HACKING HUMANS: THE NEXT NATIONAL SECURITY THREAT

Date: June 20, 2024

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 June 20, 2024, Dr. Patrick Neal presented "Hacking Humans: The Next National Security Threat" at our June Digital Roundtable. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were the evolution of human augmentation and enhancement technologies, and the unique security threats that such advancements could produce. He also focused on the need to address ethical and moral concerns around transhumanism, possible legal gaps, and national security obligations.

NATURE OF DISCUSSION

Dr. Neal's presentation focused on the immediate need for the security environment to focus on the moral, ethical, and practical threats emerging from the new hybrid warfare battlefields that are being created due to the expanding use of technological augmentation in humans. As these technologies expand, there are new national security threats facing numerous actors, including individuals, such as a potential ability to manipulate their own bodily data or from civil unrest as society changes; organizations, such as new markets for organized crime to exploit; and states, such as the possibility of another state hijacking augmentation devices in its population. Dr. Neal emphasized the need for the security industry to think ahead and begin to consider preemptive measures before these technologies advance in order to maintain control over their application and mitigate risks.

BACKGROUND

Presentation

Improvements in AI and 3D printing are having substantial effects in the medical field, creating opportunities to explore human augmentation via technological implants and additions. Further advancements made in this area will create opportunities for malicious actors to mimic biometrics and hack implanted devices, and will require consideration from a security perspective.

Dr. Neal identified positive effects of these developments, such as possible increases in organ supply, leading to reduced wait times for transplants and a reduction in black market sales; an increased ability to provide real-time threat notifications to rural communities; partnerships with civil and self defence models, allowing for crisis response at a local level. He described these technological developments to be unavoidable, and argued that it is important for security professionals to be leaders in determining how these advancements will shape the future of security.

Dr. Neal additionally identified many possible threats, proposing that it may become possible for people to generate and project a fake self-image, allowing them to dupe mass surveillance techniques at will, either online or in person. Additionally, any control over augmented parts could be hijacked by enemy state actors. He raised concern that the societal changes correlated with these changes would lead to mass job loss and civil unrest, citing the unrest during the transition to an industrial society as an example. He also noted that these technological advances have created a projected 19% increase in markets that organized crime groups could exploit for additional revenue streams, and he suggested that this is an area requiring attention before it grows the way tobacco and oil did.

Many threats exist within the supply chain for augmentation devices, Dr. Neal explained. He emphasized the risk of zero-day exploits and the lack of knowledge regarding what they would look like and how they could be used. Additionally, the way that supply chain privacy will be embedded and encoded for the augmentation devices will need to be specially determined in order to minimize risks. Standards will need to be considered, including in regards to who will set them. Finally, he considered how third-party vendors could require unique vetting in order to fit into this system.

Dr. Neal urged for ethical and moral considerations to begin in order to address matters related to transhumanism, and cybernetics or cyborgs. There would be new types of intangible violence against augmented people, requiring there to be

a system in place to address these attacks and building public trust. There also needs to be discussion around whether there are gaps in existing laws or new ones are required altogether; Dr. Neal identified current laws as being applicable within these areas, and minimal need for new ones specific to this space. He also brought up questions around security obligations, considering what obligations nations have towards non-combatants, specifically at the body level. Lastly, he discussed the need to consider what new battlefields will emerge from this, what winning would entail in such conflicts, and what winning would comprise altogether.

Dr. Neal identified key topics discussed in forums related to these matters, including the possibility of requiring an enclave for transhumans with minimal trust in the government or public safety, and changes that may need to be made to the prison system in these circumstances. Regarding the latter, he considered that there would be a need for new methods that cut transhuman inmates off from the outside world in order to limit internal threats. He additionally highlighted the possible ethical and moral issues around preventing augmentation device use and working around extended lifespans.

Question and Answer

Do you see an international regulatory body coming out of these advancements/national security implications to ensure that international norms are established basically from the get-go (i.e. on the same level as CWC and the BWC or the NPT?) If so, do you think it could/should come out in advance of a real threat, or do you see it only coming after?

International standards have already evolved themselves, so any norms that are desired would need to be added posthumously. New standards would be unnecessary, as the pre-existing frameworks and laws would still apply in this area. The area of lethality would need to be explored more, however, in order to determine what kinds of harm are being committed against augmented humans. There will not be an international body because countries will choose to address AI and human augmentation differently due to religious and moral differences. It is most likely that anything will come after the event, following the patterns of history.

Does this mean that terrorists could create artificial fingerprints or irises to evade biometric controls or ID checks?

This has already been done and research is being done in forensic sciences to mimic hands. The missing question here is whether it is the hand of an existing person. This could allow others to access private information, such as phones, and use the access to violate body privacy. This has not been seen yet.

At what point would an implant be considered "part of you" as much as anything you were born with, and its removal in a criminal sentence be considered "cruel and unusual punishment?

If someone willfully adds something to their body, it is likely to be seen to be part of themself. This connects to the concept of the Ship of Theseus, or Theseus's Paradox, which questions whether a boat that has all new parts when it arrives at its final destination is the same one that left the original port. This can also be extended to encompass the fact that all cells in the human body regenerate every seven years. Bringing up cruel and unusual punishment leans back into the prison dilemma, where someone that is permanently connected to the world digitally would have to be forcibly disconnected, for example with a faraday cage, and at what point that is deemed to be cruel and unusual punishment itself.

KEY POINTS OF DISCUSSION

- AI and 3D technology are advancing rapidly, amplified by the medical benefits that this technology can produce. As the technology expands, so do the security risks.
- Human augmentation technology can pose risks to individual security, national security, and the supply chain. The responsibilities that national security agencies hold regarding the non-combative population will need to be discussed, as will what measures need to be enforced to protect the supply chain of the technology itself.
- Threats can come from individuals, unstable supply chains, organized crime groups, and other states. The possible risks from each of these sources will need to be considered and mitigated before they are able to cause significant harm.
- Ethical and moral considerations will be important to discuss as early as possible in order to limit the challenge of changing the pre-existing standards.

FURTHER READING

Harper, T. A. (2023). The Unlikely Alliance between Tech Bros and Radical Environmentalists. Retrieved from

https://slate.com/technology/2023/01/transhumanists-anti-humanists-misanthropy-revolt-against-humanity.html

Prox, R. (2023). DATA & INFRASTRUCTURE SECURITY: THE RISK OF AI ENABLED CYBER ATTACKS AND QUANTUM HACKING. The Journal of Intelligence, Conflict, and Warfare, 5(3), 117–121. https://doi.org/10.21810/jicw.v5i3.5179

Richards, J. (2023). OPENING REMARKS: CYBER RESILIENCE AND INTERNATIONAL PERSPECTIVES PANEL. The Journal of Intelligence, Conflict, and Warfare, 5(3), 241–243. https://doi.org/10.21810/jicw.v5i3.5210

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