AI and Implications on National Security

Views, Critique and Recommendations of AI's developments in forming national policy for AI Security.

KVA Sachintha

IT 16158528

September 5, 2019

Introduction

Artificial intelligence (AI) may be the most important global issue of the 21st century, and how we navigate the security implications of AI could dramatically shape the future of Sri Lanka. Recent advances in AI and computing has led to an unprecedented growth in AI based technologies. While this may be counted as a positive, one should closely and thoroughly reflect on the implications of such findings. A pro-step in that direction is being set forward by the Sri Lankan Government as part of National Policy which can tame and simultaneously allow space for AI to flourish in our island.

This document aims to address key points where AI interacts with governance structures in social, political and economic contexts.

Secure integration of AI with other technologies and Systems

AI in itself is a multifaceted technology that can be adopted and used in unison with prevailing systems and technologies. The use of AI with governmental systems such as traffic management, energy distribution, military etc. can have a huge impact into the efficiency and profitability of those services. But, understanding the implications and the authority placed on AI in each instance of its deployment within public infrastructure should be introspected deeply. For instance, the use of AI in military decision making and/or threat identification could be destabilizing if an AI system fails to identify the true nature and implication of a threat, regardless of it magnitude.

Since Sri Lanka is (still) not a nuclear state, the catastrophic premonition of using AI with military systems could be disregarded for the near future. However, the Government should play an active role in the integration of AI into public (digital) infrastructure with the expertise from individuals in AI research to philosophical experts (to a varying degree).

There are numerous uses for AI in the military, but the boundaries around what constitutes acceptable uses are highly contentious. Weapon systems with certain degrees of automation are already in use. Israel Aerospace Industries has developed a warhead missile nicknamed Harpy that detects and attacks autonomously; Harpy has already been sold to the Air Forces of several countries[1].

[1] Harpy is a "Fire and Forget" autonomous weapon, launched from a ground vehicle behind the battle zone https://www.iai.co.il/p/harpy

Government-led direction and expertise in AI and Digital Infrastructure

AI systems will facilitate governments manage administrative burdens and resource constraints, for instance by automating data entry, optimizing planning and designing, and providing support with client service[2].

However, in the absence of uniform safety and effectivity standards for AI models, finding safe, reliable, and fair AI tools is as much a challenge as getting the tools themselves. Governments are attempting to balance the goals of grasp and profiting from this technological advance, while additionally considering applicable policy environments for AI development and use.

"Government AI Readiness Index" published by Oxford Insights measured how prepared national governments are to take advantage of the benefits of automation[3]. The index looks at metrics such as digital skills, government innovation, and data capabilities. The report found the UK government to be the most prepared, and the US government to be second. Sri Lanka should take example from these nations as to how these "measurement indexes" could be improved or implemented if Sri Lanka is to utilize AI in the coming future.

In September 2018, the Artificial Intelligence in Government Act was introduced by a group of bipartisan US senators as an acknowledgment of the need to improve the use of AI across the federal government of USA[4]. The bill seeks to achieve this by providing resources and directing federal agencies to include AI in data-related planning. The AI in Government Act would,

- expand an office within the General Services Administration to provide technical expertise to relevant government agencies; conduct forward-looking, original research on federal AI policy; and promote U.S. competitiveness through agency and industry cooperation;
- establish an advisory board to address AI policy opportunities and challenges for executive agencies;
- direct the Office of Management and Budget to establish a strategy for investing and using AI as part of the federal data strategy; and
- direct the Office of Personnel Management to identify skills and competencies for AI and establish a new or update an existing occupational series.

The bill specifically states that the Federal Government will liaise with private industries to spearhead the governments' competency in AI. It also states the establishment of an Advisory

---

[2] William D. Eggers, David Schatsky, and Peter Viechnicki, "AI-augmented government using cognitive technologies to redesign public sector work," Deloitte Center for Government Insights, Deloitte University Press, 2017, https://www2. deloitte.com/content/dam/insights/us/articles/3832_AI-augmented-government/DUP_AI-augmented-government.pdf.

[3] Richard Stirling, Hannah Miller and Emma Martinho-Truswell, "Government AI Readiness Index," Oxford Insights, April 26, 2018, https://www.oxfordinsights.com/government-ai-readiness-index.

