National Intelligence Postdoctoral Grant Research Topics 2021

Contents

Reference Code: NIPG-2021-001

Research Topic Title:

Explainable and Trustworthy Artificial Intelligence

Research Topic Description, including Problem Statement:

Artificial intelligence (AI) capabilities must be adopted if analytical insights into big data are to reach their full potential. A key barrier to adoption appears to be user trust in 'black-box' algorithms, especially under uncertainty and when dealing with high-stakes consequences. A thorough understanding of user trust, interpretability of AI techniques and design methodologies for assistant uptake and trust in these systems is imperative if these technological advantages are to be adopted in order to achieve required analytical outcomes.

The issue of explainable AI remains a major obstacle to the broader application of AI-powered products and services due to issues of transparency and accountability. In addition to public debate around the need for transparency and accountability to be built into AI applications, this issue remains an obstacle for governments developing regulatory frameworks and legislative changes to govern the use of AI technologies. Many engineers and data scientists have questioned whether meaningful explainability, to the degree required, is technically possible, particularly as approaches such a neural networks and deep learning are becoming increasingly ubiquitous and complex.

Example Approaches:

Research proposals could approach this from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of data science, engineering, psychology, human-centred computing, systems and design thinking, software development and UX and UI design, with links into social sciences.

Proposals could consider:

- Explainable AI and approaches for increasing the transparency and reasoning behind more complex deep learning methods.
- Understanding the antecedents to trust and propensities user have to trust new technological capabilities
- Understanding barriers to user trust and how to regain trust once lost
- How the measured consideration of design of systems could influence trust and how system features may be manipulated to mitigate loss of trust
- How human-machine interfaces can be better designed to enable a symbiotic working relationship between the human and computer

Relevance to the Intelligence Community:

As data volumes and complexities increase and become more difficult to analyse manually, AI capabilities will need to be adopted in order to produce critical results in any meaningful timeframe. It is imperative that the IC understand user trust in new technological capabilities and designs AI systems accordingly in order to facilitate trust amongst end-users, and ensure systems can recover when perceived trust is lost.

Deep learning and neural networks are built into the core of many applications and capabilities of high interest and worth to intelligence services. The ‘black box’ problem remains perhaps the best known issue commonly discussed in public discourse about AI and machine learning. The issues raise concerns around the ethics and accountability of AI applications, particularly where applied to counter security threats and challenges. Improving the explainability of neural networks would assist developers to refine and improve neural networks applications. Additionally, improvements in the accountability of AI solutions would support public trust in AI, particularly within government AI capabilities and solutions.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Australian Government
Office of National Intelligence | oni

National Intelligence Postdoctoral Grant

Reference Code: NIPG-2021-002

Research Topic Title:

Forecasting climate impacts upon agriculture, water supply and public health in South East Asia and the Pacific

Research Topic Description, including Problem Statement:

Impacts of climate change on Pacific Island nations and South East Asian nations may be estimated by joining global and regional climate models with models of local horticultural, agricultural, fishing, water supply and public health (disease and disease vectors) which factor in climate inputs. As climate models improves and the sophistication food, fibre, water and public health models improve, the resolution and accuracy of these combined forecasts will improve. The challenge is to develop methodologies to join currently disparate models which will render forecasts of impacts that are sufficiently robust to inform policy makers.

Example Approaches:

One approach would be to identify the characteristics (frequency, modality and plug-in-ability) of all relevant models, and scope potential interoperable solutions. The scale difference between small-island state horticulture models and global climate models presents distinct compatibility challenges. Models of disease with respect to populations, pollination and livestock similarly present distinct interoperability challenges. Another approach may be to develop models or connections to enable joint operation of existing models of different scales and types. A third option may be to devise methodologies to inform the cooperative, inter-operative development of global / regional climate models and models of food, water and public health of Pacific nations.

