senior law partner, diagnosed patients with more accuracy than a doctor, written news articles with the smooth hand of a seasoned reporter, and driven vehicles on urban highways with far better control than a human."[10]

One of the most impressive uses of algorithms and artificial intelligence has been IBM's supercomputer Watson that embarrassingly dispatched the top human contestants on the game show *Jeopardy!*. Watson is loaded with hundreds of millions of unconnected digital documents, including encyclopedias, other reference works, and newspaper stories. "When it receives a question, it immediately goes to work to figure out what is being asked (using algorithms that specialize in complex communication), then starts querying all these documents to find and match patterns in search of the answer."[11] IBM is now applying Watson's extraordinary algorithm-driven capabilities to the field of medicine to assist in diagnoses. "Watson doesn't tell a doctor what to do; it provides several options with degrees of confidence for each, along with the supporting evidence it used to arrive at the optimal treatment."[12]

Advanced algorithms have also been critical to the National Security Agency's surveillance effort. Through its "PRISM" program, the NSA has been using algorithms such as Hadoop, which is used by Google and Yahoo! and is available for free,[13] to sort through, correlate, and

[8] John Gantz and David Reinsel, Ibid.

[9] Christopher Steiner, *Automate This: How Algorithms Came to Run Our World* (New York: Penguin, 2012) p. 214.

[10] Christopher Steiner, p. 6. Brynjolfsson and McAffee are less impressed, however. They maintain that "for all their power and speed, today's digital machines have shown little creative ability. They can't compose very good songs, write great novels, or generate good ideas for new businesses." Erik Brynjolfsson and Andrew McAfee, op.cit., p. 25

[11] Erik Brynjolfsson and Andrew McAfee, p. 15.

[12] Bruce Upbin, "IBM's Watson Gets Its First Piece of Business in Healthcare," *Forbes*, February 8, 2013, http://www.forbes.com/sites/bruceupbin/2013/02/08/ibms-watson-gets-its-first-piece-of-business-in-healthcare/.

[13] "Open-Source Spying," *Business Week*, June 17-23, 2013.

analyze billions of phone call records, emails, and other data flowing over the global Internet every day. Robots run on algorithms and they are becoming increasingly connected to the web, feeding data into “big data” streams, and using the computational power of the cloud to enable their artificial intelligence as they become increasingly ubiquitous, moving out of the confines of the factory to work directly with human beings.

Algorithms are being unleashed on massive data flows from potentially billions of sensors on natural and human-created objects as well as on humans themselves, who are carrying data generators such as smartphones. A smartphone’s GPS-enabled tracking system sends information on an individual’s location to the cloud, and returns it as (for example) analyzed traffic information on Google Maps. Virtually everyone will be connected by 2020, Google Chairman Eric Schmidt predicts, thus creating a world of 50+ billion unique nodes producing data through use of the Internet, smartphones, tablets, and other digital devices, as well as through use of machines that leave digital traces from ATMs to airport kiosks, and smart homes, offices and cars that will be awash with sensors monitoring every aspect of our lives. But the big data produced will be useless without algorithms to parse it and take actions based on the analysis.

Next: Algorithms Running the “Internet of Everything”

We are on the cusp of a huge uptake in algorithm-based automation over the next 20 years as the “Internet of Things,” increasingly referred to as the “Internet of Everything” or IoE, comes to the fore. More and more “objects” (robots, home appliances, smart shipping pallets, smartphones, and many more sensors than you can imagine) will have a fixed IP address and be connected—whether on private networks or the Internet itself. This is being made possible by the adoption of a new standard for Internet addresses, called IPv6. IPv6, with its 64-bit address space, enables us to assign 10^39 unique “permanent” fixed IP addresses—in essence, providing a separate IP address to virtually anything. CISCO estimates that with IPv6 there could be 100 IP addresses on the Internet for every *atom* on the surface of the earth.[14] By another calculation you could hand out a million fixed IP addresses per second for almost 600,000 years before you ran out. In any case, every object on earth could have a unique IP address and act as a sensor. These sensors will be able to provide data identifying the object, its geolocation, and any specific information it is programmed to gather and transmit, such as temperature, humidity, wind speed, moisture levels, and health data—all of which will be analyzed by algorithms. This will provide the critical building blocks for the IoE. CISCO estimates that there will soon be 15 billion “things” connected to the Internet, with 50 billion predicted by 2020. Within a few decades, there could be trillions.

