Chapter 5: State Sponsored Hacktivism and the Rise of 'Soft' War

George R. Lucas

INTRODUCTION

The focus of this essay is the phenomenon of "soft" war. This concept offers an obvious comparison with a concept now well-established in international relations: namely, "soft power" (Nye 2004), according to which diplomacy, trade agreements and other policy instruments may also be used, alongside or in lieu of threats of military force or other "hard-power" (kinetic or forceful) measures, in order to persuade adversary nations to cooperate more readily with any given state's strategic goals.

"Soft war" (or "unarmed conflict), by analogy, is a comparatively new term designating actual warfare tactics that rely on measures other than kinetic force or conventional armed conflict to achieve the political goals and national interests or aspirations for which wars (according to Clausewitz [1830] 1976) are always fought. Importantly, I will argue that "soft war" is fully equivalent to what Chinese military policy strategists earlier deemed "unrestricted" warfare: i.e., "warfare" carried out within domains in which conventional wars are not usually fought, employing measures not previously associated with the conduct of war (Lo 2012; Liang and Xianangsui 1999). Cyber conflict one type should be included within the purview of "soft" or "unrestricted" warfare, but the particular kind I describe here is *not* the "effects-based" conflict like Stuxnet, nor the kind of "cyber Armageddon" long predicted by analysts like Richard Clarke (Clarke 2010; Brenner 2011). Instead, it is a distinctive type of conflict that has evolved to dominance in their place: a phenomenon I label "state-sponsored hacktivism." To clarify this claim, I begin with a background review of malevolent activities in cyberspace itself.

A BRIEF HISTORY OF CYBER CONFLICT (OR MALEVOLENT ACTIVITES IN THE CYBER DOMAIN)

Not so long ago, cyber "activism" (on the internet, at least) was limited to pranks, practical jokes, and random acts of vandalism carried out by individuals or perhaps small groups or "gangs." Pranksters attached software "viruses" to emails that, when mistakenly opened, quickly spread through an organization's internal network, posting goofy messages and perhaps even erasing valuable data or software store on hard drives. Cyber vandals posted offensive messages or unwanted photos, or otherwise defaced an organization's website for no apparent reason. About the only crimes committed in those early days were trespassing (technically, by "invading" a private company network or an individual's computer itself) and destruction of property. Apart from mean-spiritedness or a perverted sense of humor, however, about the only reasons given for such malicious activities were a collective grousing by disaffected programmers and computer "geeks" about the monopolistic practices, and mediocre software distributed by Microsoft Corporation (Greenberg 2012).

Malicious behavior in the cyber domain, however, quickly evolved into a variety of more serious and sinister activities. On the one hand, it was not long before sophisticated individuals and criminal gangs exploited the very same software vulnerabilities as did the pranksters, but did so in order to steal bank deposits, credit card numbers, or even one's personal identity. On the other hand, cyber "activism" itself likewise evolved into ever more sophisticated acts of political sabotage: defacing or even temporarily shutting down government or commercial web sites with so-called "DDoS" attacks (distributed denial of service), dispatching software "worms" that traveled from computer to computer, penetrating each machine's firewall and virus protection software in order to gain control over the PC's or laptops themselves, transforming each into a "bot" (from "robot") or "zombie" (indicating the transfer of control and agency from the original owner/operator to a remote hacker). These individual machines were then remotely networked with others into a massive "botnet" controlled by political dissidents or criminal organizations, who, in turn, used them to launch

DDoS attacks on banks and financial institutions and divert their funds to secret accounts.

"Hacktivism" is a term that came into somewhat indiscriminate use to classify all these distinctive and diverse acts of malevolence and mischief in the cyber domain, ranging from straightforward crime and vandalism, to many forms of political protest carried out on the internet. Technically, the "hacktivist" is one who engages in vandalism and even in criminal activities in pursuit of political goals or objectives, rather than simply for personal satisfaction or financial gain. Early on, the term designated solely the internet activities of individuals and dissident groups (and was not applied to the activities of nations like China or North Korea, or terrorist groups like Hamas). Well known individuals (like Julian Assange of Wiki Leaks) and loosely-organized groups like Anonymous, LulzSec, and "Cyberwarriors for Freedom," resorted to internet malevolence to publicize their concerns, or otherwise further their political aims. These concerns ranged from personal privacy, liberty, and freedom of expression to opposition to political regimes like Syria or Egypt.

