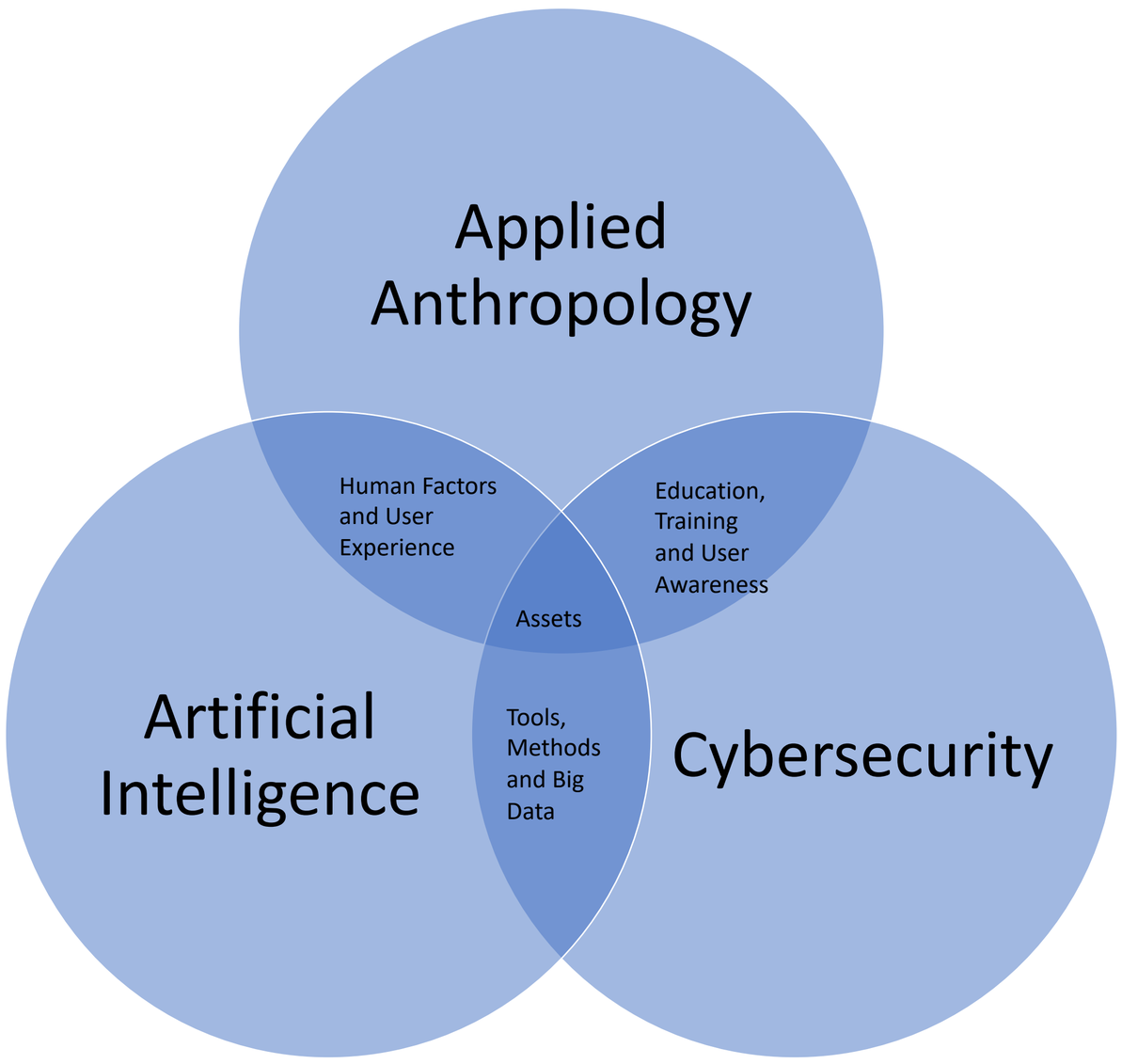
The Triumvirate of Protection

Author: Alex Cadzow

Cadzow Communications Consulting Ltd (C3L) alex@cadzow.com

Abstract: **This poster will aim to show how the area of Cybersecurity, Artificial Intelligence (AI) and Applied Anthropology (A.A) complement each other in the goals of protecting systems, data and users. The reasons these three areas can work together because cybersecurity is a field with the goal of protecting assets. It does this by making use of tools and actions. This means it is able to accept new means that improve those tools and action. AI is able to bring the means to better protect and identify threats from big data collections and a large number of devices from IoT to server farms. While A.A offers means to study people/users within organisations, their customers and threat actors in order to understand how they are using the tools at their disposal to either protect themselves or carry out attacks thus allowing the means of protection to be improved.**



Introduction:

Applied anthropology refers to the application of the method and theory of anthropology to the analysis and solution of practical problems. When applied to the discipline of cybersecurity the methods of data collecting that are used in anthropology with the aim to help solve problems with the field of study. The primary methods used in applied anthropology are work shadowing, contextual interviews and semi-structured interviews. These can also be supported by literature reviews and surveys of relevant groups of people. These are done to gather qualitative and quantitative data in order for the anthropologist to provide recommendations or guidelines. Applying anthropology to the field of AI may seem like a strange choice since anthropology largely is about people and human behaviour while AI is a complex piece of technology. But there are key areas in the field of AI where the anthropologist can play a useful and supportive role.