Risks of an Algorithm-Run World

While algorithms, big data, and the IoE are making important contributions in science, health care, efficient use of resources, and smart cities, there are concerns about a “dark side” of algorithm-driven big data. There have been increasing privacy concerns about businesses such as Google, Yahoo!, Amazon, and others accumulating massive amounts of data that will be sifted and analyzed by algorithms to target specific individuals in their marketing. A Netflix challenge embarrassingly demonstrated that with just a few data points, analysts using the Netflix data and public information could pinpoint a specific individual Netflix subscriber.[15] While businesses may gather massive amounts of personal data that can be used to sell products to you, government could potentially use that data to spy on and prosecute you. The recent revelations about the NSA’s PRISM program have provoked a major debate over the potential for surveillance by governments now and in the future. The algorithms behind big data analytics could be used to identify specific individuals, including dissidents.

Algorithms unleashed on big data can lead to misuse at the expense of innocent individuals. Spurious correlations can affect an individual’s future; for example, employers making hiring decisions on the basis of what kind of

[14] http://blogs.cisco.com/wp-content/uploads/internet_of_things_infographic_3final.jpg.

[15] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, (New York: An Eamon Dolan Book-Houghton Mifflin Harcourt, 2013), p. 155.

Benefits of the Algorithm-Powered Internet of Everything (IoE)

The IoE will enable computers powered by increasingly sophisticated algorithms to know where everything is and be able to track it and make decisions based on this information and analysis. This will result in many cost efficiencies. A few examples:

- A reduction in energy wasted on inefficient shipping and warehousing.
- Supply chain efficiencies. A reduction in the cost of the "Cold Chain"[1] in particular would result in huge energy savings.
- A reduction in the cost of repairs for many larger appliances and machines. "Things" will call the repairman themselves with full diagnostics when a small part is on the verge of failure instead of waiting for a human being to notice failure which could have spread to many other parts by then.
- Smart (very smart) homes that would know to manage energy. The primary automation unit would be able to change the state of anything consuming power in the house and provide the owner with centralized control of everything electrical (infotainment, power, lighting, etc.).
- New heights of factory automation, including powering the Third Industrial Revolution with 3D printing and other advanced manufacturing technologies that rely on increasingly sophisticated algorithms. Provides the ability to track everything at all times on the factory floor and feeder warehouses as well as monitor the assembly process and all the machines involved.
- Far safer food supply allowing nearly instantaneous sourcing of tainted goods as well as the ability to detect and report spoilage automatically.
- Automated surveillance that will be much easier and cheaper.
- Tracking virtually everything in the health care system, including patients.

[1] A cold chain is a temperature-controlled supply chain. An unbroken cold chain is an uninterrupted series of storage and distribution activities which maintain a given temperature range. It is used to help extend and ensure the shelf life of products such as fresh agricultural produce, seafood, frozen food, photographic film, chemicals and pharmaceutical drugs. See Wikipedia, http://en.wikipedia.org/wiki/Cold_chain.

Internet browser was used to file an online application,[16] or Google Flu Trends analysis being used in a pandemic to quarantine an individual who made a search correlated with flu symptoms because the individual feared coworkers exhibiting symptoms and wanted protection.[17]

There is also growing concern over the use of predictive algorithms that could be used in scenarios similar to the movie *Minority Report* where individuals were arrested for crimes before they committed them. Based on correlations of certain behaviors and traits, algorithms could identify people as having a "propensity" to crime, anti-social behavior, or other actions that have not yet occurred, thus justifying preventive action against that individual.[18] Already, insurance companies and parole boards are using predictive algorithms to help tabulate risk, and a growing number of places in the United States employ "predictive policing," crunching data "to select what streets, groups, and individuals to subject to extra scrutiny, simply because an algorithm pointed to them as more likely to commit crime."[19]

The Obama administration employs so-called "signature" strikes, wherein "intelligence officers and drone operators kill suspects based on their patterns of behavior–without positive identification."[20] With signature strikes, the CIA doesn't know the identity of the persons whom it is killing. NBC quotes "one former senior intelligence official" claiming "that at the height of the drone program in Pakistan in 2009 and 2010, as many as half of the strikes were classified as signature strikes."

