Chapter 4
Technology, Information, and Modern Warfare: Challenges and Prospects in the 21st Century

Wayne McCormack and Deen Chatterjee

Abstract In international law there are two long-recognized conflicts: one between self-determination and non-intervention, and the other between self-defense and non-intervention. In Sect. I, Wayne McCormack examines the first conflict in the context of informational warfare, concluding that supplying information (or misinformation) in a foreign conflict with the objective of altering the course of the conflict is within the acknowledged sovereignty rights of a state and does not violate the non-interference right of the state in conflict. In Sect. II, Deen Chatterjee examines the other conflict—that between self-defense and non-intervention. He claims that the provision of preventive war in self-defense can get unduly interventionist, especially in the context of cyber warfare, making the world less secure. To counter this prospect, Chatterjee suggests that countries should promote prevention in non-interventionist terms by relying on the soft power of diplomacy and collaboration.

The traditional debates of war and peace have become a major focus of controversy in response to the changing nature of warfare in the twenty-first century, putting in sharp focus the issues of traditional paradigms and their limits, the moral hazards of military response, and the future of warfare. All these have vast implications for international law, justice, and human rights. This chapter looks at one important aspect of the changing terrain of today's war: the normative and legal challenges of information and communication technologies in modern warfare.

The chapter is divided into two sections. In Sect. I, Wayne McCormack examines the moral and the legal implications of informational warfare related to interfering in the internal affairs of a nation facing armed uprising or going through similar violent turmoil. McCormack's focus is primarily the turmoil of the Middle East. He discusses the benign use of information in conflict zones to alter the outcome. In Sect. II, Deen Chatterjee examines the moral challenges of the growing reliance

W. McCormack (✉) · D. Chatterjee
University of Utah, Salt Lake City, USA
e-mail: wayne.mccormack@law.utah.edu

D. Chatterjee
e-mail: deen.chatterjee@law.utah.edu

L. Floridi, M. Taddeo (eds.), *The Ethics of Information Warfare,*
Law, Governance and Technology Series 14, DOI 10.1007/978-3-319-04135-3_4,

on information and communication technologies in modern warfare. Specifically, he looks at the specter of "virtual warfare" in the blurring of the distinction between preemption and prevention in wars of self-defense.

4.1 Introduction

The phrase "informational warfare" covers a host of possibilities—attacks on another entity's information (cyber warfare), promotion of reasonably accurate propaganda into another country (Radio Free America), promotion of disinformation (telling populace of impending disasters), and financial support of candidates in elections. For example, if we send misinformation about the Assad regime into the public domain in Syria, that's just propaganda or what was once called "psy ops". At the other extreme, covert infiltration into the rebel groups with training materials could be illegal under the Nicaragua decision.[1] In between those extremes, funneling government money into a political campaign in another country is highly questionable (as an intervention into internal affairs of another sovereign) but is done almost certainly as a routine matter.

I assume that the U.S. poured substantial money and personnel into the Arab Spring of 2011. I also assume that we would have supported any candidate who ran against Hugo Chavez. These efforts parallel what the U.S. Supreme Court has authorized in holding that corporations have a constitutional right to pump all the money they want into political campaigns. And most observers assume that includes "foreign" corporations because how can you tell the difference between foreign and domestic in the global economy? We can also assume that the Court would hold that the First Amendment protects corporations in funneling money into foreign political actions. One might try to distinguish taking federal government money for that purpose but it is not easy to see a rational distinction between using government money as a contractor and using money derived from other revenue sources.

The question then becomes whether that interference in the affairs of other nations can somehow be justified under international law. But first let's explore a bit more about the content or tactics of "informational warfare".