[4] https://www.schatz.senate.gov/press-releases/schatz-gardner-introduce-legislation-to-improve-federal-governments-use-of-artificial-intelligence

board to address the AI policy opportunities for executive agencies within the Federal Government.

Sri Lanka should also look into establishing an executive agency in regards to AI and automation etc. and get key and learned individuals to head the agency and provide direction to the Governments' AI agenda.

Assuring public safety through AI

AI tools are being employed to promote growth, safety, and social good around the world, for instance by supporting the advancement of the sustainable Development Goals (SDGs). However, AI tools may also be employed in ways in which curtail human rights. for instance, automatic face recognition and alternative surveillance tools are often wont to target individuals based on their physical look for added screening by law enforcement or immigration authorities[5].

Sri Lanka can use these kinds of technologies with notable supervision to handle illegal immigrant issues as well as identifying criminals. The scope of surveillance that is undertaken should be clearly disseminated to the public and all procedures in which surveillance data is processed and stored should also be defined.

Even though allegations by Edward Snowden against the NSA in the United States for mass spying on American citizens met with a sizable protest, given the subject of mass surveillance being a touchy subject, Governments should actively take part in creating surveillance schemes without exploiting the general public. Actions taken in the name of National Security should be a compromise between individual freedom / privacy and safety of the citizens.

It should also be noted that most people have grown wary of sharing personal information on digital platforms. The Facebook and Cambridge Analytica scandal in early 2018 showed that a third-party company was able to gain access to 50 million Facebook profiles and use the harvested data for mass targeting with the aim of swaying voter behavior[6]. The Sri Lankan Government with its resources and information about almost every individual in the country holds the means to build efficient AI systems with these datasets. The usage of these tools should be clearly defined and supervised such that they aren't used at a disadvantage to the general public.

---

[5] Maya Kosoff, "China's Terrifying Surveillance State Looks a Lot Like America's Future," Vanity Fair, July 9, 2018, https:// www.vanityfair.com/news/2018/07/china-surveillance-state-artificial-intelligence.

[6] Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," The New York Times, March 19, 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Promotion of Research and Development into AI

Advances in artificial intelligence promise to fuel significant global economic growth, but without adequate investment in research and development this outcome will not be accomplished. For instance, China increased research and development (R&D) financing for AI by 200 percent between 2000 and 2015, and anticipated to overtake the U.S. in investment by the end of 2018[7]. If Sri Lanka is to utilize AI, the need for Research and Development within the country is salient.

To propel the development of AI technologies, many countries are interested in expanding and improving the opportunities for training and education in AI research. Simultaneously, there is growing acknowledgment of the need to revamp educational opportunities for a world in which automation is playing a greater role. This includes not only STEM fields (science, technology, engineering, and math), but also social sciences and the humanities, as it has become more apparent that so-called "soft skills" may be more uniquely human and less prone to automation[8].

This includes, but not limited to,

- Establishing R&D Institutions in Sri Lanka
- Bringing in foreign investments in terms of finances and researchers.
- Increasing Government Funding into AI Research
- Establishing syllabuses that align with AI and Data Science from School / undergraduate students.
- Increasing social awareness of AI predominantly among school children and youth.
- Providing access to AI resources / training materials / lab environments for accelerated learning.

Since some of the above recommendations take time to fruition, Sri Lanka can take France as an example in which the French Government with the intention of tripling the number of people trained in AI over the next three years, they are amending existing educational programs in the country to refocus on AI and by establishing new programs and courses specifically designed to teach AI skills to more people[9]. In addition, the French also hopes to establish a network of four to six interdisciplinary institutes for AI at universities across the country. These direct steps can assure that a country's population will be leaned and read in the field of AI, ready to contribute to the workforce.

---

[7] Chairman Will Hurd and Ranking Member Robin Kelly, "Rise of the Machines," Subcommittee on Information Technology, Committee on Oversight and Government Reform, U.S. House of Representatives, September 2018, https://oversight.house.gov/wp-content/uploads/2018/09/AI-White-Paper-.pdf.

[8] Adam J. Gustein and John Sviokla, "7 Skills That Aren't About to Be Automated," Harvard Business Review, July 17, 2018, https://hbr.org/2018/07/7-skills-that-arent-about-to-be-automated.

[9] Cedric Villani, "For a Meaningful Artificial Intelligence Towards a French and European Strategy," March 8, 2018, https:// www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.