Conflict and Cyber-espionage: Ridding the World of Cyber War?

Shannon Brandt Ford

Lecturer in Intelligence and Security Studies
Charles Sturt University, AUSTRALIA

Presentation delivered at the Oceanic Conference on International Studies
University of Melbourne, Melbourne

Panel Title: War, Conflict and Cyber(in)security
08:30 – 10:00
Thursday, 10 July 2014

CONTENTS

Introduction

This paper examines Thomas Rid's argument that physical violence is a necessary condition of war and that attacks from cyberweapons cannot meet this condition because they are not physically violent and, in many cases, will not even result in permanent damage. In particular, my research interest lies in understanding the ethical principles that justify the use of armed force.

In the first section, I outline Rid's argument that most discussions of "cyberwar" are exaggerated because there is no known act of "cyber" war, when war is properly defined.

Then, in the second section, I argue that the "warfighting distinction" is not as useful for dealing with modern conflict as Rid assumes it is.

Finally, in the third section, I argue that there remains no shortage of serious concerns when it comes to the use of cyberweapons.

Espionage is not war

I start by outlining Thomas Rid's recent argument that most discussions of "cyberwar" are exaggerated because there is no known act of "cyber" war, when war is properly defined. An important part of his argument is that the most widespread use of state-sponsored cyber capabilities is for the purpose of espionage, which, he argues is neither crime nor war. I agree with Rid that the novelty of cyber conflict makes it unclear what actions constitute an act of war and that there is an important distinction between acts of war and espionage.

a. Defining war

Thomas Rid makes the point that attacks from cyberweapons are not physically violent and, in many cases, will not even result in permanent damage. He argues that, 'so far there is no known act of cyber "war," when war is properly defined. This of course' he states 'does not mean that there are no political cyber offenses. But all known political cyber offenses, criminal or not, are neither common crime nor common war. Their purpose is subverting, spying, or sabotaging.'[1]

In defining war, Thomas Rid borrows from Thomas Mahnken who, in turn, uses Clausewitz's famous formulation,

"War is thus an act of force to compel our enemy to do our will."

According to Rid (and Mahnken), three aspects of this definition are notable for the purposes of discussing cyberwar.

First, war is "Instrumental." This means that war is not senseless slaughter, but rather an instrument that is used to achieve a political purpose. This differentiates it from other types of violence, such as criminal activity.

Second, war is "Political." It is not the use of force against an inanimate object, but rather against an organisation that possesses its own values and objectives, and responds to attack with reciprocal action.

Third, war is "Violent." War involves a specific type of force and this separates it from other types of political, economic and military competition. War involves violence, bloodshed and killing.

b. Violence and war

Now I agree that war is "Political" and "Instrumental." But I'm not convinced by Rid's view of war and violence. Rid argues that "most cyber attacks are not violent and cannot sensibly be understood as a form of violent action. And those cyber attacks that actually do have the potential of force, actual or realised, are bound to be violent only indirectly."[2]

He then goes on to explain this point in more detail and suggests that, "violence administered through weaponised code is limited in several ways: it is less physical, because it is always indirect. It is less emotional, because it is less personal and intimate. The symbolic uses of force through cyberspace are limited. And, as a result, code-triggered violence is less instrumental than more conventional uses of force. Yet, despite these limits, the psychological effects of cyber attacks, their utility in undermining trust, can still be highly effective."[3]

In short, Rid's argument is that cyberweapons are more limited than kinetic attacks because they are not directly violent. Presumably this means we should be less concerned about cyberweapons than we should about kinetic weapons. But I want to challenge Rid's conclusion on two grounds. First, his approach to defining war and applying it to modern conflict is problematic. And second, we should be equally concerned about the use of cyberweapons because they still have the potential to cause serious harm to objects and the lives of humans.

In-between Conflict

Now in this second section of my paper, I briefly address the problem with Rid's approach to defining war and applying it to modern conflict. I argue that when it comes to modern conflict, the conventional "warfighting" distinction leaves us with insufficient guidance.

a. Modern conflict

Let me start out by suggesting that the challenges of modern conflict are changing the conventional understanding of warfare to some degree.

One challenge is the problem posed to state military forces by asymmetric conflict.