There are many ways of carrying out "hacktivism." I find it useful to focus upon the political goals of the "hacktivist" (as opposed to the financial interests of the conventional criminal). These political goals can be categorized as: transparency, whistle-blowing, and vigilantism. WikiLeaks purports, for example to provide greater <u>*transparency*</u> regarding the otherwise covert activities of government and large corporate organizations. The actions of <u>*whistle-blowers*</u> (like U.S. Army Private Bradley (Chelsea) Manning, and NSA Contractor Edward Snowden), somewhat in contrast, aimed specifically to expose what each individual took to be grave acts of wrong-doing or injustice on the part of the U.S. government or military (in these specific cases).

The <u>*internet vigilante*</u>s like "Anonymous," for their part, are a bit harder to pin down, since the loosely organized federation's individual members espouse a wide variety of disparate causes. The organization's behavior in response to each chosen cause, however, clearly involves taking the law (or, in its absence, morality) into the group's hands unilaterally. That is, based upon their shared judgments regarding immoral or illegal behavior by individuals, organizations, or governments to whom the group objects, the group launches attacks against selected targets ranging from the Syrian government of Bashir al Assad (for engaging in massive human rights violations), to organizations and individuals who might be engaged in perfectly legitimate security and defense operations to which members of Anonymous nevertheless object (Knappenberger 2012).

This is vigilantism. And, as its name suggests, the members of Anonymous cannot easily be traced or held accountable for their actions. As in all instances of conventional vigilantism, the vigilante's judgment as to what or who constitutes a moral offense is deeply subjective, and often wildly inconsistent or otherwise open to serious question.

Importantly, in all cases involving transparency, whistle-blowing and vigilantism, the *burden of proof* is on those who deliberately violate fiduciary duties and contractual (legal) agreements into which they may have entered, or who disobey or flout the law itself, in order to expose or protest against activities they deem to be even more egregious than their own actions. Such actions constitute important forms of democratic moral discourse in what Jürgen Habermas termed "the public sphere" (Habermas 1991; Calhoun 1992). This comparative judgment on the part of the protestor or whistle-blower, for example, is technically known as "the Principle of Proportionality." It demands of them that the degree of harm brought about through their own actions be *demonstrably less* than the harm already done by others to which they seek to call attention, or bring to a stop. The problem is that this comparative judgment is notoriously difficult to make. Vigilantes often exaggerate or misrepresent the harm against which they protest, and seriously underestimate the effects of their own activities on public welfare.

Otherwise, the remaining difficulty with such actions is that there is no independent or adversarial review of these decisions. According to what is likewise termed the "Principle of Publicity" or the Principle of Legitimate Authority, the final authority to evaluate the legitimacy of the protestor's or dissident's actions rest not with that individual or dissident organization, but with the wider general public, in whose collective interest the individual purports to act. So, in all these cases, it must be possible in principle to bring the individual dissident's actions and intentions before an impartial "Court of Public Opinion" for independent review (O'Neill 1986; de Oliviera 2000). The last criterion is the one most frequently ignored, and most often failed by both vigilantes and would-be whistle-blowers. They are prone to suffer from an abundance of self-righteousness.

THE ADVENT OF STATE-SPONSORED INTERNET ACTIVISM

Having established this context for the discussion of cyber hacktivism generally, what now are we to make of its most recent evolution: namely, the rise of state-sponsored or government "hacktivism?" Nations and governments are entering the cyber fray alongside private groups, either attempting to combat or shut down other hacktivists and stifle dissent within their own borders, or instead, to pursue political objectives against other states that were traditionally resolved through diplomacy, economic sanctions, and finally, a resort to kinetic force. *Many states at present appear to be resorting to massive cyber-attacks instead.* Such nations are thought to include pro-government groups or organizations in China (e.g., PLA Shanghai Unit 61384), the Russian Federation, and especially North Korea.

A recent high-visibility example of such state behavior was the apparent attack by North Korean operatives on Sony Pictures, over the pending release of the movie comedy, "The Interview." Never (it was frequently remarked) had such a bad movie received such first-class publicity (e.g., see: Neumaier 2014; Burr 2014; Kelner 2014). The entire affair seemed itself almost comedic, save for the important principles at stake: interference in the internal affairs of another nation, freedom of expression, violations of personal privacy for foreign state purposes. The kind of extortion and blackmail involved, and its impact on corporate and individual behavior in a sovereign land, might not have seemed so funny in alternative circumstances. The U.S. thus treated this instance of massive, state-sponsored hacktivism as a serious act of international conflict.

