

"Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets."

George R. Lucas, Jr.*

Abstract

Evaluations of cyber war and weapons range from denunciations of their widespread and indiscriminate destructiveness and deliberate targeting of civilian infrastructure, all the way to appraisals of cyber warfare as a morally preferable, less destructive alternative to conventional warfare. To achieve greater clarity, I distinguish permissible from impermissible forms of cyber conflict, as well as genuine cyber “warfare” from large scale criminal enterprises (including commercial and state-sponsored espionage) in the cyber realm. I criticize the lack of discrimination often encountered in the formulation of cyber strategy and development of cyber weapons, and argue in favor of international governance and guidance with reference to key just war principles of proportionality, discrimination, and last resort. This results in restricting the use of cyber weapons to justified military targets, with Stuxnet as a positive case study. In morality, we infer or derive operable constraints on, and guidelines for, acceptable practice by examining instances of what all agree is either good or bad practice. Likewise, in international law, we recognize the evolution of customary law through the accepted conduct of otherwise law-abiding states. On these grounds, and with reference to recent cases of cyber war, I argue that an act of cyber warfare is permissible if it aims primarily at harming military (rather than civilian) infrastructure, degrades an adversary’s ability to undertake highly destructive offensive kinetic operations, harms no civilians and/or destroys little or no civilian infrastructure in the process, and is undertaken as a “last resort” in the sense that all reasonable alternatives short of attack have been attempted to no avail, and further delay would only make the situation worse.

* George Lucas is Class of 1984 Distinguished Chair in Ethics at the Stockdale Center for Ethics, U.S. Naval Academy (Annapolis, MD), and Professor of Ethics & Public Policy at the Naval Postgraduate School (Monterey, CA). He is author, most recently, of *Anthropologists in Arms: The Ethics of Military Anthropology* (AltaMira Press, 2009), and editor and contributor to *New Warriors/New Weapons: Ethics and Emerging Military Technologies*, a special issue of the *Journal of Military Ethics* (9, no. 4: December 2010).

I.

Ours is the age of “cyber anxiety.” Pundits opine, especially in developed, highly industrialized countries, on the global vulnerabilities to cyber attacks or to acts of cyber terrorism. Cyber security, and fending off cyber crime, are a constant obsession and an ongoing concern. The potentially indiscriminate and uncontrollable aspects of cyber weapons, once unleashed in acts of terrorism or warfare, is the subject of grim and frightening prognostication.¹ In many respects, the fear of uncontrolled proliferation and widespread destruction from cyber warfare has come to occupy a place in the public mind very similar to the current fear of terrorist attacks, or even more to the threat of uncontrolled nuclear destruction that haunted public consciousness during the decades of the Cold War. The situation of the U.S. and its allies in Western Europe *vis a vis* potential adversaries (like China or the Russian Federation) has, indeed, been portrayed as analogous to the nuclear cold war: a proliferation and virtual “arms race” in the cyber arena, with only a presumed balance of destruction holding adversaries at bay.

Apart from the Convention on Cybercrime sponsored by the Council of Europe a decade ago,² however, not much progress has been made in the field of governance: that is, on discussions of the most likely ethical constraints on cyber conflict, or on the content of feasible treaties, or the formulation of bright-line statutes in international

¹ Former U.S. National Security Adviser, Richard A. Clarke, dramatically outlines the terrifying contours of an imagined, full-scale cyber attack on the United States at the conclusion of chapter two of *Cyber War: the Next Threat to National Security and What to Do About It*, co-authored with Robert K. Knake (New York: HarperCollins Publ., 2010): 64-68. This popular account of cyber vulnerability engages in all of the equivocation, confusing hyperbole, and threat inflation that I attempt to describe below.

