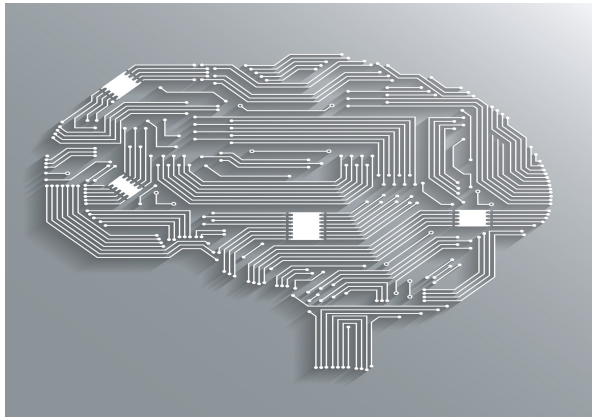
AI Friends, AI Foes

Summary: AI systems will become central to ever more activities, with human-machine cooperation increasingly pervasive in business and industry. Automation will enhance security by enabling new types of threat detection and response. However, these tools in the hands of malefactors will expose and create new vulnerabilities in systems previously thought secure.



Forecasts

- Automation could increase the general public's expectation of security and protection: everything can be monitored, so it should be. Consumers will expect that the tradeoff of privacy for security will yield positive results.
- The combination of AI and sensors could create pervasive security nets. For example, there would be no need to spot-check shipping containers, if each is self-monitoring and reporting.
- Multiple countries, especially the U.S. and China, will vie for leadership in developing and deploying AI, and the outcome of this competition could create security issues.
- AI's use in information-gathering in security could benefit from people feeling more comfortable interacting with an AI than with a human on sensitive matters.
- The "black box" results of AI systems could lead to user confusion as these systems analyze and draw connections beyond the scope of human reasoning.

Key uncertainties affecting AI and security:

- Speed of AI technical advances
- The degree and speed of automation deployment
- International competition in AI innovation
- Consumer concerns over algorithmic bias built into AI systems
- How private and governmental use of automation are regulated
- Consumer comfort with the convenience/security vs. privacy trade-off

Supporting trends

Self-teaching AI. Artificial intelligence systems are now capable of self-teaching. The AlphaGo Zero software was able to train by playing Go against itself and beat the previous world-champion AlphaGo program after only a few days of learning.

Accountable AI. Accountability and transparency technologies for machine learning are making it easier for humans to understand the decision-making of AI systems and neural nets.

AI-to-AI collaboration. Experimental AI systems are able to develop new AI languages to improve their own collaboration and effectiveness.

Machine learning model extraction. Machine learning algorithms can be used to uncover hidden information, such as pixelated images or the inner workings of algorithms themselves.

AI for national power. Artificial intelligence is increasingly seen as a vital component of national power, with national governments restricting foreign investment or technology transfer.

Trait identification via facial features. Researchers claim success in developing machine-learning systems for predicting traits like criminality or sexual orientation from facial images.

Smart surveillance. Smart surveillance systems are able to use sensor-fusion technologies to track shoppers picking specific products off shelves in real time.

Secure machine learning. Techniques that enable machine learning using encrypted data sets allow AI analysis to be outsourced or crowdsourced, even for sensitive data.

Data points

Data is the new oil. Data is what fuels machine learning and AI systems, and the sheer size of its consumer population allows China to generate a lot of data. China's bikeshare program alone generates 30 terabytes of sensor data a day.

The right to know how a system thinks. In response to concerns about algorithmic decision-making and AI, the EU is implementing rules in 2018 that will require companies to explain to people how a decision was made, even if the decision was made by an AI system.

Pentagon spending on AI. The U.S. Defense Department spent $7.4 billion on AI in 2016, up from $5.6 billion in 2011.

Topics for additional research

- What human skills need to be developed to serve human-machine cooperation
- What AI systems being developed are likely to have future security relevance

ASIS INTERNATIONAL

Strategic insights

For the security industry

- The threats posed or created by expanding AI systems will evolve rapidly and the industry will have to keep up with rapid advances.
- China is working to make itself a leader in this space, but its efforts could be hampered by the fact that AIs trained in one culture will in some cases not easily transfer to another culture, where norms and behaviors are different. Still, China is likely to be a font of AI innovation, especially in the security realm.
- As AI systems come online and become more integrated with security there will be pressure—from customers and the C-suite—to apply AI to all manner of issues, outrunning actual capabilities.
- The spread of AI systems will further the integration of security with organizations' IT functions. Cybersecurity will need to include protecting proprietary AIs and the functional integrity of AIs.

For ASIS

- Going forward, there will be a 'Wild West" period when society, corporations, and governments figure out the line between the capabilities of these systems and what is allowable. There is a role for ASIS to help put forth ideas for governance and usage standards.
- ASIS could play a role in educating internal and external customers in the evolving capabilities—and limitations—of automated security tools and functions.
- The wide interest in and the flood of stories about AI, along with the speed of change in the field, mean that there is a lot of confusion and uncertainty around the technology. ASIS could serve as a clearinghouse for its members, not only passing along the newest, most relevant information about new AI products, but also best practices for further professional development of members.

Timing

- **Stage**: Growth stage, in a period of strong expansion, and hype
- **Speed**: Rapid and accelerating as proofs-of-concept are deployed

Potential alternative futures

- **Black box doubts:** Inexplicable results from AI systems confuse users and cause them to ignore solutions and analysis, impeding AI adoption.
- **Privacy pushback**: Citizen concerns over how much AI security systems are learning about their lives leads to a backlash and increasingly restrictive regulations.
- **AI eats the industry:** The expanding ability of AI to monitor and analyze security data, and in some cases forecast potential security problems, leads to a rapid automation of security jobs.