Topic Paper 1: Cyber Terrorism and Security

"What a computer is to me is the most remarkable tool that we have ever come up with. It's the equivalent of a bicycle for our minds."

—Steve Jobs

Many of us share this exact sentiment with Steve Jobs. Hundreds of thousands of discoveries have been possible solely due to computers. The world has been forever altered thanks to the innovations of computer software.

This remarkable advancement in technology is utilized by all, including friends, families, coworkers, and terrorists. Black markets can be found online for various terror needs, whether they are weapons, communications, or even personnel. Terrorist groups, such as ISIS and Al Qaeda, have used the Internet to post propaganda in order to recruit members and share weapon tutorials.

The Internet has not just been a means for acquiring dangerous materials in preparation of attacks, but a mechanism of committing the terrorist attacks as well. In May 2017, chaos erupted in the United Kingdom as terrorists attacked the National Health Service's computer network, preventing the service's physicians from reading x-rays and various test results. As a result, the NHS was forced to close until it was able to get its network up and running. [1] Recently, hackers breached the Equifax, a credit-reporting agency, database disclosing millions of people's personal and financial

[1] https://www.theatlantic.com/news/archive/2017/05/global-cyberattack-reaches-unprecedented-scale/526647/

information.[2] These types of actions are what worry our generations as cyber terrorists threaten our way of life with such crimes.

To combat future cyber terrorism, whether it manifests as actual computer attacks or preparations for violent attacks, we will discuss preventative methods. How can we regulate the corporations that hold our personal information? Is there a standard level of security we can hold these businesses to? If so, what is it? How can we ensure that all companies will adhere to these recommendations? If certain countries cannot afford updating their security systems, what will we do?

In December 2015, Syed Farook and his wife, Tasheed Malik, committed a terror attack in San Bernardino, California, killing 14 and wounding 22 people. During the investigation, the FBI, the United States' national police force, recovered an iPhone 5C, which they believed to be relevant to the investigation. The phone was locked and Apple had not had the technology to access the phone. Should we require that corporations manufacture devices to create the software to override their password protection? Is there a concern of hackers gaining access to this software?

Some countries have given their citizens the right to privacy. Only with various court orders are law enforcement agencies permitted to access the contents of a personal computer. In many cases, though, terrorist attacks could have been prevented had the agencies been able to access the suspect's information instantly or even detect terrorist activity on unsuspected devices. Is there a balance that can be struck between personal privacy and crime prevention? If so, what is it?

---

[2] https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed

If you have any questions or concerns, please feel free to contact me at Hochman.ariel@gmail.com. Looking forward to engaging discussions with all of you!

All the best,

Ariel Hochman
Chair, CTC