These dangers highlight a key limitation of algorithm analysis of big data: the results are based on correlations, not causality. That is, certain factors are correlated

[16] "Robot Recruiting: Big Data and Hiring," *The Economist*, April 6, 2013, http://www.economist.com/news/business/21575820-how-software-helps-firms-hire-workers-more-efficiently-robot-recruiters.

[17] Viktor Mayer-Schonberger and Kenneth Cukier, p. 169.

[18] Viktor Mayer-Schonberger and Kenneth Cukier, Ibid., pp. 157-158; 163.

[19] Viktor Mayer-Schonberger and Kenneth Cukier, Ibid., pp. 176-178.

[20] Richard Engel and Robert Windrem, NBC News,"Exclusive: CIA didn't always know who it was killing in drone strikes, classified documents show," June 5, 2013, http://openchannel.nbcnews.com/_news/2013/06/05/18781930-exclusive-cia-didnt-always-know-who-it-was-killing-in-drone-strikes-classified-documents-show.

with certain outcomes but without discovering a causal relationship.[21] The algorithms analyzing the data do not explain why things happen but only that they correlate with each other. “Of course, causality is nice when you can get it,” according to Viktor Mayer-Schonberger and Kenneth Cukier, but, they insist, correlations are often good enough and they can be found “far faster and cheaper than causality.”[22] The authors of *Big Data* note that algorithm-driven big data analysis correlations can predict flu outbreaks, translate languages, and enable cars to drive themselves. But correlations can also lead to mistaken analyses and harmful decisions based on the “fallacy of numbers” and the “dictatorship of data.”[23]

Algorithm-driven decision-making can take humans out of the loop with disastrous results. An often-cited example resulted when two algorithms competed to outbid each other on Amazon to buy a rare book, bidding up the price of a $100 book to $24 million before a human finally intervened to stop the madness.[24] Another example was the 2010 stock market flash crash of nearly 1,000 points that erased $1 trillion in wealth in a few minutes. Although the precise cause of the flash crash was never determined with certainty, it was at least in part due to algorithms leading a massive sell-off without a human ordering the actions. A similar algorithm-generated sell-off occurred in April 2013, when AP’s Twitter account was hacked and a false tweet sent asserting that President Obama had been injured by a bomb at the White House. An algorithm “reading the news” by associating “bomb” and “White House” and apparently concluding that the reported bombing would send stocks sharply lower ordered a quick sell, triggering a brief $136 billion sell-off in the market.[25] While there have been efforts to establish safeguards, future algorithms-triggered actions leading to “flash crashes” are inevitable. This is no small matter since increasingly, “algorithms are the stock market,” according to Steiner, who estimates that 60 percent of all trades in the United States are carried out by algorithms.[26] Kevin Slavin from the MIT Medialab estimates that on Wall Street alone, 70 percent of trades are made by algorithms. Moreover, he argues that “we are living in a world designed for—and increasingly controlled by—algorithms. These complex computer programs that determine espionage tactics, stock prices, movie scripts, and architecture,” Slavin warns, “are based on code we can’t understand with implications we can’t control.”[27]

Algorithms can also be used as the basis of autonomous cyber weapons capable of creating physical destruction. Jason Healey, director of the Atlantic Council’s Cyber Statecraft Initiative, notes that “Stuxnet, part of the ‘Olympic Games’ covert assault by the United States and Israel on Iranian nuclear capability, appears to be the first autonomous weapon with an algorithm, not a human hand, pulling the trigger.”[28] Unlike semi-autonomous military hardware such as drones that have a human in the loop to make final decisions about whether to proceed with an attack, Stuxnet was designed to infect systems and decide unsupervised whether and when to launch an attack that led to the self-destruction of Iranian centrifuges reportedly producing weapons-grade uranium. “Whoever created Stuxnet should be congratulated for having crafted it so carefully that it made the correct autonomous decisions,” Healey maintained, “but autonomous military destruction may not ultimately be in our national (or indeed human) interest. It was good that Stuxnet’s American designers took this care, but will Russian or Chinese developers be so cautious?” He adds, “Now that we know about Olympic Games, we should begin the real debate of whether and when our cyber weapons should make their own decisions about when to destroy on our behalf.”