In other, earlier instances: the “Russian Business Network,” a branch of organized crime in the Russian Federation, is believed to have cooperated with the government in launching a preemptive cyber-attack on government organizations and military sites in the Republic of Georgia in 2008, prior to a conventional Russian military incursion into the breakaway Georgian province of Ossetia (Harris 2014). The U.S. indicted five members of the PLA Shanghai unit by name in the spring of 2014, for having been responsible for massive thefts of patents and trade secrets from U.S.-based aerospace and defense industries (DOJ 2014). The indictments were not expected to result in actual arrest and prosecution, but were intended instead to send a message to the Chinese government that its disavowal or denial of state accountability for these crimes under international law was no longer plausible.

One of the most interesting of these earlier developments was the work of “Cyber Fighters of Izz ad-Din al-Qassam,” an organization that takes its name from a prominent early 20th-century Muslim cleric and anti-colonialist. In 2012, on the anniversary of the 9/11 terrorist attacks in the U.S., this group allegedly carried out a massive DDoS attack on U.S. financial institutions. The attack was described in a Twitter post by the group as having been launched in retaliation for the continued presence on YouTube of the American-made film, “The Innocence of Muslims,” which portrays Islam and the prophet Mohammed in a very scandalous and unflattering light. The group vowed to continue the attacks until the offending film itself was removed from the Internet.

Two things stood out regarding the resulting, very serious disruptions of American financial institutions. First, despite its claim of independence, the group's attack was not indiscriminate. The institutions targeted were primarily those that had complied with the terms of the ongoing U.S. economic sanctions against Iran. In particular, the group's demand that a film be censored on account of its political or religious content seemed hollow: their leaders had to know that this was a demand that was beyond the power of a democratic government anywhere to grant, even were they willing in principle to comply with this demand.

The second oddity was that the anonymous Twitter site from which this group issued its September 2012 proclamation turned out to be the same account from which messages had flowed a few weeks earlier (allegedly from another vigilante group entirely) in the aftermath of a massive cyber-attack on the internal computer network of ARAMCO, the Saudi Arabian oil giant. Those attacks, on 15 August 2012, allegedly carried out by an organization calling itself the "Cutting Sword of Justice," erased data on all affected computer drives, and inserted in their place the image of a burning American flag. U.S. security officials seemed quite certain that the first of these attacks was an act of retaliation by Iranian agents in response to the damage done to their own nuclear and oil infrastructure by Stuxnet and Flame, respectively, both weapons attributed to (but never acknowledged by) the U.S. and Israeli governments.

Suppose all these allegations and counter allegations are true: in particular, suppose that the two attacks in close sequence in 2012 (and others since) were not carried out by distinct and independent organizations, but instead represent the coordinated actions of a state government (Iran), retaliating for similar attacks upon its cyber infrastructure by other states (Israel and the U.S.). Add to these the known and ongoing, state-sponsored, malevolent cyber activities of the People's Liberation Army in China, the "Russian Business Network," and

North Korean operatives. The conclusion is that states, as well as individuals and dissident groups, are now directly and deeply involved in hostile activities that increasingly transcend the boundaries of traditional espionage, covert action, and the "dirty tricks" of the past. Rather, this ongoing, high-stakes, but low-intensity conflict carried out by states against one another has evolved into what a number of experts (e.g., Gross 2015) are coming to call "soft war."

CYBER HACKTIVISM AND "SOFT WAR"

By analogy with the concept of "soft power," soft war is a mode of warfare or conflict that is intentionally non-kinetic: i.e., it does not entail the use of conventional weapons, or the destruction that accompanies conventional armed attacks. But it is a disruptive new innovation in international conflict, and *it is still a very grave matter*. As the cases cited above demonstrate, "soft war" cyber-attacks – state-sponsored hactivism – can do real damage, and inflict genuine harm, although rarely (in contrast to the case of Stuxnet) does this involve causing real physical harm to physical objects. Rather, the conflict results in loss of information, loss of access to information processing, and an inability to carry out essential activities (such as banking, mining, medical care, trade, and commerce) that rely largely upon information processing. Why bother to pursue the risky and wantonly-destructive traditional strategic objectives of conventional warfare that Clausewitz describes as "destroying the enemy's army, occupying his cities, and breaking his will to resist" when the strategic objectives can be met instead by rendering the enemy's armies inoperable and non-functional, bringing his cities' commercial and civil activities to a standstill, and forcing his military leaders to commit suicide when they are "doxed," or "outed" to their families and the wider public on Ashley Madison?[1] The harms inflicted through "state-sponsored hacktivism" may be

[1] This infamous "dating" website actually promoted and facilitated adultery, including among highly-positioned MPs in the U.K. Belgium, France, as well as members of Congress and the

far more precise and less genuinely destructive than their conventional counterparts, even those inflicted through "effects-based" cyber warfare. But they are every bit as effective, destructive to those whose lives and careers they destroy, and are far easier for adversaries and rogue states to master and utilize than the sophisticated techniques of "effects-based" cyber warfare (Lucas 2016).