Christoper Kutz, for example, argues that state military conflict today rarely occurs in the form of major battles between armies, but increasingly through the tactics of "asymmetrical" warfare, including guerrilla raids, hiding among either one's own or one's enemies' populations, infiltration of enemy lines, sabotage, and joint operations with collaborating civilians.[4]

Michael Gross suggests that an air of criminalization permeates asymmetric conflict as more and more adversaries view one another as despicable villains rather than honorable foes or brothers in arms.[5]

And Fritz Allhoff suggests that rather than being fought on conventional battlefields, 'wars' against terrorists are fought in urban environments where the

combatant/noncombatant distinction has become blurred and their command structure is often unclear and decentralized.[6]

A second challenge of modern conflict to the conventional understanding of warfare is the emerging use of UAVs and the problems created by targeted killing.

Claire Finkelstein argues that the practice of targeted killing, and its perceived role in judgments of military necessity, casts in relief the complicated realities of modern warfare. This, she believes, is in significant part a reflection of the degree to which the practice of targeted killing departs from the traditional battlefield form of combat, and hence from the core justifications for killing in war.[7]

And a third significant challenge for the conventional understanding of warfare is the development of cyberweapons, and their emerging use.

Radical changes in technology continue to transform the norms of conflict. The emergence, evolution and global expansion of the Internet are central to developing an understanding of the issue of security (and insecurity). Although the ubiquity of computer technology itself has been important, it is the emergence of the complex global system of interconnected networks – linking hundreds of millions of computers around the world – that makes cyber security an omnipresent domain that reaches deeply into multiple facets of existence, and as such presents a multitude of gaps for potential security threats to manifest.

In his article on "cyber war and cyber warfare,"[8] Thomas Mahnken highlights the unique attributes of what he describes as the "cyber instrument of warfare" (and what I refer to more generally as "military cyber-capability").

First, Mahnken suggests that unlike other military capability, the effects of cyber-weapons can be both instant and global.

Second, cyber-weapons are available both to state and non-state actors.

Third, as a relatively new military instrument, cyber-weapons surrounded by a great deal of uncertainty. Attributing cyber actions to actors may be difficult, though this difficulty is likely to be less in wartime than in peacetime.

Finally, the novelty of cyber conflict makes it unclear what actions may constitute an act of war and which actions may lead to escalation.

b. The conventional warfighting distinction

Now this in-between area of conflict is sometimes referred to as the murky world of "cyber-espionage." Thomas Rid makes further distinctions between espionage, sabotage and subversion but I don't have time today to go into more detail about these particular distinctions.

This approach to understanding conflict demonstrates the importance of the conventional "warfighting distinction." As I have argued elsewhere, the warfighting distinction says that designating a context as "war" alters the way in which we should understand the basic moral principles for justifying the use of cyberweapons (or other types of weapons). The conventional "war" context presupposes that a damaging act that intends harm is part of a larger struggle between two or more political communities engaged in armed conflict.

Blank and Guiora, for example, describe the way in which the conventional warfare paradigm explains conflict to those who fight. The enemy is obvious and the role of civilians as passive victims of war is generally clear. The objective — to defeat a clearly identified enemy — is easily articulated; the means — military hardware — is obvious; and the outcome, from a military perspective, is black and white — one side surrendered. Opposing soldiers openly carrying weapons posed dangers that led to concise and precise "open fire" orders. The rules of engagement ("ROE") in the conventional context are uncontroversial and simple to interpret: soldiers killed soldiers and protected innocent civilians and others *hors de combat*. In that sense, the rules of yesterday's battles were obvious.[9]

But when it comes to the use of military cyber-capabilities, the "warfighting" distinction still leaves us with insufficient ethical or legal guidance for the use of cyberweapons in war. For example, the 'warfighting' approach to judging the use of military 'cyber-capabilities' doesn't help us reduce unnecessary collateral harm. "Targeting joint-use industries and systems in a lawful military conflict is generally permitted by international law and Just War Theory."[10] Whereas, "Targeting primarily civilian structures and networks is prohibited by international law and by almost all theories of morality in warfare."[11] So, "Cyberweapons could target joint-use infrastructure, that is, systems and structures for both civilian and military uses, or even civilian targets with the goal of demoralising, weakening, or confusing an enemy's military of civilian leadership."[12] In other words, designating the context as "war" doesn't help us solve this type of problem with the use of cyberweapons.

