Curtin University

Cyberwarfare and Cyberespionage

Dr Shannon Brandt Ford

29 March 2019

Welcome to Country

I would like to acknowledge the Whadjuk Noongar people as the traditional custodians of this land, and pay my respects to their elders past, present and future

Introduction

- A return to cyber-conflict (for me)
  - An opportunity to pull together different elements of this problem
  - Particularly the social aspects
- The Cyberwarfare debate
  - Expectations/predictions
  - An unexpected turn
- Cyberespionage and subversion
  - The emerging “Soft” War debate
  - China, Russia and the U.S.
- Policy approaches
  - Hacking back
  - Cybernorms
  - Equilibrium
  - Australia’s offensive cyber capability

A. The Cyberwarfare debate

- Cyberwar is the first major new form of warfare since the development of nuclear weapons
  - Cyberthreats to national cybersecurity are complex and diverse
  - Threats might be isolated to single machines or consist of distributed attacks against large numbers of machines at once
- What are the concerns?
  - Potential harm to critical infrastructure
  - Lowering the threshold for conflict
  - Increased likelihood of escalation
  - Attacks on joint-use infrastructure (difference between dual use, joint use and civilian information systems)

The era of sophisticated cyberweapons?

- Cyberweapons
  - Neil Rowe (2010) “software used to attack other software or data within computer systems”
  - Randall Dipert (2010) “intentional cyberharms that are instigated or controlled by political organizations (or their military services) on other political organizations or services”
- Stuxnet
  - Frequently cited as a successful example of a sophisticated cyberweapon
  - A computer worm (discovered in June 2010) specifically designed to attack, and physically damage, Iran's nuclear facilities
- Attributing an attack from a cyberweapon to a specific party is notoriously difficult
  - The problem of quickly and reliably attributing responsibility
  - Thus the credibility of denial of responsibility on the part of culpable aggressors

Cyber Armageddon

- Richard Clarke and Robert Knake (2010) argued that a sophisticated cyber attack by one of several nation-states could:
  - Take down the Pentagon's classified and unclassified networks
  - Trigger explosions at oil refineries
  - Release chlorine gas from chemical plants
  - Disable air traffic control
  - Cause trains to crash into each other
  - Delete all data – including offsite backups – held by the federal reserve and major banks
  - Plunge the country into darkness by taking down the power grid from coast-to-coast
- The result:
  - Thousands die immediately
  - Cities run out of food
  - ATMs shut down
  - Looters take to the streets

Thresholds of harm

- Thresholds of harm provide important benchmarks for establishing the seriousness of an action by one state against another
  - This then determines the range of measures available to the transgressed state in response
- For instance, this understanding of what constitutes a harmful action is particularly important when it comes to determining what is (and what is not) considered to be an act of war
  - The Tallinn Manual aims to be the most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations
  - It argues that such thresholds in cyber-conflict should be specified in terms of the nature and/or extent of the injury, loss of human life and/or physical destruction caused
  - The idea informing this approach is that cyber-attacks cannot, in and of themselves, constitute warfare
  - Only the physically harmful outcomes count

A human-technical problem

- Yet cyber conflict is more than a physical-technical problem
  - In some cases, trust between people is the main target (or casualty) of a cyberattack
- Stuxnet
  - A key aspect of the attack was trust in the nuclear program itself
  - The information being communicated to the operators did not match the actual output of the system
- Ashley Madison hacks
  - The hacks caused a loss in trust between humans
  - The loss of trust in the service provider (to guarantee anonymity) and the consequent revealing of betrayal to one's partner
- Snowden revelations
  - A goal was to undermine the trust relations between the state and its citizens
  - In particular, the public's willingness and capacity to trust in state mechanisms of national and international security

Trust

- Trustworthiness is a foundational principle for resilient cybersystems
  - Henschke, Adam and Ford, Shannon B, (2017). “Cybersecurity, Trustworthiness and Resilient Systems: Guiding Values for Policy.” *Journal of Cyber Policy 2*(1): 82-95
- The success of cyberspace depends on information technologies to reliably mediate important relations between people
  - E.g. Banking, News, Public Safety
  - These interactions typically occur without physical proximity
  - Must be able to trust the overall human-technical systems that support cyberspace
- Principles
  - Acknowledge the reality of vulnerability
  - Map trust relations
  - Develop and protect a reputation for trustworthiness
  - Promote oversight and good governance