Relevance to the Intelligence Community:

Improved understanding of near-term, medium-term and long-term physical impacts upon populations and economies in the Pacific and South East Asian nations will inform regional security assessments and provide a stronger basis upon which to estimate trends.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-003

Research Topic Title:

To Find a Needle in Haystack, Build a Needle-stack: A Novel Technique to Tackle Large-scale Class-imbalance

Research Topic Description, including Problem Statement:
There is a vast amount of literature around imbalanced learning. Solving imbalanced learning problems is critical in numerous data-intensive networked systems, including surveillance, security, cyber, finance, biomedical, defense, and more. Some recommendations to tackle the class-imbalance problem are collecting more labeled data, changing performance metric, resampling of data, generating synthetic samples, trying various classification algorithms and penalizing the models for mistakes on minority classes. Almost all of these solutions utilize an element of randomization which leads to different detection outcomes from a single classification algorithm. This research aims at embedding supervised learning practice in preprocessing to build a deterministic data resampling for the benefit of underlying anomaly detection methods. It is like building a stack of hay-aware needles alongside the existing haystack to hugely increase the chance of picking the lost needle.

Example Approaches:
Undersampling mainly involves random selection of majority samples to balance them with the minority ones. In contrast, oversampling mostly generates random samples considering the statistics in minority samples to balance them with the majority ones. This research intends to employ majority statistics plus minority guidelines to train a novel supervised resampling model ahead of conventional classification or anomaly detection phase in the pipeline. The core idea is that generating augmented minority samples should minimize inter-class variance while maximizing intra-class discrepancy (Fisher Discrimination). Roughly speaking, synthetic samples should mimic both minority and majority patterns to build a high-quality deterministic class-balanced data fed to the classification/detection phase.

Relevance to the Intelligence Community:
Intelligence agencies frequently deal with ‘incomplete’ datasets with few identified targets. Efforts to resolve the imbalanced learning problem may help agencies improve the accuracy of their analytic approaches to identify ‘unknown known’ targets within collected datasets despite the challenges of incomplete data. Real-world intelligence practice deals with few hostile anomalies compared to the large number of legitimate actions. Detection of these anomalies is of critical due to the possible damage that they can impose to the national interests and community well-beings. Due to infinitesimal ratio of anomalies to normal behaviors i.e. passengers importing illicit goods vs all other travelers, machine learning techniques usually suffer from class-imbalance syndrome and cannot produce viable detections. This research will address this shortcoming by applying supervised learning to build context-aware class-balanced training data for maximizing detection performance to find needles in haystack.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-004

Research Topic Title:

Information Security Classification of Disparate Data: Artificial Intelligence/Machine Learning

Research Topic Description, including Problem Statement:

Data, and the insights analysts obtain from it, are crucial for IC agencies to perform their mission. The volume and variety of data are increasing, and they are interconnected so that insights are obtained from the combination of data from many sources. Data classification is traditionally based on the content of the data, although context and metadata may also have an impact on its sensitivity. Typically classification of the data is based on the potential impact on the national interest, organizations or individuals if the data is compromised. Classifications range from no business impact for unclassified data to catastrophic impact for top secret data. In some cases appropriate classification of data is straightforward since either the nature of the data or the way in which it was collected clearly indicate its level of sensitivity. Increasingly, organizations in the IC are drawing on a variety of data derived from unclassified or low classification sources. In this case, the level of sensitivity of the derived data is not clear, particularly when it is comprised of a range of data-types including structured, unstructured and multimedia data.

The classification level of data has substantial implications for its ability to be shared and analyzed or combined with data from other sources, which can limit its usefulness and the ability of IC agencies to partner with other agencies, industry or academia. At present the risk-based guidelines do not provide clear guidelines as to the sensitivity of derived collections of disparate data. Hence the goal of this project is to use mathematical and statistical principles to establish a framework for classifying disparate collections of security relevant data based on its importance, value or sensitivity, taking into consideration the need to maximize the availability and hence usefulness of the data.