In my lifetime, I have seen the War on Poverty (I don't recall that LBJ tried to justify the shooting of homeless persons), the War on Crime (some in the Nixon years might have tried to justify shooting criminals), the War on Drugs (I remember one Navy captain asking if he was supposed to shoot pharmacists), and now the War on Terror (I honestly don't know how you shoot a feeling). As a rhetorical flourish, the word "war" is useful for mobilizing resources. As a legal concept, however, it has very important and detailed consequences. Now people are starting to talk about "informational warfare" as if it were different from the propaganda campaigns of the past. I can think of some TV channels that might be worth destruction but that would probably fit into the category of MOOTW (military operations other than war) because it would not be a prolonged conflict.

[1] Nicaragua v. United States, I.C.J. Reports 1986, p. 14.

In recent years, a rather Orwellian notion has arisen around the concept of "Lawfare." I objected to this term back when General Dunlap introduced it about 10 years ago. But it quickly picked up favor in the Justice Department. It implies that anyone who objects to the legality of a US action is engaged in an act of warfare.

Here is a quote from the "Lawfare Project" website:

> The enemies of the West and liberal democracies are pursuing a campaign of lawfare that complements terrorism and asymmetric warfare. Terrorists and their sympathizers understand that where they cannot win by advocating and exercising violence, they can attempt to undermine the willingness and capacity to fight them using legal means….
>
> The precedents set by lawfare actions threaten all liberal democracies equally. It is imperative that lawfare be opposed and that international human rights law and its interpretation be managed properly and in line with the tenets of democracy.[2]

It is certainly true that legal challenges can be frivolous, that allegations of violations by democratic governments can be fabricated. But it is also quite true that democratic governments, notably the United States, in the recent past have engaged in illegal detentions, interrogation, and surveillance—as well as questionable lethal drone attacks. If every allegation of wrongfulness by a democratic government were itself unlawful, then how would democratic institutions correct themselves under the rule of law?

The whole thing is quite reminiscent of the SLAPP (strategic lawsuits against public participation) controversy 30 years ago, in which industry would file suits against environmental groups[3] (who might then counterclaim for "abuse of process" or basic Rule 11). Those issues eventually just died away as people grew up and litigated under the rules.

This notion of "lawfare" seems to challenge the very idea of claims of abuse or human rights violations. So even drawing into question the validity of targeted killing could be considered lawfare—a chilling prospect in itself.

I think the ethics of propaganda allow for plenty of hyping and even misinformation but the degree of covert intervention into the internal affairs of another country has never been seriously delineated (how much did we do to foster Arab Spring?). If the topic is about cyber attacks, the ethical implications arise primarily from two points: the inability to control the weapon once it's loosed, and the degree to which you could bring down the infrastructure of another country and cause widespread suffering—a basic WMD.

In terms of international law, there has been a long-recognized conflict between the principles of self-determination and non-intervention. If an indigenous group is struggling to achieve independence or self-government, then their rights could include demands for assistance from outsiders, who are then subject to accusations of interference in the internal affairs of another sovereign.[4]

---

[2] http://www.thelawfareproject.org/what-is-lawfare.html (last visited Oct. 14, 2013).

[3] http://www.law.cornell.edu/wex/slapp_suit (last visited Oct. 14, 2013).

[4] The ability of an outside nation-state to come to the assistance of a rebel group traditionally depended on the fuzzy line between "insurgent" and "belligerent." But in recent times, a debate has arisen over whether it is permissible to intervene on behalf of liberation groups (see Gray 2000, pp 45–50).

The most important statement of the International Court of Justice on these matters is still Nicaragua v. United States:

> A prohibited intervention must […] be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices.

The implication of this statement is that methods other than coercion would not be wrongful. Indeed, the basic prerogatives of "sovereignty" on the part of the interfering state would seem to support its right to use not just "diplomacy" or "propaganda" but any means short of force in pursuit of its own foreign policy. Indeed, hamstringing other states from pursuing their aspirations of global governance could run counter to the very idea of sovereignty.

So far, so good, as concerns "informational" exchanges and even disinformation. But what about "material support" of rebel groups? In the Nicaragua case, the U.S. was found to have interfered in the affairs of another nation by training and equipping the Contra forces. But what if the U.S. had merely supplied money and organizational assistance without the training and equipment? Is this level of "informational warfare" prohibited?

