Issues in Contemporary Ethics:

War: Cyber Warfare

The Questions

What relationship does soft and hard power share?

Has soft power become more prevalent? If so, how?

Should we consider supercomputers to be weapons?

How do these digital battlegrounds affect daily life?

How can cyber warfare be controlled?

What rights are we willing to give up?

Are privacy and security mutually exclusive?

How can states regulate transnational entities?

What responsibilities should corporations have?

What role do individuals and citizens pay?

How can we educate people on cyber awareness?

Should we allow censorship?

How tolerant can we be of fringe and controversial discourse online?

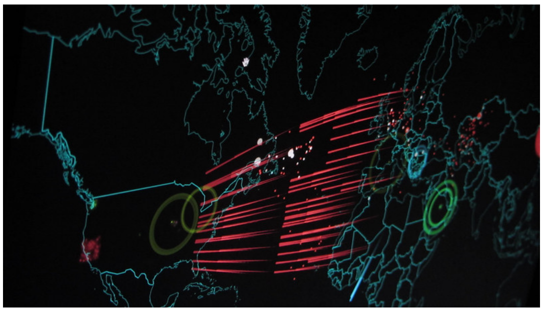
How are you affected by cyber-attacks?

How protected do you think you are?

Should we be worried about foreign governments, or our own?

At a Glance

The face of warfare is changing. Countries, firms, and citizens are now facing a force that is both incredibly hard to regulate and very easy to misuse. Cyber warfare is one of the new forms that states, groups and individuals have utilised in order to carry out attacks online and across borders. This brief explores how cyberwarfare is changing war and conflict and how the international community struggles to set boundaries on it.



Photos taken from the Norse Attack Map (Colen 2015)

Case Study: 2014 North Korea Internet Shutdown

In 2014, North Korea suffered a series of cyber-attacks wherein their internet and 3G mobile networks were shut down for extended periods of time (Kim 2014). North Korea was able to get their access back in a matter of days, and the damage this caused to the nation is relatively unknown. Kim Jong Un, the leader of North Korea blamed America and President Barack Obama for the attack, citing President Obama's prior warning as an admission of guilt. The National Defence Commission dismissed American involvement in the attack, however. Furthermore, the attack was relatively weak and the internet connection was only completely shut off nation-wide for 5 hours, so some theorize it could have been an amateur hacker. Nevertheless, nobody has claimed responsibility for the attack and it is anyone's best guess as to who is really behind it. This attack was one of many in the same year, which saw cyberattacks on a South Korean nuclear power plant operator, the hacking of Ukraine's power grid, and the hacking of Sony Pictures following the announcement of their controversial movie depicting Kim Jong Un, The Interview.

Implications

The cyberattacks can be seen as acts of aggression, yet they are hard to trace back to a perpetrator. How does this affect accountability? What about the possibilities of false flag attacks? Suppose a cyberattack shuts down an electrical grid in a large city. Is that non-discriminatory? Is power being shut down in essential services for civilians, such as hospitals? Since methods of cyberwarfare vary and the international community has agreed upon little regarding the subject, who is to say what states can and cannot do? Cyberattacks do not always need to be explicit hacking. Consider the Russian troll factories and news-bots during the 2016 American election. Is the spreading of false news and discord from a foreign nation a cyberattack? Or, is this an extension of propaganda states have promoted in the past?

Author: Maximilian Lee; Editor: Dr. Logan Cochrane

Further Reading

Michael Klipstein

Seeing is Believing: Quantifying and Visualizing Offensive Cyber Operations Risk

Brian M. Mazanec

Why International Order in Cyberspace is not Inevitable

Daniel Abebe

Cyberwar, International Politics, and Institutional Design

Carolyn Meinel

Code Red for the Web

Stephan Evans

Why did North Korea's Internet go Down?

Anna-Maria Talihärm

Towards Cyberpeace: Managing Cyberwar Through International Cooperation

Scott Shackelford

What the World's First Cyber Attack has Taught Us about Cyber Security

SentinelOne

The History of Cyber Security – Everything you Wanted to Know

Bozorgmehr Sharafedin

Iran says it Dismantled a U.S. Cyber Espionage Network

Alex Woodson

A New Era of Cyberwarfare, with Arun Vishwanath

Comparing Perspectives

Ethical theories have been divided into rationalist theories and alternatives to them. Rationalist theories include: deontological, utilitarian, contractualist and discourse ethics. Alternatives include virtue ethics, feminist ethics, postcolonial, and postmodern ethics. In this series of Briefs, one rationalist and one alternative will be explored to present contrasting views on the issue.

Contractualism

Contractualism is a theory that indicates that ethical values are determined by a contract or agreement. Thus, it as a rules-based theory that is dependent on the clear communication of these rules. Breaking these rules, within this contractual system, would be unethical. All parties agree to this and are bound by it. This basic structure, however, leaves the possibility of loopholes. The first recorded cyber-attack occurred in 1988 (Shackelford 2018). Since then, we still have relatively weak and vague international laws on cyberwarfare. There is no Geneva Convention for the virtual realm. The responses are mostly taken by individual states themselves or a coalition of states, such as the African Union, European Union, or the North Atlantic Treaty Organization. All of which have their own policy on cyberwarfare and cyber security. However, it can be argued that none of these have any real binding properties worldwide unless they are agreed upon at that scale. This brings into question the effectiveness of the international community to respond to new and emerging technology as well as challenge ethical qualms with cyber-attacks. Without a rule, how can there be responsibility?

Feminist Ethics

Some ethicists, drawing upon feminist critique, argue that many ethical theories leave out valuable and insightful perspectives underrepresented and marginalized people in society as well as those less able to shape the discourse. When it comes to cyberwarfare, feminists might consider how it is not just states and their resources involved, but the impact such attacks have on citizens. For example, let us say there is a hospital that has numerous patients on life support and people that require urgent medical attention. When every second counts, a power outage can have devastating effects. Who are these cyberattacks targeting? Is it a military base or a city? Just War Theory requires that you must be able to distinguish between combatants and non-combatants. Furthermore, a feminist would consider how the system favours those with power. How does the development and use of cyberwarfare propagate pre-existing power imbalances? For example, those with the budget to initiate cyberattacks and defend themselves with have more agency than those without, which have historically been subject to surveillance of more powerful states.

Questions for Reflection

As the virtual and real world become intertwined in warfare, the battle of hearts and minds gets closer to non-combatants. How does this affect our perception of war? Is war just guns and drones, or is it something less tangible? Can cyberattacks on vulnerable populations be considered a war crime? How can leaders protect the citizens from cyberwarfare without engaging in similar tactics? If this becomes the norm, how can we legislate it and how does that affect the life of the average person?

Christiaan Colen, (2015). Web Source.
Kim, J. (2014, December 28). North Korea blames U.S. for Internet outages, calls Obama monkey.
Shackelford, S., and Indiana University. (2018 November 5). What the Word's First Cyber Attack has Taught Us About Cyber Security.