Algorithms are eliminating many jobs, and this is expected to be a long-term, structural trend. The jobs that will be lost are not only those of assembly-line workers and those doing menial, repetitive tasks, but also professionals such as lawyers, doctors, psychiatrists, and writers as well as

[21] Viktor Mayer-Schonberger and Kenneth Cukier, p. 191.

[22] Ibid., p. 191.

[23] Viktor Mayer-Schonberger and Kenneth Cukier, op.cit., p. 166.

[24] Christopher Steiner, pp. 1-2.

[25] “False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked,” CNBC, April 23, 2013, http://www.cnbc.com/id/100646197. “That goes to show you how algorithms read headlines and create these automatic orders – you don’t even have time to react as a human being,” said Kenny Polcari of O’Neill Securities, on “Power Lunch,” CNBC reported.

[26] Christopher Steiner, p. 49.

[27] Kevin Slavin, op. cit.

[28] “Stuxnet and the Dawn of Algorithmic Warfare,” *New Atlanticist*, Atlantic Council, April 17, 2013, http://www.acus.org/new_atlanticist/stuxnet-and-dawn-algorithmic-warfare.

those of truck drivers and musicians.[29] In the legal industry, for example, on one estimate, moving from human to algorithm-power data analysis during the discovery process could enable one lawyer to do the work of five hundred. [30] Beyond algorithms assisting humans in performing more and more professional and service jobs, algorithms are increasingly replacing people completely as computers talk to other computers without human intervention, performing such mundane tasks as handling airport check in and performing banking transactions. The long-term possible implications are the elimination of jobs by algorithms with a widening gap between the top and the bottom of society and increasing "technological unemployment" as many well-paying jobs just disappear. Whether they will be replaced by entirely new, well-paying jobs is uncertain and worrisome to many analysts.[31]

Algorithms can be vulnerable to malicious hacking with potentially catastrophic effects. Hackers potentially could alter basic algorithms guiding transportation vehicles such as airplanes and cars, leading to crashes, or bring down critical utilities such as electric power grids and water supply systems.

Failsafe and Safeguard Systems

A more vigilant approach to the construction and maintenance of critical infrastructure will be required in the future. Key systems relying heavily on software and its underlying algorithms are becoming progressively more capable and complex. To keep pace with the potential of failure, we need to increase investments in both up-front testing and subsequent monitoring of these systems. Software testing is a known art, but often given short shrift because of budget and time constraints. The creation of complete test coverage for a software system usually requires considerably more effort than writing the original code, potentially doubling or tripling the cost. NASA has spent a great deal of money in the past identifying and enforcing a very high level of software quality assurance and testing.[32]

No matter how well written or extensively tested algorithms are, there will almost always be real world exceptions to the "rules" they define. Exceptions will occur when algorithms face an unforeseen combination of events/inputs and can make the system fail partially or completely. This state can be brought about in many ways including communications failures, sensor failures, computer or data storage failures, incorrect input, unforeseen data volumes, or simply bugs in the code.

Given the potential for sizeable damage, key systems should always require a separate infrastructure to instrument and monitor them. Ideally it should run on separate hardware and communications infrastructure and be able to use raw sensor data and other external inputs. A simple example for illustration would be an automobile monitoring system that would intentionally cripple the engine if it senses oil pressure cannot be maintained at a proper level. This would allow the car to be driven to a repair facility by limiting the engine to a low RPM. While potentially running on the same computer (the car's electronic control unit), which is not optimal, the software itself would be separate from the real time engine management algorithms that would let you merrily drive your car until the engine is ruined—even with a warning light on.

A more complex example would be NASA's real-time instrumentation and monitoring of all extraterrestrial probes and satellites. These systems monitor a very large number of sensors and time series data as well as the performance of the control software. The monitoring system can automatically put the vehicle in a safe mode if a fault is detected. Human intervention is most often required to analyze the anomaly and correct it, but the system itself

[29] Steiner, p. 217.