It is hard to believe that support of rebels, short of supplying arms, would be found unlawful for two reasons. First, there is the very pragmatic difficulty of trying to prove the case. Any clandestine operative worthy of the name would cover his/her tracks sufficiently to avoid obvious involvement in rebel movements. Despite the well-publicized accusations of U.S. interference in the Egyptian uprising, nothing very concrete can easily be laid at the feet of the American government.

Second, substantively supplying organizational services is closer to supplying information than it is to supplying arms. Supplying organization and information are both protected elements of free speech in the American system, at least until one reaches the level of supplying "expert advice and assistance" as those terms are defined in the "material support" of terrorism statutes.

In Holder v. Humanitarian Law Project,[5] the Supreme Court upheld a prohibition on providing "expert advice and assistance"[6] on the ground that it was possible to distinguish between providing "advice or assistance derived from scientific, technical or other specialized knowledge" from those types of support that are more general in nature. The Court argued that the plaintiffs' professed desire to train members of a designated foreign terrorist organization (FTO) in peaceful dispute resolution could promote the illegitimate aims of the organization by "buying time to recover from short-term setbacks, lulling opponents into complacency, and ultimately preparing for renewed attacks."[7] In turn, the proposal to teach FTO members on how to petition bodies such as the UN for relief might yield monetary aid that could then be redirected to fund the organization's violent activities. Finally,

[5] 130 S.Ct. 2705 (2010).

[6] 18 U.S.C. § 2339A(b)(3).

[7] 130 S. Ct. at 2729.

the Court made quick work of the freedom of association. The statutory scheme was distinguishable from the Communist Party cases on the ground that membership was protected. "The statute does not penalize mere association with a foreign terrorist organization," only the provision of material support to FTOs. The Court asserted that the "statute does not prohibit being a member of one of the designated groups or vigorously promoting and supporting the political goals of the group…. [It] prohibits the act of material support."

Applying these thoughts in the context of a criminal prosecution for "material support" is slippery enough, but taking them into the international arena seems utterly inappropriate. The corollary of the U.S. individual freedom of speech for a nation is the right to pursue its foreign policy. To pursue that policy by providing support and assistance—not technical training nor tangible goods such as arms and equipment—is within the basic definition of the nation-state.

Did the U.S. violate international law by assisting the organizers of protests and demonstrations in El-Tahrir Square? It would be extremely difficult to make that argument.

But is it permissible to fund the political campaign of a favored candidate in an election? Surely not. Despite the U.S. Supreme Court's obstinacy in thinking that money is protected speech, it is surely an unwarranted interference in the affairs of another nation to fund political campaigns. In fact, U.S. law makes it a crime for a "foreign national to contribute to a campaign in the United States".[8] Money is not the same as information or assistance.

On the other hand, individuals are not the same as governments. If a U.S. employee or contractor in Iraq or Afghanistan campaigns personally for either the incumbent or an opposition candidate, it is difficult to say that there is a violation of international law—violation of U.S. employment contracts, perhaps, but not international law.

Providing money to a partisan campaign is more akin to providing arms and equipment to the rebels. Indeed, since money is fungible, the Supreme Court has recognized that it can be criminalized as "material support" to a terrorist organization. As a practical matter, there is nothing to prevent money provided for campaign purposes from being used for purchase of arms. Even on a theoretical or ethical basis, there is a world of difference between personal service and money, especially given the enormous disparity in wealth between the U.S. and some of the nations whose elections it might wish to influence.

"Informational warfare?" There is nothing wrong with putting out information, even disinformation. There is nothing wrong with providing personal assistance to groups organizing to promote self-determination. But there is something very wrong with providing campaign money to candidates in other countries.

