Thought Paper - Artificial Intelligence

Introduction

Artificial Intelligence or 'AI' is a collection of computer technologies that are able to perform tasks that emulate human intelligence. Technologies of AI include Machine Learning, Deep Neural Networks, Deep Learning and Natural Language Processing; these technologies are used to create various types of Cognitive or 'Smart' Applications.

The massive computing power of today combined with Deep Learning (Google's neural network has more than a billion connections[1]) will lead to further breakthroughs in image recognition, search capabilities, machine 'reasoning', predictive analytics and Natural Language Generation. As an example: speech to speech technology has led the 'Chatbot' revolution as a more efficient way to interact with clients or customers. Gartner estimates an increase in the use of Virtual Customer Assistants from less than 2% in 2017 to 25% in 2020, reducing inquiries up to 70% and allowing for a 33% cost reduction per interaction, with significantly greater customer satisfaction.[2]

The fear that Artificial Intelligence will displace workers is a notion generally confused with automation. The greatest benefit of AI is **AI augmentation**, a complement of artificial and human intelligence together. With AI will come a demand for unique skills (data scientists and intelligence engineers) creating an estimated 2.3 million jobs in 2020. By 2021, AI augmentation is forecasted by Gartner to generate an amazing $2.9 trillion in business and recover 6.2 billion hours of worker productivity.[3]

Definitions

Machine Learning (ML), through exposure to large data sets (sometimes repetitively), discovers patterns and generates conclusions based on historical information or human behaviour models.
Deep Neural Networks, through isolating key areas or fields of Machine Learning, create a specialized version of advanced and predictive analytics such as customer behaviour, big data analytics and machine to human interface.
Deep Learning (subset of ML) studies layers of neural networks going beyond tasks and data analytics to mimic the neocortex of the brain. The software 'learns' to recognize patterns in digital representations of sounds, images, and other data.
Natural Language Processing (NLP) breaks down structured and unstructured inputs into language the machine can understand, act upon and respond to in a way the user will understand.

Government Use Cases

Governments are using Artificial Intelligence to develop **'Smart Cities'**, **'Smart Buildings'** and **'Smart Services'**. The superior computing power of AI components allow for 'intelligent automation' of government functions by integrating the Internet of Things, performing predictive and risk modeling, automating tasks, controlling back end content and services and providing video or image analytics, to name a few. AI is already being used in the areas of Finance, Law Enforcement, Defence, Terrorism, Investigation, Intelligence, Threat Intelligence, Intrusion Protection, Public Safety and Emergency Response.[4]

The Province of BC is integrating policies and programs with the following AI projects (most are under development):

Natural Resources Sector: Robotic Process Automation (RPA) – FrontCounter BC
- The Natural Resource Sector's proposed Virtual Assistant for over 120 online applications

Education Sector: NGN IAC Project – School Districts
- Using ML and AI for predictive planning of network usage, bandwidth cost and education analytics

Jobs and Tourism: Integrated Data Office, Stats BC
- Large volume analysis and statistical learning to improve voter registration, NLP to analyze survey feedback

Citizens' Services: Real Properties Division 'Energy Smart' Smart Building Strategy
- Building a strategy to invest in energy reduction and integration of AI to create smarter, more efficient buildings

Justice Sector: Civil Resolution Tribunal (first wave AI)
- Expert knowledge base providing expert advice and guidance for problems and disputes

AI Specific Policies and Standards

While existing privacy, security, data transfer and data sovereignty legislation and regulations need to be considered, there are no formal definitions or approved standards governing the development or use of Artificial Intelligence.