[30] Bjornjolfsson and McAfee, p. 23. The authors also cite a *New York Times* story by John Markoff from March 2011 that one company helped a client analyze 1.5 million documents for $100,000.

[31] This is the theme of Bjornjolfsson and McAfee's *Race Against the Machine*. See also David Rotman, "How Technology Is Detroying Jobs," *MIT Technology Review*, June 12, 2013, http://www.technologyreview.com/contributor/david-rotman/, and W. Brian Arthur, "The Second Economy," *McKinsey Quarterly*, October 2011, http://www.mckinsey.com/insights/strategy/the_second_economy. Arthur maintains: "Now this second, digital economy... is running an awful lot of the economy. [...] In any deep transformation, industries do not so much adopt the new body of technology as encounter it, and as they do so they create new ways to profit from its possibilities."

[32] See JPL Laboratory for Reliable Software (LaRS) for additional information: http://lars-lab.jpl.nasa.gov.

is able to shut itself down for protection. These systems are especially important for planetary probes with long communication delays between the probe and ground control. Even so called "self-healing" systems still require a separate monitoring system to detect failure.

The financial system especially requires failsafe and safeguard systems. The NASDAQ and New York Stock Exchange have market monitoring systems that alert the exchange when erroneous trades occur or there is a much more serious issue occurring such as the Flash Crash. This allows them to halt trading in a particular security or to potentially halt the entire exchange.

Conclusion

The world already runs on algorithms, and this dependency will only increase in the future, especially as our planet is wired up with tens of billions of sensors in the Internet of Everything. They are key to the systems supplying our basic needs and the foundation of civilization. They are critical to our energy systems, our food production and distribution systems, our water supplies, our communications systems, virtually all of our governmental, health, educational, and financial systems. Algorithms are critical to the functioning of our national defense systems–from the systems that provide intelligence and reconnaissance to those that enable weapons to defend us. The list of systems in modern society depending on algorithms is virtually inexhaustible. Failure, breakdown, hacking, or sabotage of algorithms could threaten any of those systems–and algorithm failure in the energy systems would ricochet through most of our other critical life-support systems from water to heating and cooling to food supplies.

We don't "see" algorithms like we see the devices that use them–from our smartphones and computers to our trains, planes, and automobiles. We don't even "see" the algorithms when we become aware of the massive accumulation and analysis of data on us by business and government. But without them there would be no computers, no Internet, no modern communication, transportation, or energy and water systems. In short, our modern world would grind to a halt.

Algorithms are essential and mostly reliable, but the world is highly vulnerable should they be misused, hacked, sabotaged, or simply fail. Measures to protect society and government from algorithm risks start with recognition of their critical, the risks they pose, the range of systems and types of algorithms that run them, and the vulnerability of these algorithm-powered systems. Enhancing cyber security in all forms, to protect against algorithm hacking and failure, is essential. But the vulnerabilities of embedded algorithms may pose problems beyond the usual concerns about cyber security, especially as billions of poorly protected algorithm-run sensors are connected to each other and the Internet. And algorithms can be used as cyber weapons to create destruction in the physical world, as demonstrated by the Stuxnet worm.

There may also be need for regulation of the use of algorithms, especially in financial systems and the exponentially-increasing collection and analysis of personal data by a growing number of businesses. Additionally, we may need to regulate the use of algorithms acting without human supervision. Christopher Steiner warns that "left unsupervised, algorithms can and will do strange things. As we put more and more of our world under the control of algorithms, we can lose track of who-or what-is pulling the strings."[33]

We should not lose sight of the huge benefits of algorithms, not only in running our basic systems but in pushing the frontiers of science, especially in understanding our natural environment, improving our health, making our cities more energy and resource efficient, increasing access to knowledge and education, widening our personal networks, and enhancing productivity. Nearly all the benefits and promise of the modern world depend on algorithms. Governments should not only protect against the risks of algorithms, but also foster and promote the benefits of an algorithm-run world.

JULY 2013

[33] Christopher Steiner, p. 5.

Atlantic Council Board of Directors

**Members of the Executive Committee*
List as of April 24, 2013

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005
(202) 463-7226, www.acus.org