Unlike the highly-publicized concept of a "cyber war," however, *the weapons and tactics of "soft war" are not limited to the cyber domain.* They can involve state use of the media, including cyber social media as well as conventional media, for purposes of propaganda, confusion, obfuscation, and disinformation. Soft war could involve the use of non-lethal (or "less-lethal") weapons in conventional attacks. For terrorist "pseudo-state" groups like Hamas, soft war could involve forms of what has elsewhere been called "lawfare," (for example) using civilian volunteers as "human shields" to deter conventional attacks on physical infrastructure or military installations by adversaries, one among a range of non-violent tactics termed "lawfare" (Dunlap 2011): e.g., using the law itself (in this instance, the Law of Armed Conflict) to thwart an adversary. Cyber tactics are only some of a range of options employed in the deliberate waging of so-called "soft" war.

The evolution of cyber conflict itself toward the "soft war" model of hacktivism, specifically, is quite different than the full-scale, effects-based equivalent of cyber "warfare"

military in the U.S. The "hacking" of its discrete and highly confidential clientele database was featured in the Times of London and the New York Times, not to mention Rupert Murdoc's tabloids during the summer of 2015. See, for example: Dino Grandoni, "Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions," The New York Times (July 21, 2015): B3. Posted 20 July 2015: http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html [accessed June 27, 2016].

predicted by many pundits (such as Richard Clarke 2010 and Joel Brenner 2011) during the last decade. The much-touted "cyber Armageddon," or "cyber Pearl Harbor" was to be a massive disruption and destruction of conventional systems, like air traffic control and electrical grids, resulting in widespread death and destruction on parallel with a massive conventional war. But state-sponsored vigilantism and hacktivism appear to signal something quite distinct from this familiar, but often highly exaggerated and implausible scenario. This state-sponsored conflict is virtual, not physical; non-violent, rather than kinetic; but nevertheless quite destructive and malevolent in other respects, equally capable of causing massive social upheaval, or bringing about a "death by 1,000 cuts" through pilfering of industrial and state secrets, or by interference in trade, commerce, finance, medical care, and transportation.

And, just as with increased reliance on the exercise of "soft power" (diplomacy, sanctions, media relations and the like), the advent of "soft war" has distinct advantages for those nations that engage in it. Essentially, *this kind of warfare proposes to substitute cleverness and ingenuity for brute strength.* It is less costly to wage, less destructive of property, of lives, and of national treasure (as well as international prestige). Yet it is quite capable of achieving the same political goals, when properly utilized, as "hard" kinetic war, as well as capable of undermining or fending off an adversary that relies solely upon "hard" war tactics. It is, in short, the equivalent of bringing Asian martial arts that rely on balance, timing, and tactical sophistication to bear upon an enormous, powerful, but wholly conventional bully. The martial arts expert can hold his or her own, and even prevail, even though smaller, lighter, and perhaps less physically strong than the bully.

This comparison is apt, since "soft" war is directly attributable to two Chinese military strategists, reflecting on the future of military conflict in the aftermath of the lopsided victory of U.S.-led coalition forces in the 1991 Gulf War against the conventional forces of Iraqi

President Saddam Hussein. In a landmark essay in 1999 cited earlier, entitled “Unrestricted Warfare,” two senior colonels in the People’s Liberation Army, Qiao Liang and Wang Xiangsui, argued that the U.S. had become an international bully, physically too strong and too reliant on extensive war-fighting technology to resist by conventional means. Instead, they proposed, new forms of conflict needed to be devised, more indebted to subtleness and cleverness than to brute force, in the spirit of Sun-Tzu, in order to effectively oppose the brute physical power of the American “hegemon.”