The First Triumvirate

A.A and AI:

The definition of AI is the capability of devices or mechanisms and machinery to perform functions usually associated with human intelligence, including scientific systems, reasoning, optimization through experience, and automated motor systems. The why, what and how anthropology can be used in the field of AI include understanding of the mechanisms underlying thought and intelligent behaviour and their embodiment in machines, and can aid in increasing public understanding of artificial intelligence, improve the teaching and training of AI practitioners, and provide guidance for research planners and funders concerning the importance and potential of current AI developments and future directions. [1]

Studying the application allows for a better understand how society interacts with technical aspects of AI. An anthropologist has the potential to play a role within the field of AI in developing how it is applied to real-world applications beyond technology labs. An anthropologists role is to ask the key questions and find the answers, such as how do you make what is technically possible but also what people wanted? They also need to look at new technology, how they work, what people do and do not do with them. [2] This will become vital when cyber-physical systems become the norm.

A.A to AI can be linked back to ethnographic research. In the 20th Century, anthropologists would be employed to aid companies in understanding how their customer used products or in the interactions within a company. [3] Therefore anthropologists working on AI in the 21st Century can be considered a natural progression of applying the skills sets of one field and using them in another. This is possible because it is the same concept, watching, learning how people are working and what kinds of patterns they are following.

End-goal of A.A to the field of AI is to achieve a better understanding of how the tools and systems of AI are used by people and how they are used for key roles. [4] [5] In order to lead to a better Human-System interactions for companies and users.

AI and Cybersecurity:

Cybersecurity designers have turned to AI and Machine Learning (ML) to provide insights that would otherwise be impossible for humans to achieve alone. Once set-up, trained and monitored, solutions that detect threats using AI/ML can reduce the time from breach to discovery, reducing the amount of damage an attacker can cause. [9] Shortening the time to discovery is critical for security

Though for AI to be used effectively in cybersecurity there are key factors that need to be taken into account. [10][11]

Contextual Data is King – Cybersecurity challenges are broadly design and data problems, rather than machine learning problems. The nature of constantly evolving cyber threats dramatically increases the need for real-time intelligence flow to power ML algorithms, as it becomes harder to detect the signal among the noise of massive data sets, solutions require that these data sets be labelled to train ML algorithms.

Variation is Native to Security – In a landscape of rapidly evolving threats, trying to detect and defend against a moving target is difficult with no predictable progression of threats.

Decisions Require the Right Data Set – Data in isolation yields limited benefits and may require context.

Data Requirements Collide with Privacy Concerns – The best behaviour/anomaly detection needs to leverage data across multiple systems, both within the environment and outside of it. However this ideal "360" data collection erodes individuals' data privacy. In policy and regulatory environment attuned to privacy concerns, it's expected to see companies leveraging the power of ML to analyse data "at the point at the site", without retaining data.

A.A and Cybersecurity:

The categories of cybersecurity that A.A can be applied to include: Human Factors – training, culture and communication. [6][7]

Organizational factors – risk management, open environment and academic freedom, lack of budget, security as a secondary priority, tight schedules, access control to sensitive data, size of the organisation, managerial support.

Technology – complexity of the systems; vulnerabilities in systems and applications; mobile and distributed access, efficiency of security tools.

Anthropologists aim to understand the areas of cybersecurity between users and the tools they make use of. [8] The end-goal of anthropologists is to improve cybersecurity within organisations.

Conclusion:

This poster aimed to show as how different the different methods of protecting assets can be used together to offer means and a level of protection that wouldn't be achieved by cybersecurity on its' own. While cybersecurity can stand alone as field there is a danger that it will stagnate or become set in its' ways if it fails to embrace new ideas and methods. This is where AI and AA can be used to ensure this doesn't happens. AI can be applied to analytical tools and data. While AA can be applied behaviour, education and training. They complement each other thus overall cybersecurity as field would be able to offer expanded means and a higher level of protection by working with other fields.

BRAHMA VISHNU SHIVA

Bibliography:

1. https://cybersecuritysummit.co.uk/cyber-insider/digging-cyber-security-talk-chris-rivinus-tullow-oil/
2. http://www.cyber-anthro.com/2014/01/cyber-extortion/
3. http://people.cs.ksu.edu/~sathya/anthro_reading.html
4. https://www.applied-anthropology.com/
5. https://uwaterloo.ca/alumni/blog/post/artificial-intelligence-and-anthropologist
6. http://anthropology.iresearchnet.com/artificial-intelligence/
7. https://www.cio.co.nz/article/646447/anthropologist-asking-critical-questions-around-ai/
8. https://www.cio.co.nz/article/466330/Cio_next_hire_digital_anthropologist/
9. https://www.aiaa.org/Pages-from-Migration/Cybersecurity/Artificial-Intelligence-for-Cybersecurity
10. https://benhamouglobalventures.com/2018/03/27/applying-ai-cybersecurity-separating-hype-reality-part-1/
11. https://benhamouglobalventures.com/2018/03/29/applying-ai-cybersecurity-separating-hype-reality-part-2/