An unexpected turn: Cyberespionage

- Intelligence collection might target the confidential data and communications of:
  - Foreign government officials (espionage)
  - Terrorists (law enforcement)
  - Ordinary citizens (infringement of privacy rights)
  - Private corporations (industrial espionage)
- In some recent cases of cyberespionage, sensitive information has been stolen on a massive scale
  - e.g. The U.S. Office of Personnel Management data breach
  - Approximately 21.5 million personnel records stolen
- The conventional understanding tends to overlook the seriousness of aggregating harms
  - Aggregated harms are the small harms that sit below conventional thresholds but that together can add up to pose a significant threat to national interests

Subversion

- What about meddling in election processes?
  - E.g. Russia's DNC hacks
- Subversion is a step beyond intelligence collection
  - Subversion has the goal of undermining the authority of an existing political order
  - Groups doing this are now benefitting from new communication technologies
- Subversion using cyber means is a type of covert action
  - Covert action involves a state seeking to intervene secretly into the affairs of other states or factions
  - Meant to influence events overseas through the use of non-attributed propaganda, political action, economic manipulation, and paramilitary (war-like) operations
  - It's a type of "soft war"

“Soft” war

- “Soft war” fuses the notion of “soft power” with coercive tactics that fall short of armed attack
  - Non-kinetic tactics are soft warfare inasmuch as they fall short of conventional armed conflict
- Soft war is a broad concept that includes non-kinetic measures such as:
    - Cyber warfare
    - Economic sanctions
    - Propaganda
    - Nonviolent resistance and civil disobedience
    - Boycotts
    - Lawfare
- MI6 Chief Alex Younger speech on Fourth Gen espionage (Dec 2018)
  - “Article 5 of the North Atlantic Treaty, which states that an armed attack against one or more of the NATO allies will be considered an attack on all, is the cornerstone of our defence and security. But it presupposes a clear distinction between a condition of war and a condition of peace – precisely the distinction that our opponents are seeking to obscure”

Policy and practice

- Different forms of “soft” war already exist in the policies and practices of many countries
- China: Unrestricted warfare
  - A book on military strategy written in 1999 by the PLA Colonels Qiao Liang and Wang Xiangsui
  - How to defeat a technologically superior opponent by discarding existing conventions about how and where “war” is fought
- Russia: Strategic spoiler
  - Spoil the US’s ambitions to retain the rules-based global order
  - The DNC hacks were not technologically sophisticated
- U.S.: Covert action
  - U.S. Executive Order 12333 says that:
    - covert activity is a foreign policy option (as distinct from intel collection)
    - identifies the appropriate agency to conduct covert action during peacetime
    - By definition, it is non-attributable

‘Hacking back’

- An argument based on self-defence
  - Devolve the responsibility for defence to potential targets
  - “Active cyber defense”
  - A counter-response to an attack rather than an unprovoked first strike
- Why?
  - Responses to an attack need to be very fast and, at least in some cases, automated
  - The right of self-defence
  - An obligation to protect corporate assets
- Problems
  - Illegal?
    - An obligation to protecting corporate assets does not extend to breaking the law
  - Increases the likelihood of unintended consequences
  - Many corporations don’t have the required technological sophistication
- Patrick Lin (2016) Ethics of Hacking Back: Six arguments from armed conflict to zombies, http://ethics.calpoly.edu/hackingback.htm

Cybernorms

- The preferred approach is to agree on international norms of behaviour
  - Not a great deal of progress so far
- In Nov 2018, two competing resolutions at the UN
  - U.S. sponsored resolution to create a new Group of Governmental Experts (GGE)
    - To study how international law applies to state action in cyberspace and identify ways to promote compliance with existing cyber norms
  - Russian sponsored resolution to create an open-ended working group of the General Assembly to:
    - Study the existing norms contained in the previous UN GGE reports
    - Identify new norms
    - Study the possibility of “establishing regular institutional dialogue . . . under the auspices of the United Nations”
- Expertise is largely found in Silicon Valley rather than in the Government/Military
  - Requires significantly improved cooperation with tech giants such as Apple, Amazon, Alphabet (Google), Microsoft and Facebook
  - Alibaba and Tencent?