I take it that Rid's purpose in addressing the issue of "cyberwar" is to downplay some of the more alarmist discussions surrounding cyberwar. But the problem with his approach is that it is not simply a matter of distinguishing espionage, sabotage and subversion from conventionally understood warfare. As I pointed out earlier in my paper, the challenges of modern conflict go deeper than this: they highlight the inadequacy of the conventional understanding of the warfare distinction itself.

c. Non-war role

A second problem with this conventional approach to the warfighting distinction is its failure to acknowledge the necessary non-war role played by military cyber-capabilities.

For example, Blechman and Kaplan point out that the armed forces can be used as an instrument of policy in time of peace because of its general character, deployment and day-to-day activities. In peace, as in war, a prudent statesman will turn to the military not as a replacement or substitute for other tools of policy but as an integral part of an admixture of means.[13] A political use of the armed forces occurs when physical actions are taken by one or more components of the uniformed military services as part of a deliberate attempt by the national authorities to influence, or to be prepared to influence, specific behaviour of individuals in another nation without engaging in a continuing contest of violence.[14]

The Harm in Cyberweapons

In this final section, I argue that there remains no shortage of serious concerns when it comes to the use of cyberweapons. Cyberweapons are software designed to attack and damage other software (or data within computer systems) with the intention of doing harm. And this harm includes both the destruction of objects and the lives of humans.

a. Harm to critical infrastructure

First, the damage to software caused by conflict in cyberspace has the potential to harm critical infrastructure and threaten the lives of people. It might prove that such threats are not that serious, but currently there is a great deal of uncertainty about this one way or the other. And that uncertainty is cause by the fact that cyber-weapons are a relatively new military instrument.

b. Lowering threshold for conflict

Second, there is the potential that the use of cyberweapons could lower the threshold for conflict between states. The novelty of cyber conflict makes it unclear what actions may constitute an act of war and which actions may lead to escalation. In particular, the perception that cyberweapons are not seriously "harmful" could lead to their increased use and potentially instigate more serious forms of conflict.

We don't want States overreacting to cyber-attacks. The key mistake here is to conflate the threat from a cyber-weapon with one that involves "cyber-exploitation." There are non-damaging cyber "attacks" which aim to exploit an information system

without doing harm. Examples include: 1) theft of information (both state-sponsored and criminal); 2) creating unauthorised access (or a back door) to a system; or 3) attempts to take control of an information system. The important point here, so the reasoning goes, is that we should acknowledge an important distinction between attacks using "cyber-weapons" (which aim to harm infrastructure and persons) and "cyber-exploitation" (which involves a non-damaging "attack" on cyber-infrastructure), and then respond accordingly.[15]

c. Attacks on joint-use infrastructure

Third, as I mentioned earlier, cyberweapons might also increase the likelihood of civilians being targeted and/or becoming victims of disproportionate attacks on joint-use infrastructure. The problem here is that the distinction between joint-use and civilian information systems is much less meaningful when the military use of civilian cyber-infrastructure is ubiquitous. As Ed Barrett has observed, the "tight linkages between legitimate and illegitimate targets, will combine to frequently render internet-delivered cyber-attacks indiscriminate."[16] And, "Even if cyber-weapons are discriminate, questions of unnecessary harm to combatants and disproportionate harm to civilians remain."[17] That is, the problem is that the distinction between joint-use and civilian information systems is much less meaningful in cyberwarfare when the military use of civilian cyber-infrastructure is ubiquitous.

Conclusion

In conclusion, I agreed with Rid that the novelty of cyber conflict makes it unclear what actions constitute an act of war and his general point that there is an important

distinction between acts of war using cyberweapons (i.e. attacks intended to cause serious harm) and cyber-exploitation (for example, espionage and crime).

But I am not convinced by Rid's argument that cyberweapons are more limited than kinetic attacks (which presumably means we should be less concerned about them) because they are not directly violent.

First I argued that the "warfighting distinction" is not as useful for dealing with modern conflict as Rid assumes it is.