There is no explicit regime under international law that specifically governs this kind of conflict. Ought there to be? Or is it sufficient to rely on state interests, and the norms emergent from accepted state practice, to serve as a guide for when, and for how, to engage in “soft war?” Ought the same or similar guidelines applicable to kinetic war also guide entry into and conduct during this “soft” mode of warfare as well? Or ought it to remain, as its original formulators speculated, “unrestricted” or “without bounds?”

In the accounts of conventional hacktivism above, I used terms like “proportionality,” “publicity,” and “legitimate authority” advisedly to describe ways in which vigilante groups like Anonymous, or whistle-blowers like Manning and Snowden, might be determined to have gone astray in their otherwise well-intentioned cyber activities. In a manner similar to earlier discussions of *jus ad vim*, the morally justified use of force generally (e.g., Brannstetter and Braun 2013; Ford 2013): might we now reasonably require that states only engage in such conflict when presented with irreconcilable differences sufficiently grave to justify conventional use of force (as, admittedly, happened on both sides of the Iran/U.S.-Israel dispute over Iran’s nuclear weapons program)? And ought we to demand or reasonably expect that, when faced with the alternative of resorting to “soft” or kinetic warfare to resolve such disputes, that (consistent with a Principle of Last Resort), not only should all viable and reasonable alternatives short of war be attempted, but that the “soft war” alternative should always be chosen in lieu of the conventional resort to the use of kinetic force? Perhaps most importantly, might we demand, or reasonably expect, that nations engaging in such conflict with one another should do their utmost to avoid deliberate targeting of purely civilian, non-combatant individuals and their property, as is legally required in conventional war? Or, as in the example of using volunteer civilians as human shields, should attacks on financial institutions or civil infrastructure that merely involve a denial of access or service be subject to a more tolerant regime in which the combatant-noncombatant distinction is less viable, and perhaps less significant?

"SOFT WAR" AND "SOFT" LAW (ETHICS)

The foregoing are chief among the questions waiting to be addressed and clarified in the wake of the advent of “soft war” generally, and specifically in the aftermath of the increased resort by state-sponsored agents to the kinds of tactics once limited to dissident individuals or non-state groups. While the lion’s share of such normative work has occurred within the context of existing international law (most notably, the *Tallinn Manual* [Schmitt 2013]), that legal framework will simply not suffice to provide reliable guidance in this new domain of conflict. There are a number of reasons for this skepticism (see Lucas 2016, ch. 3).

Contributors to the *Tallinn Manual* (Schmitt 2013), for example, including some of the most eminent legal minds in the world today, brilliantly attempted to interpret and extrapolate existing international law (the regimes pertaining to armed conflict and humanitarian treatment of war’s victims, and those pertaining to criminal activity in particular) so as to bring existing legislation to bear upon conflict in the cyber domain. But as demonstrated in this essay, *“soft war” is not “war,”* strictly speaking, and so not subject to the jurisdiction of international legal regimes pertaining to armed conflict. Neither is it simply crime (although it sometimes involves the commission of otherwise-criminal actions by state agents). Nor can it be easily dismissed as merely the routine crimes committed by covert agents in the midst of conventional espionage operations (Rid 2013; Lucas 2016, chs. 1-2).

Finally, as noted above, "soft war" *includes, but is not limited to* the cyber domain. "Media war" is not "war," and it is also not limited to cyber conflict. Use of non-lethal weapons, or tactics of "lawfare" (including human shields) not only occur outside the cyber domain (and so are obviously not addressed within the *Tallinn Manual* [Schmitt 2013]), but (in the latter instance) are also designed precisely to frustrate the bright-line statutes of existing international law, turning the letter of the law against its underlying regulatory purpose. The same seems to be true, as Gross argues, of kidnappings and hostage-taking, when undertaken for political motives (Gross 2015).

Even within the cyber domain alone, "soft war" tactics there more akin to espionage than to war or crime, and thus, once again, not explicitly addressed in international law, nor are state parties to existing legal arrangements eager to see such matters addressed there. In fact, this is the chief obstacle to pursuing normative guidance through the medium of law: those who are party to the law, and whose consent would be required to extend or amend it, are deeply opposed in principle to any further intrusion upon their respective interests and activities through treaty or additional legislation. Insofar as international law rests fundamentally upon what states themselves do, or tolerate being done, this opposition to further legislation (the one issue in the cyber domain on which the U.S., Russia, and China seem to agree) seems a formidable obstacle to pursing governance and guidance through legal means.