Equilibrium

- Equilibrium emerges from tit-for-tat measures
  - Focus on developing proportionate “counter-measures”
- Dipert (2010) argued that cyberwarfare is not amenable to regulation by international pacts
  - So we can expect long periods of low-level, multilateral cyberwarfare as a game-theoretic equilibrium is sought
  - i.e. a Cyber Cold War
- Gross (2018) argues that the doctrine of counter-measures provides the necessary legal framework
  - The defining criterion is equivalence
  - Counter-measures exact a measure of harm equal to what the victim suffers
- In most cases, cyber counter measures would aim to enforce the legal regime governing cyber activities and restore the status quo
  - But in response to serious ongoing cyber-aggression, states may reasonably turn to active defence measures or cyber retaliation
  - Deterrence then plays a key role

Australia's offensive cyber capability

- The Australian Signal Directorate's (ASD) offensive cyber capability was disclosed in April 2016
  - Additional insight in a speech by Director General ASD Mike Burgess on Wed 27 April 2019
  - A broad range of activities designed to disrupt, degrade or deny adversaries
  - Activities are focused offshore
- Offensive cyber operations have helped disrupt Islamic State's ability to communicate, launch attacks and spread propaganda
  - Use specialised tools and techniques to disrupt their communications or interfere with the way they operate online
- Rather than destroying the target's ICT completely, they might find that:
  - Their communications won't work at a critical moment
  - Or not in the way they are expecting
  - Or they can't access crucial information, such as their bank accounts

Discriminate and Proportionate

- Missions must follow principles of discrimination and proportionately
  - Subject to rigorous oversight
  - Planning includes considerations of unintended consequences
- Clear statement ruling out hacking back in self-defence
  - This is considered illegal in Australia
- Australia's Cyber Security Strategy (2016)
  - https://cybersecuritystrategy.homeaffairs.gov.au/
  - "Australia's defensive and **offensive cyber capabilities** enable us to deter and respond to the threat of cyber attack. Any measure used by Australia in deterring and responding to malicious cyber activities would be consistent with our support for the international rules-based order and our obligations under international law"
  - First Annual Update (2017)
  - https://cybersecuritystrategy.homeaffairs.gov.au/australia%E2%80%99s-cyber-security-strategy
  - "Following the declaration of Australia's **offensive cyber capability** in the Cyber Security Strategy, the Prime Minister announced in November 2016 that offensive cyber capabilities are being employed in support of Australian Defence Force operations against Islamic State. This contributes to our national deterrence posture, and promoted mature discussion about the application of such capabilities under international law."

Conclusion

- Cyber-conflict has not gone in the direction predicted
  - We need to get a better handle on the social aspects of what is a human-technical problem
- Does the scale of some cyberespionage programs make a significant difference to how Australian policymakers should think about this problem? What about meddling in election processes?
  - Yes in both cases
  - Falls into the category of serious ongoing cyber-aggression
  - It is reasonable to consider active defence measures or cyber retaliation for the purposes of deterrence
- Develop a range of counter-measures to proportionality deal with “soft war” threats to national security
  - What are the principles of discrimination for Australia’s offensive cyber capability?
  - i.e. where do we draw the line on who can be targeted?

Questions?

- References:

  - Allhoff, Fritz, Henschke, Adam and Strawser, Bradley J. (2016). Binary Bullets: The Ethics of Cyberwarfare. New York, Oxford University Press.
  - Clarke, R. A. and R. K. Knake (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York, HarperCollins Publishers.
  - Dipert, Randall R. (2010). "The Ethics of Cyberwarfare." Journal of Military Ethics 9(4): 384-410.
  - Gross, Michael L. and Meisels, Tamar (2017). Soft War: The Ethics of Unarmed Conflict. Cambridge, Cambridge University Press.
  - Henschke, Adam and Ford, Shannon B, (2017). "Cybersecurity, Trustworthiness and Resilient Systems: Guiding Values for Policy." Journal of Cyber Policy 2(1): 82-95.
  - Lucas, George (2016). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare, Oxford University Press, USA.
  - Rid, Thomas (2013). Cyber War Will Not Take Place. Oxford, Oxford University Press.
  - Rowe, N. C. (2010). "The ethics of cyberweapons in warfare." International Journal of Technoethics 1(1): 20-31.