Example Approaches:

Graph networks are widely used for social network analysis. When applied to entities extracted from text-based data (for example) they can help to quantify the amount of information within a given dataset, providing guidelines for the scope of potential damage if different types or quantities of data are compromised. There are already many publically available datasets than can be used to test these methods and develop principles for the potential impact of a data breach. An important aspect of this work will be to identify the type and extent of damage and to relate that back to statistical properties and characteristics of the data.

Machine learning (ML) and artificial intelligence (AI) can be used to classify the content of data collection into relevant groupings and to identify outliers and anomalies. These methods show substantial promise for analyzing aggregated datasets of disparate data to find sensitive information they may contain. Applying these methods to disparate collections of data will help quantify the level of risk associated with these collections and hence inform the appropriate classification of the data.

Historic data breaches and unauthorized disclosures provide an opportunity to evaluate the amount of damage that can be attributed to a given volume and type of data. Methods for evaluating identification of sensitive information stemming for privacy research, as well as methods outlined above, can be allied to these datasets to quantify the probability and extent of compromise for a given dataset (which may depend on the type, volume and nature of the data), providing empirical indicators of damage.

An alternative approach could be to consider the potential level of compromise if sensitive attributes were made available at a low classification (for example if shared between agencies or made available to industry partners) with or without context and in either an open or encrypted form as a reference for AI or ML analysis, or for context based searching.

Relevance to the Intelligence Community:

This is an escalating problem for IC agencies as there is an increasing need to partner across agencies, and with industry and academia. Higher classification of data restricts its availability, usefulness and hence its value. Moreover, the classification of data has an impact on its use for IOT applications, edge technologies and AI. Having a well-defined set of objective principles for classifying disparate collections of security-relevant data would assist in balancing the risks associated with sharing data against the benefits of sharing the data.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-005

Research Topic Title:

Cyber influence on behaviour change: Prevalence, Predictors, Progress and Prevention

Research Topic Description, including Problem Statement:

The aim of this project is to understand and forecast the impact of cyberspace on changes in human behaviour which has implications for social and political outcomes. Social cyber security has been identified as a key area where social behavioural science (SBS) can exchange knowledge and contribute to issues and challenges for the Intelligence Community. How cyber may mediate behavior change and the boundary conditions to such influence ('when and for whom') are core research areas for the SBS. There are recently developed models of social influence that draw, in particular, on group-level identity processes tied to common interests, belonging and shared norms. A key step forward would be to investigate the applicability of these models to cyber and their implications for actual behaviour change in the 'real-world'. Key questions are whether 1) existing models of social influence translate straightforwardly to the cyber environment and if not, how to redefine them accordingly and 2) cyber influence does have a direct relationship to behaviour and when this is most likely to occur. This research area is of broad scope and interest with potential to form a much larger research enterprise.

Example Approaches:

Proposals could consider the following approaches or perspectives:

- Investigate the personal and social characteristics of users (strengths and vulnerabilities) that are most and least likely to be cyber influenced.
- Identify and demonstrate through experimental studies key factors that facilitate and disrupt cyber influence on users' behaviour.
- Understand the factors that escalate the success of cyber influence to widespread behavior
- Explore methods that can prepare and inoculate users to cyber influence tactics and assess their success.
- Examine the underlying personal and social motivations that underpin certain areas of cyber influence including extremism and promoting actions that present security threats.

Relevance to the Intelligence Community:

Much human activity is occurring in cyber space. Developing better models of cyber influence will aid the Intelligence Community in being able to understand, track and predict events.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-006

Research Topic Title:

Digital Cities/Countries for Intelligence and investigative purposes

Research Topic Description, including Problem Statement:

A digital twin is a virtual recreation of any systems. With the future rollout of Smart Cities this presents the opportunity for incredibly detailed mapping of an entire town/City function. This includes electrical systems to traffic flows, to pedestrian footfall. Visual mapping will likely become prevalent with the cameras and sensors on autonomous and connected vehicles. A National Digital Twin has already been proposed by Cambridge University's Centre for Digital Britain. Digital Twins of cities already exist, notably in China. Such detailed mapping will be powered by IoT and 5G.

