Key Events

On January 17th, 2019, the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its eleventh roundtable meeting which covered "The Cyber Kinetic Singularity Affecting National Security." The following presentation was hosted by Dr. Patrick Neal, the lead researcher for CASIS Vancouver's cybersecurity team. As well, he has published research articles on vehicle arson patterns, police uniform standards, information sharing between federal agencies, and more. In his presentation, Dr. Neal was determined to tell a story to better connect with the audience with the complexities of cyber kinetic singularities. Using *War of the Worlds* written in 1898, parallels are made to the dangers of rapidly advancing technology to areas where humans have yet to fully grasp the consequences.

Nature of Discussion

Presentation

The presentation first began with presenting the audience different examples in which technology has pushed past a point where we cannot fully understand the consequences that come with new inventions. Moreover, the presentation continued to cover different definitions within the realm of cyber kinetic singularity, finishing off with discussing the ethical framework present.

Roundtable

The roundtable discussion focused on both the security of physical structures from malware programs such as *Stuxnet.* Dr. Neal used the Alberta oil fields as an example of a prime physical structure that could be vulnerable to such malware. The conversation then shifted towards protecting Canadian democratic integrity against foreign interference, which could likely be cyber interference to some degree.

Background

Presentation

Dr. Neal presents starts off his presentation with discussing how currently, scientists have found a way to neuro-map a mouse's brain in which they could become a cannibalistic. The idea of presenting this was to showcase that much of what humans thought would be unachievable has become realistic, faster than many presumed. This advancement has caused not only ethical debates about some of the ways technology has purposed our society; but also showcases the national security threats that come with rapidly advancing technology and slow policy implementation. Moving forward, Dr. Neal then presents that there are three main types of singularity known which are: mathematical, natural sciences, and technological. However, it will just be technological singularity that will be focused on.

Technological singularity is the idea that any automated system can potentially operate without human interaction. The idea of technology becoming smarter than humans is not new, Dr. Neal discusses how even in 1843 people were thinking that objects will become smarter than humans. However, the level of intelligence these computers have taken is beyond to what any human could arguably truly understand. Examples such as the *Facebook Robot* or *Newman Bots* have been known to not only look after of itself, but also take care of itself as well. However, these are prime examples in which technological singularity has

challenged national security. The Newman Bot famously turned itself on, in which Dr. Neal compares that to a baby becoming self-aware. This could have massive implications as it mirrors human memory, meaning that it could learn things that countries may not want it to particularly learn. Dr. Neal finishes his presentation off with a discussion of kinetics and the ethics of artificial intelligence.

Dr. Neal discusses how the word kinetics is a funny word, as it is a euphemism for the army. However, the idea of kinetics is changing as the way warfare is handled has shifted. As such, Dr. Neal also discusses how the nature of information has changed which has posed a threat to national security. Information has become extremely short lived, which furthers the complexities with protecting nations against any sort of kinetic threat. Lastly, Dr. Neal discusses the ethics of technological singularity by asking if we as humans have gone too far? It is important to note the ethical framework because since there is arguably limited legislation around singularity, there should be some moral code.

Roundtable

During the roundtable, two important ideas were brought to light. First, with malware programs out like Stuxnet, how should governments and businesses protect themselves against such? The second idea brought to attention was the possibility that the next Canadian election will have interference to what was seen during the 2016 American election. To discuss the first of two, Stuxnet has been a malware program known for attacking infrastructures that produce important commodities to governments such as oil or missiles. To exemplify, Dr. Neal discusses how intricate the oil fields are out in Alberta, if they were to be comprised, due to the properties of Stuxnet, it could potentially compromise the entire system. This demonstrates how governments and businesses are potentially ill-prepared should an event happen as such on a national level.

The second part of the roundtable had a focused on how since technology has rapidly advanced to the point where we cannot fully defend against it, how can Canadians be protected against interference during the next election. Dr. Neal discusses how Russia has possibly tried tapping into our electoral networks before and could possibly try again. The biggest solution that was posed however during the presentation is to have a well-informed public. The better informed the public is, the higher chance that Canadians will be able to detect interference better. Another solution that was also posed is to have cyber-structures. Therefore, having layers of laws that protect Canadians and better equip them against cyberattacks.

Key Points of Discussion and West Coast Perspectives Presentation

- Three main types of singularity are known to exist which are: mathematical, natural sciences, and technologic. Technological singularity is the idea that any automated system can potentially operate without human interaction.

- The notion that technology will outsmart humans is nothing new in terms of theory. However, it is only recently where such technology has factually surpassed human intelligence.

- Physical structures are just vulnerable to malware attacks such as Stuxnet. This connects the possibility of kinetic and cyberwarfare being carried out in the same attack.

- Policy has always been implemented slower than technology has been produced, this creates vulnerabilities in the public domain when attempting to regulate usage and application.

Roundtable

- One of Canada's current upcoming threats is arguably foreign interference with the next general election.

SFU LIBRARY DIGITAL PUBLISHING

- Malware programs such as Stuxnet should be viewed as a weapon no different than a gun or missile.

- Regulating these technologies without interfering with privacy rights will arguably be an upcoming challenge for policymakers.

- So much software has been engrained into the public domain via social media apps that when these norms are challenged, it can cause public unrest.

SFU LIBRARY DIGITAL PUBLISHING