CASIS - VANCOUVER - ACERS

SAPERE AUDE

SECURITY AND CYBER INTELLIGENCE: WHERE IS THE LINE?

Date: May 19, 2022

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 May 19, 2022, the Canadian Association for Security and Intelligence Studies (CASIS)-Vancouver hosted a Digital Roundtable titled *Security and Cyber Intelligence: Where is the Line?* conducted by Mubin Shaikh, a counter extremist specialist at Parents for Peace and a Professor for Public Safety at Seneca College. The presentation was followed by a question-and-answer period with questions from the audience and CASIS-Vancouver executives. The main discussion topics centered around the evolving means to perform intelligence and security operations, transforming cyber biology elements, and the elusive vulnerability of the average person as it relates to these security challenges.

NATURE OF DISCUSSION

Presentation

Mubin Shaikh discussed the growing involvement of non-state actors in cyber intelligence operations. These operations are becoming pervasive in the public space and are rapidly transforming security and cyber intelligence functions, introducing more opportunities for nefarious actors to exploit and target vulnerable individuals.

Question & Answer Period

Emerging cyber space and capabilities such as the Metaverse renders the space increasingly versatile and vulnerable to extremist and criminal exploitation, and the abuse of the principle of freedom of speech. Since social media corporations are profit-driven, moral accountability becomes marred over the market demand for social media activity. Mr. Shaikh highlighted the growing need for civic empowerment through education that could build public resilience against these challenges.

BACKGROUND

Presentation

Mubin Shaikh began by exploring the traditional notions of security and intelligence, such as obtaining information while physically and covertly breaking into places, and how with the advent of technology, these modes have been transferred over to cyberspace. These changes lend more flexibility and autonomy for the security and intelligence operations to be executed anywhere, anytime.

However, Mr. Shaikh argued that these kinds of operations are now carried out by non-state actors; for instance, the Elderwood group targets human rights groups in China that denounce the government or show potential to promote human rights activism. On the other hand, some examples of state-versus-state adversaries include the network Crack Program Hacker Group (NCHP) from China, which collects military intelligence that may infiltrate Canadian political institutions and affect policy. These examples demonstrate the increasingly varied types of intelligence collection and the means used in the contemporary security space.

Mr. Shaikh stated that while counterintelligence has previously been largely understood as a state-based arrangement, there is now ample opportunity for non-state actors to be developing their own counter-intelligence programming. For example, online ISIS magazines have been targeted and through broken URLs, many individuals have been compromised; specific bomb-making ingredients and measurements posted online by ISIS were also compromised, which disrupted their bomb-making process and jeopardized their safety. As a result, there have been attempts by ISIS cyber activists to train their people on how to prevent being targeted.

Mr. Shaikh emphasized that the average person is getting caught up in the middle of this increasingly complex interplay of state and non-state actor involvement. For instance, the public has already encountered numerous attempts to steal personal and financial information, and it will most likely increase in frequency and volume as tools for cyber intelligence become increasingly available for both state and non-state actors. In particular, when global conflicts such as the Russia-Ukraine war emerge, there will be a surge in cyber activity in a wide variety of forms, targeting military, non-state groups, and individuals, such as researchers and policy makers. These attacks will be direct or indirect and will make the civil society space more vulnerable as technology continues to advance.

Mr. Shaikh also stated that Virtual Reality (VR) brings forth different opportunities for nefarious actors to act on the metaverse platforms. In addition, Neuralinks introduces a wide array of considerations pertaining to the possibility of manipulating electrical signals in the brain; a Neuralink device is set up by physically inserting a regulator/controlled chip into the brain tissue. The neurons act as electrical energy which is then converted into a chemical chemical reaction that shares information between neurons. This brings forth important considerations centered on the role of neuroscience in technology and the increased propensity for it to become weaponized.

Mr. Shaikh further emphasized now that Elon Musk has hinted at the possibility of weaponizing drones, such as kamikaze killer drones, it is becoming more likely for the security field to enter an unchartered territory that is incapable of dictating ways to detect and counter cyber security challenges.

Mr. Shaikh concluded by highlighting the rapidly transforming security and cyber intelligence functions that make it increasingly likely for nefarious actors to exploit easily available tools. For example, targets may be basic utility infrastructures, such as electricity, water, and Wi-Fi, to create catastrophic disasters. In addition, extremists, terrorists, and white supremacists would increasingly recruit and live-stream their activities through many different platforms, and while these platforms can respond and remove content, their responses have often been after millions of views have already been accumulated.