It seems highly likely that creating digital twins of cities and even the entire country, would allow for extremely accurate mapping and modelling of events in real time, drawing in data from a range of open source and classified material to support investigative requirements that are necessary and proportionate. The combination with AI would allow for the efficient deployment of officers to likely hotspots, identify high risk areas and also the testing of variables to understand and predict reactions within a city to events, whether natural or otherwise.

Example Approaches:

Creation of a digital twin as a case study for law enforcement and/or intelligence purposes, incorporating the relevant information and data streams. This would also require mapping of what data is available and timely. An Agile approach would likely work best, small sprints producing results that layer on one another. E.g. Twin a street, that a university campus, then a borough etc. Incorporation of behavioral analysis and relevant AI. For example, predicative aftershock analysis (earthquakes) has been trailed by police to predict future crime hot spots. Such a volume of data could be exploited by adversaries.

Such a project will require a collaborative approach as it incorporates very technical data but would also need detailed behavioral analysis drawing from a range of open source and government data.

Relevance to the Intelligence Community:

Such technology would also be extremely useful in a national security context. Mapping behaviour patterns would allow for the early detection of anomalies from the city/country/locations baseline. This could be the early signs of just a burst water main, or of subthreshold hostile state activity such as probing of CNI, economic pressure ratcheting up of societal stresses through to supporting in the detection of serious and organised crime. If such Twins could be created easily, the could also be applied overseas for modelling of other cities and countries, allowing for better decision making around foreign policy.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-007

Research Topic Title:

Satellite IoT communications

Research Topic Description, including Problem Statement:

The Internet of Things (IoT) has now reached space, and start-up companies such as Lacuna are hoping to roll out a service using modified LoRaWan that will allow users to transmit data to a satellite from low power remote devices in locations that lack terrestrial infrastructure. Applications amongst others include asset tracking (including vehicles, aircraft and vessels), wildlife conservation, climate change monitoring, situation awareness for disaster relief, policing and border control.

The concept of worldwide universal IoT connectivity from remote locations normally not serviced by terrestrial networks is potentially a game changer for so many applications however this scheme will only offer one-way communication from the ground to the spacecraft and the initiative is predicated on a modified stack/silicon so the IoT devices must be specific to space transmission. This research topic aims to explore the theory, practicality and limits of operating native IoT communications waveforms for bi-directional IoT communications to and from a low earth orbit satellite. This focus on groundbased technologies for satellite IoT will investigate radio waveforms and protocol designs, maximising exploitation of entropy sources for secure cryptographic communications, and constraints from necessary power saving/harvesting and 'wake-up' designs. Optimisation is for power efficiency and endurance, and effective exploitation of channels with very low link budgets. Low gain antennas with limited efficiency can be assumed to be a real-world constraint of any practical system.

Example Approaches:

As an example of possible inclusion in the research, ultra-narrowband as typified by SIGFOX devices use a very low power transmitted waveform which coupled with digital processing gain techniques are achieving communications over many tens of kilometres in terrestrial applications. The questions the research would be addressing is could such a waveform be used in a space application? What are the limits to its use given the constraints of link budgets through the atmosphere and the effects of doppler.

Relevance to the Intelligence Community:

We are interested in remote sensing and actuation in a number of security applications requiring remote command and control.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-008

Research Topic Title:

Optimal and Autonomous Control of Satellite Formations

Research Topic Description, including Problem Statement:

Satellite formation flying offers two significant benefits: 1) graceful degradation: if one satellite in the formation fails, the remaining satellites may be able to continue collecting mission data, and 2) potential performance increases: distributed aperture sensing technology theoretically provides transformational improvements. However, in order to realize these benefits, one must be able to maintain the formation in the presence of dynamic perturbations. Classical control approaches involve targeting desired orbital elements or relative orbital elements, but these approaches assume that one knows what the desired elements are. If the orbital dynamics were perfectly known, this would not be an issue. However, there are still uncertainties in the gravity field and atmosphere, and more importantly, minor differences in satellite makeup and orientation; combined, these uncertainties introduce inefficiencies into formation control. Furthermore, if one satellite is lost from the formation, how does the formation optimally reconfigure itself? It is hypothesized that a better approach to achieving and maintaining satellite formations can be found. The goal of this research project is to review the state-of-the-art literature and explore methods to improve satellite formation control in the presence of dynamic model errors.