And second, the purpose of a cyberweapon is to attack an information system in order to perpetrate some harm. And we should be equally concerned about the use of cyberweapons because they have the potential to cause serious harm to objects and the lives of humans.

Additional Points

.

REFERENCES

Allhoff, Fritz. *Terrorism, Ticking Time-Bombs, and Torture: A Philosophical Analysis*. University of Chicago Press, 2012.

Barrett, Edward T. "Warfare in a New Domain: The Ethics of Military Cyber-Operations." *Journal of Military Ethics* 12, no. 1 (2013): 4-17.

Blank, Laurie, and Amos Guiora. "Teaching an Old Dog New Tricks: Operationalizing the Law of Armed Conflict in New Warfare." *Harvard National Security Journal* 1 (2010): 45-85.

Blechman, Barry M., and Stephen S. Kaplan. *Force without War: U.S. Armed Forces as a Political Instrument*. Washington, DC: The Brookings Institution, 1978.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (2010/12/01 2010): 384-410.

Finkelstein, Claire. "Targeted Killing as Preemptive Action." In *Targeted Killings: Law and Morality in an Asymmetrical World*, edited by C. Finkelstein, J.D. Ohlin and A. Altman. Oxford: Oxford University Press, 2012.

Ford, S. Brandt. "Warfare, Cyberweapons and Morality." In *Cybersecurity: Mapping the Ethical Terrain*, edited by A. Henschke, S. Brandt Ford, N.G. Evans, Adam Gastineau and Levi West. Canberra: National Security College, The Australian National University, 2014.

Gross, M.L. *Moral Dilemmas of Modern War: Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict*. Cambridge University Press, 2009.

Kutz, Christopher. "The Difference Uniforms Make: Collective Violence in Criminal Law and War." *Philosophy & Public Affairs* 33, no. 2 (2005): 148-80.

Mahnken, Thomas G. "Cyber War and Cyber Warfare." In *America's Cyber Future: Security and Prosperity in the Information Age*, edited by Kristin Lord and Travis Sharp. 55-64. Washington, DC: DNAS, 2011.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.

[1] Thomas Rid, *Cyber war will not take place* (Oxford University Press, 2013). 10.

[2] Ibid., 12.

[3] Ibid., 34.

4 Christopher Kutz, "The difference uniforms make: collective violence in criminal law and war," Philosophy & Public Affairs 33, no. 2 (2005): 154-55.

5 M.L. Gross, *Moral Dilemmas of Modern War: Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict* (Cambridge University Press, 2009). 12.

6 Fritz Allhoff, Terrorism, Ticking Time-Bombs, and Torture: A Philosophical Analysis (University of Chicago Press, 2012). 36.

7 Claire Finkelstein, "Targeted Killing as Preemptive Action," in Targeted Killings: Law and Morality in an Asymmetrical World, ed. C. Finkelstein, J.D. Ohlin, and A. Altman (Oxford: Oxford University Press, 2012), 162.

[8] "Specifically, this chapter explores both the independent use of the cyber instrument of warfare, which I term "cyber war," as well as the use of the cyber instrument as a dimension of a larger military conflict, which I term "cyber warfare." Thomas G Mahnken, "Cyber War and Cyber Warfare," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristin Lord and Travis Sharp (Washington, DC: DNAS, 2011), 58.

[9] Laurie Blank and Amos Guiora, "Teaching an Old Dog New Tricks: Operationalizing the Law of

Armed Conflict in New Warfare," *Harvard National Security Journal* 1(2010): 58.

10 Randall R. Dipert, "The Ethics of Cyberwarfare," Journal of Military Ethics 9, no. 4 (2010): 390.

11 Ibid.

12 Ibid.

13 Barry M. Blechman and Stephen S. Kaplan, Force Without War: U.S. Armed Forces as a Political Instrument (Washington, DC: The Brookings Institution, 1978). 4.

14 Ibid., 12.

[15] S. Brandt Ford, "Warfare, cyberweapons and morality," in *Cybersecurity: Mapping the Ethical Terrain*, ed. A. Henschke, et al. (Canberra: National Security College, The Australian National University, 2014), 20.

16 Edward T. Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," *Journal of Military Ethics* 12, no. 1 (2013): 10.

17 Ibid.