Question & Answer Period

In the topic of Metaverse, Mr. Shaikh expressed concerns regarding its versatility and noted that in VR, users have the autonomy to take any form of character and interact with others while concealing their identity. Even back in the mid-90s, text-based chat forums enabled people to build connections online and mobilize criminal activities offline. Now with the Metaverse, it offers even more opportunities for violent actors such as terrorists, human traffickers, and white supremacists to recruit and spread their influence.

Next, Mr. Shaikh discussed how contemporary barriers to counter online radicalization, such as the market-driven nature of social media corporations, may prime these corporations to be incentivized by the demand for social media activity instead of moral accountability. Another barrier pertains to the technical implausibility of staffing enough people to monitor chats all the time. Further, many of the screeners hired have reportedly developed Post Traumatic Stress Disorder (PTSD) from constant exposure to horrible imagery and extremist rhetoric. Lastly, the ambiguity surrounding the principle of freedom of speech may also mar the efforts to counter radicalization. According to Mr. Shaikh, there is a general inclination to lowering racism and hatred and accepting these practices as a matter of one's right to the freedom of speech. In the context of law, the deliberate and clear demonstration of racism, hatred, harassment, or any other forms of abuse is deemed illegal; however, up to that point, abusive nuances are deemed legal. This may be a problem, as it creates ambiguity to what social media companies should be held accountable for.

Regarding the Bill C-11 Online Streaming Act, Mr. Shaikh highlighted that such government action is a necessary avenue to continuously uphold the need for companies to take responsibility. When considering the market-driven nature of these platforms, it is likely that they are less incentivized to act on their own accord, as they benefit from the shared networks and social media activity. In demonstrating this, Mr. Shaikh brought forth an analogy between the regulation of toxins in the environment with the regulation of extremist content online. Government imposes regulations on the amount and type of environmental particulates that companies are allowed to produce into the air, based on the scientific research that back up these regulations. On a similar vein, Mr. Shaikh argued that the government can regulate companies that are putting violently influential narratives into the cyber atmosphere since they threaten public safety.

Mr. Shaikh also examined the role of Artificial Intelligence (AI) in detecting and countering extremism and noted that currently, AI only serves to flag potentially extremist content. However, Mr. Shaikh warned of potential problems. For instance, Google has compiled religious phrases — such as "caliphate" — as potential indicators, but "caliphate" is a mainstream concept in Islamic discourse. In effect, there is a risk of generalization as AI continues to identify these phrases that it has been tasked to detect, regardless of the bias and hyper-representation that it creates. Further, the question of bias brings us to the question of who should regulate the ways AI collects information. Thus, the role of AI in security has been a complex process that would possibly become even more complicated as cyber capabilities continue to expand.

Mr. Shaikh concluded the question-and-answer period by illustrating that solutions will have to come in the form of education through think tanks, non-governmental organizations, and other actors in the civil society. While government solutions are also needed, a generated volume of counter-narratives that could build public resilience against extremist content is also needed. As the public grows increasingly reliant on the internet, it is important for the public to be aware of the realities of the cyberspace security challenges.

KEY POINTS OF DISCUSSION

Presentation

- Uncovering secrets and obtaining information used to involve physically breaking into places, but with the advent of technology, these modes have been transferred over to cyberspace, lending increased autonomy to execute security and intelligence operations anywhere, anytime.
- The means by which these operations are carried out now include non-state actors in addition to the traditionally prevalent state adversaries.
- The average person has been getting caught up in the middle of the increasingly complex interplay of state and non-state actor involvement in cyber intelligence operations, making the civil society space more vulnerable to the increasingly varied types of intelligence collection that take place in the contemporary security space.
- The move toward virtual reality and Neuralinks brings forth different opportunities for nefarious actors and introduces a wide array of considerations pertaining the implications to security that may negatively impact the average person.
- With the weaponization of technology, it is becoming more likely for the security field to enter into an unchartered territory that is incapable of dictating ways to detect and counter cyber security challenges.

Question & Answer Period

- The metaverse and its versatility offer more opportunities for violent actors such as terrorists, human traffickers, and white supremacists to recruit and spread their influence.
- The contemporary barriers to counter online radicalization include market-driven incentives of the social media corporations; technical implausibility to staff and ensure the well-being of online screeners; and the challenged notions of freedom of speech that lends ambiguity to dictate the legality of regulating extremist content.
- Counter-radicalization solutions will have to come in the form of education and civic empowerment through think tanks, non-governmental

organizations, and other actors in the civil society that could build public resilience against extremist influence.

- The role of artificial intelligence in security has been crucial, but there is a risk of generalization, bias, and hyper-representation.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/