This is not as unpromising as it might seem, however, when one recognizes the historical fact that the principle bodies of international law pertaining to conflict of any sort largely codify, after the fact, norms of certain kinds of practice that emerge from public reflection by the practitioners themselves upon the better and worse features of that practice, and upon the ends or goals ultimately served by these practices. Law and regulations give the appearance (at least) of being stipulative, and are thought to be imposed externally, often upon unwilling subjects or agents. Best practices, by contrast, *emerge* from the shared practices of the interested parties, and reflect their shared experience and shared objectives.

International law, seen in this light, is more properly understood as grounded in common accord, consensus, and voluntary compliance. Its inherently cosmopolitan character (often overlooked by politically-appointed "Committees of Eminent Persons," eager to impose their terms of behavior on others) instead reflects Immanuel Kant's conception of standards of regulative order that moral agents themselves have both formulated and voluntarily imposed upon themselves, in order to guide and regulate their shared pursuits. Their compliance with principles that they themselves have formulated is thus more feasible and readily attainable.

This is a somewhat prolix manner of expressing a doctrine known in international relations as "emergent norms." This concept is encountered more broadly in moral philosophy as a kind of "trial and error," experiential groping toward order and equilibrium, a process that Aristotle (its chief theorist) described generally as the methodology of the "imperfect" sciences. The moral philosopher, Alasdair MacIntyre, should be chiefly credited with having resurrected this methodology in the modern era, from whence we can discern it already at work in the cyber domain, as well as in the field of military robotics (e.g., Lucas 2014, 2015). Legal scholars, for their part, have dubbed this sort of informal and voluntary regulatory institution (as occurs in the Codes of Conduct of professional organizations, or the deliberations and recommendations of practitioners in the aftermath of a profound moral crisis) as constituting "soft" law.

What seems urgently required at the moment is a coherent and discernable body of "soft" law for "soft war." That is, the relevant stakeholders in the community of practice – in this case, frankly, adversaries engaged in the kind of low-intensity conflict that I have described under the heading of “soft” war – to formulate and publicize the principles that they have evolved to govern their practice. In earlier eras, like the Cold War, for example, espionage agents from adversarial nations evolved a sophisticated set of norms to govern their interaction and competition, designed largely to minimize unnecessary destruction, loss of lives in their respective clandestine services, mutual treatment of adversaries in captivity and prisoner exchanges, and other tactics designed to reduce the risk of accidental or unnecessary escalation of conflict (especially conflict that might cross the threshold of kinetic war in the nuclear era). All of these informal normative arrangements intended to facilitate, rather than inhibit, the principle aim or goal of espionage itself: reliable knowledge of the intentions and capabilities of the adversary. In the nature of things, there were no “councils” or “summit meetings,” and no published or publicized “codes of conduct.” Rather, these norms of prudent governance and guidance came to be “understood” and largely accepted (and complied with) by the members of this interesting community of practice.

What the broad outlines of the content of this “soft law” for “soft war” might be are already outlined above, utilizing somewhat more familiar “just war” terminology, which serves well for this purpose (Lucas 2016). Adversaries and stakeholders pursuing “soft war” have an interest, for example, in seeing that it does not accidentally “go kinetic,” or involve needless and unnecessary “collateral damage” to vital civilian infrastructure, especially of the sort that might lead to widespread physical destruction and loss of life. They share a common interest in proportionate response, and the dictates of military necessity, of the kind exhibited in the conflicts (allegedly) between the cyber warriors of Iran, the U.S., and Israel described above. And adversaries like the U.S., China, and the Russian Federation, still locked into a preliminary mode of “unrestricted” or limitless warfare, need to consult more directly and frankly than has been possible to date on where common interests lie in imposing boundaries and regulative order on their “soft” conflicts, before the incessant damage being done on an ongoing basis to all parties to these conflicts forces an escalation into something far more serious and irreparable.

I have deliberately confined myself to only one very prominent tactic in the arsenal of soft war more generally, in an effort to illustrate how cyber conflict itself is being assimilated less as a new and distinctive form of conflict, as a valuable tactic in a new form of warfare generally. I conclude on a positive note, by observing that this increased resort to “soft war” tactics, including (but not limited to) cyber conflict, holds promise that the very real conflicts and disagreements that have often led nations to make war upon one another may themselves evolve into a mode of authentic opposition and conflict resolution that nonetheless ends up resulting in dramatically reduced bodily harm and loss of life, while doing less damage -- and more easily reversible or repairable damage -- to the property of adversaries and innocents than was heretofore conceivable in conventional conflict.