Example Approaches:

Instead of viewing formations in terms of orbital elements or element differences, one could cast the problem in terms of controlling relative orbital element rate differences. For example, if two satellites were flying in the same orbital plane separated by several degrees of mean anomaly, one would expect small perturbations, due to longitude-dependent gravity and drag effects, to slowly impact the mean anomaly difference. One could execute small maneuvers to maintain the target mean anomaly difference each time the separation distance changes beyond a tolerance value. Alternatively, one could change the reference semimajor axis by a small amount to offset the unmodeled dynamic perturbation. This second approach would require far fewer maneuvers. Less elegantly, one could also approach the problem from a machine-learning point of view.

Relevance to the Intelligence Community:

Satellite formation flying offers increased resilience and potentially improved intelligence, surveillance, and reconnaissance (ISR) data collection capabilities.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.

Reference Code: NIPG-2021-009

Research Topic Title:

Development of Methods to Identify, Detect, and Describe Synthetically Derived Biological Systems

Research Topic Description, including Problem Statement:

Synthetic biology offers innovative approaches for engineering new biological systems or redesigning existing systems for useful purposes. It has been described as a disruptive technology capable of delivering new solutions to global healthcare, agriculture, manufacturing, and environmental challenges. There are, however, concerns that synthetic biology may also expand the pool of agents of concern, creating a need to develop detection, identification and monitoring systems, and to proactively build countermeasures against these new or redesigned threats. Many labs can now design and construct relatively complex gene networks capable of producing a wide variety of designer molecules in a range of host cells. The application of artificial intelligence/machine learning promises to further reduce the time and cost of such processes in the future.

Example Approaches:

Synthetic biology is driving significant change in biomedicine including the development of chimeric antigen receptor (CAR) technology, which engineers immune cells of patients to recognize and attack cancer cells. Genetically engineered viruses are being used to correct defective genes in individual patients and could be extended to target populations. Work on vectors capable of carrying larger genetic loads is helping to produce more efficient therapeutics and vaccines. Optimization of antibodies that are in an editable format will further reduce cost and time. The Human Genome Project-Write has set its sights on building entire human chromosomes. Work in whole cell and cell-free systems can be used to develop sensors of multiple specific biomarkers, which would assist in earlier detection of diseases. Synthetic biology offers the opportunity to create responsive multifunctional materials by integrating biochemical components from living organisms with inorganic components; such materials would be able to sense their environment. Cell-free environments offer a powerful route for flexible and controllable production systems. Using nanoparticles made of semiconductor materials or quantum dots can be used to enhance enzymatic activity in cell-free environments. Multistep enzymatic pathways can be tethered to nanoparticles to increase reaction rates several hundredfold. This dual use technology offers great benefits but could also be used to cause harm.

Relevance to the Intelligence Community:

Synthetic biology is a disruptive technology that could be used to cause (either intentional or inadvertent) harm to humans or the environment. The ability to engineer viruses to be more effective vectors of genetic information may also lead to the creation of even more deadly pathogens by those intent on harm. The technological advances in molecular biology with an ever-decreasing barrier to entry in the same field could pose an existential risk to everyone involved and would directly impact national security. Efforts to find solutions for identification, detection, and interpretation for synthetic biological problems is a critically relevant and immediate need.

If you have questions, send an email to NIPG@oni.gov.au. Please include the reference code for this opportunity in your email.