Now to return to the distinctions with which I began, both money and information are different physical invasion of electronic infrastructure. A cyber attack on another country's banking, electrical, or other utilities systems would be the modern equivalent of "armed attack," which is permitted only for defensive purposes. In-

[8] 2 U.S.C. § 441e.

deed, many observers worry significantly about both cyber attacks and EMP attacks that can take out a country's infrastructure and cause massive loss. This is not an attack by of use of information, but it is an attack on information itself—in this instance, the information base on which a modern country operates.

In sum, the rules regarding information and warfare depend very much on what is being attacked, by what means, by whom. An individual can spend her money as she wishes, and a government can pursue its own informational policies. But a government is constrained not to interfere in the internal affairs of another country. Meanwhile, a cyber attack on infrastructure would be subject to the ordinary rules of the Law of Armed Conflict (LOAC) and its defensive postulates.

4.2 Normative Challenges to Cyber Warfare

In this Sect. I examine the normative challenges of cyber warfare through a critical review of the moral permissibility of preventive war. I claim that any advocacy of preventive intervention, however constrained, could gain undue legitimacy, leading to more war, not less. My claim is based on two factors—one, the slippery transition from preemption to prevention and the other, that even a limited provision of preventive war for justified self-defense, construed as a rare exception, can lead to a rather open-ended advocacy and use of it in the hands of a powerful state. In the case of the "Bush doctrine," we see a mix of both. Though couched in the language of preemption to make room for unilateralism in the guise of preemptive self-defense, the doctrine embraces far-fetched preventive measures. Accordingly, the issue is the moral permissibility of preventive war, regardless of its scope and the circumstances. Indeed, the provision of preventive war in self-defense can get unduly interventionist, making the world less secure. Today's scenario of covert information warfare accentuates this prospect.

The most pronounced instance of the blurring of the distinction bewteen preemption and prevention is found in the Bush doctrine of 2002, largely in response to the September 11, 2001, terrorist attacks on the United States. The broad mandate of the Bush doctrine effectively makes the idea of "global safekeeping" an important part of national security strategy, giving the United States an open-ended unilateral license to respond militarily, in the name of "war on terror," to any acts or events in the world based solely on the internal perception of the United States.

Though most contemporary political and legal theorists advocating preventive use of force find the Bush doctrine too broad, they feel compelled to respond to the challenges of the changing nature of warfare in the twenty-first century. Consequently, the traditional debates of just-war have become a major focus of controversy in these defining years of unconventional warfare. A similar major turn in rethinking the just-war concerns occurred during the Second World War where the distinction between combatants and non-combatants blurred, making that war the first truly "total war." It compelled the Allied forces to navigate across a moral divide in deciding whether to undertake massive bombing of German civilian tar-

gets for military and strategic reasons. "I see this idea of just killing civilians and targeting civilians as being unethical—though the most unethical act in World War II for the Allies would have been allowing themselves to lose," says military historian Conrad Crane, quoted in the 2010 PBS Television's American Experience segment titled "The Bombing of Germany." We find the echo of Crane's words in Michael Walzer's classic restatement of the just-war doctrine. He writes: "But if there was no other way of preventing a Nazi triumph, then the immorality [of creating massive terror by targeting the non-combatant] …was also, simultaneously, morally defensible" (Walzer 2004, pp. 34–35). For Walzer, in cases of "supreme emergency," rules of war can be breached "when we are face-to-face not merely with defeat but with a defeat likely to bring disaster to a political community" (Walzer 2006, p. 268).

The just-war dilemma of the Allied leaders over bombing the German civilians was prompted by the German bombers attacking London for 57 consecutive nights, which indicates that the Allied response was directed at a "face-to-face" situation of dire catastrophe. The quandary facing today's political theorists who draw from the just-war tradition is provoked by a new set of challenges unique to the new century. The understanding of a "face-to-face" danger in today's world could take a whole new meaning in view of the unconventional nature of warfare and the specter of WMD. The question now is not only justifying first strike but deciding on how much in advance of the perceived threat, given the potential for catastrophic consequences if the threat is given the time to be carried out. The certainty factor of an imminent danger debated by the just-war theorists in the sixteenth and the seventeenth centuries is now put to severe test in view of this new challenge.

