DEBI ASHENDEN

DATA AND THE SOCIAL AND BEHAVIOURAL SCIENCES

The science of how we manage and leverage data is unsurprisingly an increasingly ubiquitous topic. Data is often thought of as the base of a pyramid on which information, knowledge and wisdom sit. Data science is the extraction of information from data with the aim of developing knowledge.

The emergence of data science is driven by our aspirations to make better decisions faster through automation by leveraging the unprecedented amounts of data that we can now gather, as well as exploiting our ability to design algorithms and take advantage of increased computing power.

The impact of advances in data science has the ability to touch all aspects of daily life from the so-called 'datafication' of society through to the 'quantified' self. Automated decision making is providing benefits in financial transactions, the delivery of personalised services online, health care prediction and diagnosis, and the development of government services.

However, automated decision making also has the potential to discriminate against individuals leading to the denial of some services. Further, the lack of transparency in algorithm design and implementation can cause distrust and potential social unrest. Advances in data science are not confined to social applications, the exploitation of data is unsurprisingly of interest to defence and security practitioners.

In a public speech at St Andrew's University, the Director of the UK's Secret Intelligence Service, Alex Younger, highlighted the importance of achieving mastery in the data age. He also talked about the changing context where adversaries do not see a clear delineation between war and peace.

The UK's Ministry of Defence has a similar focus on the better use of data and has issued a Joint Concept Note on Information Advantage (JCN 2/18), highlighting the way that adversaries are using advances in technology to achieve '*mass customisation of messaging, narrative and persuasion*' that extends both reach and influence. Actions by adversaries often now take place in the 'grey zone' between war and peace, frequently targeting broader society with the aim of creating uncertainty, ambiguity, doubt and undermining confidence in decision making.

It is clear that defence and security practitioners need to be able to balance taking advantage of data with ensuring that decision making processes are resilient to both attack and to misuse. As Russia expert Keir Giles has pointed out, this means understanding both the content of information processes as well as the code that underpins them.

The need for understanding spans the requirements for an algorithm, the theory that underpins the design, and construction as well as training in how data is used.

In this issue of *CREST Security Review,* we see the value that data and computer science can bring to topics such as computational language analysis for understanding the person behind the text (Ryan Boyd and Paul Kapoor). The article by Joanne Hinds highlights the potential benefits of data for predicting behaviour, while sounding a note of caution around ethical issues.

The article by Pip Thornton continues this theme by pointing to the impact that digital capitalism can have on spreading fake news, while my article on algorithmic decision making highlights the impact that conceptual models that underpin automated decision making can have on the relationship between individuals and the state. Fortunately, there are research institutes set up with the aim of addressing some of these issues. In the UK the **Alan Turing Institute** for data science and AI is well established and has a defence and security research theme within its programme.

The focus of the institute, however, is on the key disciplines of mathematics, engineering and computing. While these are of vital importance for the development of data science, algorithms are ultimately deployed in a real-world context. The aim of the Institute is to 'change the world for the better', but it is incumbent on researchers to critique this statement – who constitutes 'the world' in this instance and 'better' for whom? Fortunately, the recent establishment of the Ada Lovelace Institute (and the close working relationship between the two) provides balance. The **Ada Lovelace Institute** has the aim of ensuring that, 'data and AI work for people and society' and considers the impact of data science on society.

There are many other research initiatives that are at different stages of maturity and which address some of the emerging issues of data and data science. For example, the **Data Justice Lab** recognises that if data is misused it can heighten socio-economic inequalities and has the potential to increase social divisions. The **Not Equal Project** focuses on the socio-technical aspects of new technology considering how it can empower, emancipate and offer opportunities for economic development.

The **Unbias Project** considers ways of improving algorithmic transparency to build trustworthiness in systems. The **People Powered Algorithms for Desirable Social Outcomes** project looks at the design of algorithms and aims to understand how algorithms mediate real world relationships between the state and individuals.

Research questions around data science topics in general and automated decision making more specifically are still emerging in the defence and security space, not least because the focus of data science is on developing automated decision making processes through Artificial Intelligence and Machine Learning (AI/ML), whereas decision making is an inherently human activity. Users of automated decision making tools may feel reluctant to rely on an algorithm so how do we understand how to build trust in algorithms? Is it more acceptable for a human to make a poor decision than it is for a machine? Do we expect more from automated decision making than it can truly deliver at the moment? How do we protect algorithms during the design and development phase to ensure that training data, or the algorithms themselves are not tampered with? How do we ensure that algorithms are designed on robust theoretical principles – that they are actually doing what we want them to do? This issue of *CREST Security Review* starts to explore the topic but it is evident that there is still much that social and behavioural science can contribute to ensuring that the aspirations of data science are met for defence and security practitioners.

Professor Debi Ashenden is the guest editor for this issue of CREST Security Review. *She is Professor of Cyber Security at the University of Portsmouth (UK), Research Professor of Cyber Security and Human Behaviour at Deakin University (Australia) and leads CREST's Protective Security and Risk programme.*