There are a few standards and recommendations specific to AI:

International: Two ISO/IEC standards (*under development)* for AI (ISO/IEC AWI 22989 and ISO/IEC AWI 23053)[5]
Five IEEE-SA recommendations for the ethical use of AI (IEEE-SA 7006 through IEEE-SA 7010)[6]

Government of Canada: AI standard (*under development*), *The Treasury Board Standard on Decision Support Systems*

European Union: General Data Protection Regulation (Article. 22), *Automated Individual Decision-Making, Including Profiling*[7]

AI in Security and Privacy

The Benefits of using advanced analytics of AI in security show a dramatic decrease in time involved in detection of malware and incident detection and response. AI automation can identify, monitor and manage our cloud access security brokers, identity and access management, vulnerability scanners and security status across the network. Enhancing your system with an AI component will allow for detection of an anomaly event or degradation of a server in an instant, help to create benchmarks, strategies and predictions and track trends or performance. Major AI companies (Amazon, Google, Microsoft, etc.) offer readily available cloud-sourced ML engines, utilities and tools as a service.

The Dark Side of AI technologies can open the door for complex and sophisticated attacks against the network. An innocuous AI agent can lay in wait in a system, gather information and 'learn' which attacks would be most efficient; an attack can auto-activate when a specific target becomes vulnerable. AI technology is most effective at detecting and learning from its connections such as IP addresses or IoT devices. One of the largest Distributed Denial of Service attacks on a network used an IoT botnet containing over a million devices; in the future, it could be billions.

Privacy is a consideration as AI presents new opportunities to identify, track or profile individuals. AI enables large data sets to be collected and analyzed that may not be personally identifiable on their own, but when combined with other large datasets may become personally identifiable information (also known as the mosaic effect). Furthermore, AI may be capable of re-identifying anonymized data.[8] If information is re-identified and therefore personally identifiable, it is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or the Personal Information Protection Act (PIPA). These are risks that ministries must consider when contemplating the use of AI.

Recommendations

- Adopt an AI strategy for your organization; first assess which business outcomes would benefit most from AI and perform an evaluation as you would any new technology against its outcomes.
- Many AI applications and tools are accessed through the Cloud; ensure you have a cloud management strategy in place and adhere to the Cloud Adoption Security Framework.[9]
- When introducing an AI component, pay attention to the AI 'ecosystem', what new connections may arise and what influences may be imposed on other systems.

- Finally, ensure there are no unapproved AI applications being used in your ministry. For every new or proposed AI system, project, program or activity, a Privacy Impact Assessment (PIA) and Security Threat and Risk Assessment (STRA) must be prepared and approved outlining risks, mitigations and written acceptance of residual risks.

Final Thought

While Artificial Intelligence has come under scrutiny for its bias in decision-making processes, it has been described as one of the primary disruptors and drivers of the 'Fourth Industrial Revolution'.[10] It is here, its emerging technologies are everywhere and it is changing our world.

Endnotes:

[1] https://www.technologyreview.com/s/513696/deep-learning/
[2] Gartner article, *Is Your Digital Government Platform Ready for Virtual Assistants and Chatbots?*
[3] Gartner article, *Prepare for When AI Turns Skilled Practices into Utilities*
[4] *IDC's Worldwide Semi-annual Cognitive/Artificial Intelligence Systems Spending Guide*
[5] https://www.iso.org/standards.html
[6] http://standards.ieee.org/findstds/index.html
[7] https://gdpr-info.eu/art-22-gdpr/
[8] Privacy International, *Privacy and Freedom of Expression in the Age of Artificial Intelligence*
[9] Cloud Adoption Security Framework
[10] https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

Resources:

https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1744/RAND_RR1744.pdf
https://www.ansi.org/news_publications/news_story?menuid=7&articleid=c9c4ec49-640e-4192-a1c0-15c319ba3a86
https://searchcio.techtarget.com/news/450431970/At-AI-World-black-cat-problems-and-data-mysteries-abound
Dun & Bradstreet's chief data scientist: Don't ignore these eight AI topics
https://emerging.digital.gov/ (Atlas of open source emerging technologies by the US Government Services Administration)
https://medium.com/artificial-intelligence-policy-laws-and-ethics/the-ai-landscape-ea8a8b3c3d5d (AI Policy Landscape)
http://www.bclaws.ca/Recon/document/ID/freeside/96165_00 (Freedom of Information and Protection of Privacy Act)
http://www.bclaws.ca/Recon/document/ID/freeside/00_03063_01 (Personal Information Protection Act)