The situation is especially made complicated in view of today's scenario of cyber warfare in which a technologically advanced nation may undertake riskless covert warfare to thwart a perceived danger in another country in the name of preventive intervention for self-defense. As discussed in Sect. I above, supplying information is different from supplying arms, though both can be aimed at changing the direction of a conflict. The latter is a violation of state sovereignty and thus prohibited under international law. But covert cyber warfare is a most eggregious form of interference in the internal affairs of a state since it has the potential of bringing down the infrastructure of a country, but international law lacks specific guidelines regarding the rules of such covert operations. The morality of such warfare is also faced with unresolved issues if the imperative of self-defense is brought in as a justification for such intervention. Preventive intervention is a murky issue in the just-war thinking, so just-war doctrine does not provide much moral clarity in this debate. We may need to look elsewhere for moral guidance on this matter.

The blurring of the distinction between preemption and prevention is at the heart of the issue here. Advocacy of preventive war for justified self-defense, even when construed as a rare exception, can be rather open ended and liable to be misused. We see this in the Bush doctrine's espousal of unilateralism in the name of self-defense couched in the language of preemption, though it embraces far-fetched preventive measures. Legitimizing principled preventive war, however constrained, can give a powerful nation the moral license to expand the principle by pushing it in the direc-

tion of its own convenience. Yet some prominent contemporary just-war theorists who reject the Bush doctrine's expansive and reckless interventionism nonetheless advocate a limited provision of preventive war, even unilateral if warranted, for justified self-defense in cases of dire necessity. Their concern is to stay within the spirit of international law and devise means of accountability in offensive wars, with the goal of finding ways to respond to the new threats to peace and security posed by unconventional warfare and unconventional weapons systems. They rightly note that unilateralism in preventive ventures based on subjective and open-ended assessment of security threats can go horribly wrong in its calculations of anticipatory events and developments, and because it lacks political legitimacy and legal authority, it sets a dangerous precedent. In contrast, their provision for preventive use of force is primarily multilateral, guided by a mix of the just-war criteria and legal propriety, putting emphasis on collaboration whenever possible and citing the UN Security Council as the venue for open arbitration and debate for procedural legitimacy (Doyle 2008, Luban 2004, Buchanan and Keohane 2004). Their guidelines for assessing the gravity of the situation requiring prevention display a judicious blend of substantive and procedural considerations, including such factors as severity of threat, the likelihood of its occurrence, just-war criteria of legitimacy, and the legality of the threat and the proposed response.

Nonetheless, these guidelines are open-ended and can be misused. Just-war legitimacy criteria such as proportionality, necessity, and last resort are matters of disputation and prone to subjective interpretation, especially if a go-alone provision is allowed in the guidelines. Indeed, the just-war doctrine's major flaw is that it allows self-interested interpretation by the contesting parties (Myers 1996). The assessment of severity and likelihood of threat in anticipatory circumstances is no less subjective and open to mistakes or abuse. And the idea of legality is a moot question in claims of existential threat. As Michael Walzer has famously stated: "necessity knows no rules" (Walzer 2006, p. 254). Thus, these guidelines leave open the possibility that a powerful nation with global hegemony can construe them as an open-ended license to respond militarily, in the name of self-defense, to any emerging or anticipatory events in the world based on its own perception.

The prospect of cyber warfare compounds this problem. The growing reliance in modern warfare on information and communication technologies makes the blurring of preemption and prevention all too likely, thus accentuating unresolved moral and legal dilemmas of preventive war. There are several reasons for it. Unlike conventional warfare, regardless of its sophistication, virtual war offers the prospect of being risk free, instant, covert, and causing no immediate combatant and non-combatant injury on the enemy side. Though virtual war has the potential of making the entire infrastructure of a country dysfunctional, thereby causing untold suffering, it is still considered "clean" because it does not directly target people.

