CASIS - VANCOUVER - ACERS

SAPERE AUDE

DOES INFORMATION MAKE US SAFER OR MORE SECURE?

Date: October 19, 2023

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On October 19th, 2023, Dr. Patrick Neal, Chief Social Scientist at AQ-IQ, presented *Does Information Make Us Safer or More Secure?* The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were data protection responsibilities and obligations, and management of excessive data for future-proofing projects and security.

NATURE OF DISCUSSION

Dr. Neal provided a critical look at the use and impact of information in private and public spaces, focusing on how information could be used to weaken our cybersecurity posture. Given the increasing power of information, he queried whether privacy, in its current state, required a reevaluation and if leveraging and orienting information for our own purposes could ever make us safer or simply more vulnerable to manipulation and attack. Dr. Neal affirmed that information does not provide agency in the ways we have presented it, nor does it enhance security.

BACKGROUND

Dr. Neal began his presentation by outlining the growing significance of informational security through a record of recent events; ultimately using past themes to state that despite the power that information wields, it does not provide its holder with agency nor safety & security. For instance, having access to vast amounts of data can ironically make information holders more vulnerable to obsession and paranoia brought on by a cult of fear surrounding cyber-attacks. In addition, agency can still be constrained in the purview of controlling big data, as agents are not empowered enough to fulfill their potential. The issue of agentic potential intersects with themes of posthumanism and transhumanism which are significant to the boundaries of informational power. In the case of posthumanism, the rejection of biological, ethical, and ontological dimensions that are judged from a humanist, value-laden point of view can expand the capacity for agentic potential; whereas, transhumanism can emphasize technical improvements over time which can similarly expand the magnitude and capacity for agency, as well as the future of security.

Dr. Neal then went on to provide a thematic deconstruction of information, breaking it down to a set of rules involving knowledge, sequencing attribution, signals and messages, and measurements of these signals and messages. The element of knowledge includes various categories such as intelligence gathering that are meant to change one's perspective on some issue. Regarding attribution, the attribution of sequencing involves a particular order in which information is delivered; it does not occur randomly. However, attribution does not begin until there is a convergence of signals and messaging. When this occurs, one must be prepared to respond back to the messages. Once this step occurs, any outgoing responses involving signals and messages are measured by outside parties to determine if they are right or wrong.

Next, Dr. Neal attempted to sum up his presentation's takeaways through the acronym ECHO. The first letter relates to embracing technological advancements which will occur no matter what. This realization should be equally followed by the realizations that ethical frameworks are currently unable to keep pace with technological advancements, and that safety and security are foregone concepts simply because of the facts that external actors are mainly holding the information now. The next part revolves around counting on the likelihood of surprises occurring through small signals which will definitely be missed (ie. Gray Goo scenario) versus big signals that may, ironically, be missed as well. The letter 'H' refers to hopelessness, encompassing notions such as evolution and its entrenched position in modern civilization, as well as fear mongering attitudes around concepts of safety and security. Additionally, hopelessness can also refer to having a zero-risk bias towards ethical studies and technological research, as well as an avoidance of conversations that involve anticipating cyber risks. Finally 'O' refers to how optimism is ultimately a choice, one that must be supported by keen insight, observance of the risk, and an opportunity to contribute.

Finally, Dr. Neal concluded his presentation with a list of recommendations for prioritizing and improving agency and cyber deterrence. Agency is embedded at three levels: organization, decision maker, and the contract-level. Compared to decision maker obligations and contracts, organizations typically have more options at their disposal for averting attacks. Dr. Neal queried how decision-making agencies could utilize informational assets to create change and protect society. The answer is by legislation such as Bill C-51. When combined with other resources and considerations, agency can be significantly enhanced, allowing the decision maker to have considerable freedom to maneuver themselves towards a favorable position in cyber deterrence.

Question and Answer

Our information is vulnerable. There should be lawsuits for this level of negligence. Why can't we sue Microsoft for privacy infringements?

As technology increases, how can we ensure that ethics are upheld for for-profit organizations? At some point it will be the individual's responsibility to control their own data. Self-autonomy will only begin when an individual self-reflects and asks themselves whether they are owned by someone else or not.

Where do we draw the line with too much information? Is there a tipping point?

There is a tipping point, (e.g., 9/11). They had the data but didn't know what to do with it. We continue to look for the best bargain, and we are starting to understand the anxiety that comes with too much information. General Issa Arthur talks about the future through current science. We are building hive cities and underwater tunnels; the question is, do our brains have enough resilience to exist under those conditions? What will we do with all this information? Any future undertakings that will involve big data will need to be followed by a parallel commitment to improve our brain's resiliency to excessive overloads of data, in order to ensure successful facilitation of such projects.

Considering the rapid spread of disinformation, how can we control this?

The rapid spread of Gaza conflict-related disinformation over X is a definite example of devolution. Purveyors of such information should be held criminally responsible. At the end of the day, everyone is detectable. The public must be fully aware of how vulnerable they are to risk from such information as well.

KEY POINTS OF DISCUSSION

- Security is defined as being free from danger or threat. Safety is defined as the condition of being protected from or unlikely to cause danger, risk, or injury. The cult of fear is defined as an obsession with living in a risk-free society, with the ideological belief that "threat is everywhere".
- We must ask ourselves how safe we are in a community that is essentially a hive. What happens to our relationships? For example, the worker vs. the capitalist vs. the socialist. We must place increased emphasis on how we are going to get to the future rather than posit what it looks like.
- ECHO: E – Embracing technology; C – Counting on surprises; H – Hopelessness; and O – Optimism being a choice.
- We need to examine the commodification of security, information, and safety. Do we truly have agency?

FURTHER READING

Plecas, D., McCormick, A. V., Levine, J., Neal, P., & Cohen, I. M. (2011). Evidence-based solution to information sharing between law enforcement agencies. *Policing: An International Journal of Police Strategies & Management*, *34*(1), 120–134. https://doi.org/10.1108/13639511111106641

Neal, P. (2023). Information Through the Lens of Safety and Security. *The Journal of Intelligence, Conflict, and Warfare*, *6*(1), 64–67. https://doi.org/10.21810/jicw.v6i1.5407

Neal, P. (2021). The Dark Age of Online Civil Society: (AKA: A war of 1). *The Journal of Intelligence, Conflict, and Warfare*, *2*(3), 10–14. https://doi.org/10.21810/jicw.v2i3.1184

This work is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International License.

© (PATRICK NEAL, 2023)

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/