In the increasingly escalating use of drone attacks in the name of just-war where drones are often termed "moral predators," thus making obligatory their uninhibited use, unresolved moral and legal questions abound. Though drones are unmanned military robots and exemplify the advanced sophistication of military technology, they are still a step away from the specter of virtual war. Even then, deployment

of drones alters the reciprocal vulnerability of a conventional war and makes the asymmetries of power more pronounced by making military operations risk-free for the side using drones. This prospect has the likelihood of misuse of military options in the name of preventive intervention. In commenting on the frequent use of unmanned drones in today's US military combat overseas, Peter W. Singer writes:

> "And now we possess a technology that removes the last political barriers to war. The strongest appeal of unmanned systems is that we don't have to send someone's son or daughter into harm's way. But when politicians can avoid…the impact that military casualties have on voters and on the news media—they no longer treat the previously weighty matters of war and peace the same way." (*The New York Times*, January 22, 2012, Sunday Review)

In other words, risk-free combat technology can increase the likelihood of their use. In fact, one can make the more general claim that the permissibility of preventive use of force can make war all too tempting and frequent. This is especially true with the prospect of cyber warfare which is not only risk-free like drones, but also is instant, covert, and causes no immediate death on the other side. But all these features raise moral and legal conundrums. In essence, legitimizing preventive war, however constrained, can give a nation the moral license to expand the principle by pushing it in the direction of its own convenience. And if preventive war is made easy due to the use of cyber technology in military operations, then the chances are that much greater that the technology would be put to use in the name of preventive intervention. The certainty factor of an imminent danger, already compromised in the need for expanded preemption due to the presence of WMD in today's unconventional warfare, is now put to severe test in view of the new challenge of cyber warfare, making the claims of moral mandate in the slippery transition from preemption to prevention that much easier. But this trend is making the world progressively less secure. Neta Crawford's observation is worth noting here: "In sum, a preemptive-preventive doctrine moves us closer to a state of nature than a state of international law" (Crawford 2003).

The mindset of preventive war perpetuates the anxiety of living under the shadow of war, whereas "the stress of living in fear should be assuaged by true prevention—arms control, disarmament, negotiations, confidence-building measures, and the development of international law" (Crawford 2003, p. 36). These preventive measures are instances of proactive non-intervention that use the soft power of diplomacy and democratic collaboration. This may be a long and hard road that promises no quick results but, then, if we're looking for a fail-safe quick path to peace and security in today's murky and uncertain world, nothing can take us there. Preventive interventions make things only worse. We should pay heed to Grotius who said: "Human life exists under such conditions that complete security is never guaranteed to us."[9]

[9] Grotius (1625: 184), cited by Larry May in his chapter in Chatterjee (2013a). Portions of Section II are excerpted from Chatterjee (2013b).

References

Buchanan, Allen, and Robert Keohane. 2004. The preventive use of force: A cosmopolitan institutional approach. *Ethics and International Affairs* 17 (1): 1–18.

Chatterjee, Deen. 2013a. *The ethics of prventive war*. Cambridge University Press.

Chatterjee, Deen. 2013b. Enough about just war, what about just peace? The doctrine of preventive non-interverntion. In *The ethics of preventive war*, Hrsg. Deen Chatterjee. Cambridge University Press.

Gray, Christine. 2000. *International law and the use of force*. 45–50. Oxford.

Crawford, Neta. 2003. The slippery slope to preventive war. *Ethics and Interantional Affairs* 17 (1): 35.

Doyle, Michael. 2008. *Striking first: Preemption and prevention in international conflict*. Princeton: Princeton University Press.

Luban, David. 2004. Preventive war. *Philosophy and Public Affairs* 32 (3): 207–248.

Walzer, Michael. 2004. *Arguing about war*. New haven: Yale University Press.

Walzer, Michael. 2006. *Just and unjust wars: A moral argument with historical illustrations*. 4th ed. New York: Basic Books.

Myers, R. J. 1996. Notes on the just war theory: Whose justice, which wars? *Ethics and International Affairs* 10 (1), 115–130.