² Council of Europe, “Convention on Cybercrime” (Budapest: November 23, 2001): <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.

humanitarian law, that might serve to limit or regulate some of the most fearful or destructive prospects attendant upon cyber weapons development or permissible cyber tactics and strategy. To date, the most detailed treatment of the ethics of cyber warfare has been the analysis of philosopher Randall Dipert of the University of Buffalo, writing in the December, 2010 issue of the *Journal of Military Ethics*,³ while from the perspective of domestic and international law, an extensive survey is offered by Steven G. Bradbury in his keynote address for the annual Harvard National Security Journal symposium, “The Developing Legal Framework for Defensive and Offensive Cyber Operations.”⁴ Dipert, in his own article, laments the relative lack of attention given to the ethics of cyber war, and cites a modest body of prior work in this field undertaken largely by computer scientists and defense policy analysts: Martin Libicki (RAND Corporation), Herbert Lin (AAS),⁵ and two of my colleagues at the Naval Postgraduate School, Neil Rowe and John Arquilla (incorrectly cited as Arguilla).

³ Randall R. Dipert, “The Ethics of Cyberwarfare,” *Journal of Military Ethics* 9, no. 4 (December 2010): 384-410.

⁴ Bradbury is the former head of the Office of Legal Counsel in the U.S. Department of Justice. His essay was the keynote address for the annual Harvard National Security Journal Symposium, “Cybersecurity: Law, Privacy, and Warfare in a Digital World” (4 March 2011), and is forthcoming in the *Harvard National Security Journal*. But see also: G. Darnton, “Information Warfare and the Laws of War”, in Halpin, E., Trovorrow, P., Webb, D., and Wright, S. (eds.), *Cyberwar, Netwar, and the Revolution in Military Affairs* (Houndsmills, UK: Palgrave-Macmillan, 2006): 139-156; Duncan B. Hollis, “New Tools, New Rules: International Law and Information Operations,” in *The Message of War: Information, Influence and Perception in Armed Conflict*, eds. G. David and T. McKeldin (2008); Scott J. Shackelford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,” *Berkeley Journal of International Law* 27, no. 1 (2008): 191-251; and most recently, Matthew C. Waxman, “Cyber-Attacks and the Use of Force,” *Yale Journal of International Law* 36 (2011): 421-459.

⁵ E.g., Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Corporation, 2009); *Conquest in Cyberspace: National Security and Information Warfare*, (New York: Cambridge University Press, 2007); and Herbert S. Lin *et al.*, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Research Council/American Academy of Sciences, 2009.

Rowe primarily discusses the status of cyber warfare and weapons with reference to current statuses of the law of armed conflict, and complains quite appropriately that many of the strategies and weapons for cyber conflict currently under development constitute potential violations of prevailing international humanitarian law (LOAC), in that they deliberately target, and aim to inflict widespread damage and suffering, and even injury and death, on civilian personnel and infrastructure.⁶ John Arquilla, who coined the phrase “cyber warfare” itself while at the RAND Corporation,⁷ also wrote what is likely the very first, and in my view, the most original and path-breaking article yet produced on “ethics and information warfare.”⁸ Like Dipert, Arquilla discusses principally the ethical issues, as opposed to the legal status, of cyber conflict, and runs its principal strategies and tactics through the lens of just war theory. I will return to Arquilla’s pioneering observations in conclusion.

Dipert’s more recent account of the ethics of cyber warfare, while certainly not the first, is surely the most complete and up to date ethical account from the standpoint of the current status of the technology of cyber conflict, and also the most thorough and fully informed analysis from the standpoint of philosophy, ethics, and particularly just

⁶ Rowe, Neil C., “War Crimes from Cyberweapons,” *Journal of Information Warfare*, 6: 3 (2007): 15-25; “Ethics of Cyber War Attacks”, in Lech J. Janczewski and Andrew M. Colarik (eds.) *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008): 105-111; “The Ethics of Cyberweapons in Warfare,” *Journal of Techoethics* 1, no. 1 (2010): 20-31. Rowe is Professor of Computer Science in the Department of Computer Science, Graduate School of Engineering and Applied Sciences (GSEAS), at the Naval Postgraduate School (Monterey, CA).

⁷ See his interview for PBS “Frontline” (March 4, 2003): <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>. Arquilla is Professor and Chair of the Department of Defense Analysis in the Naval Postgraduate School (Monterey, CA).

⁸ John Arquilla, “Ethics and Information Warfare,” in *The Changing Role of Information in Warfare*, eds. Z. Khalilzad, J. White, and A. Marsall (Santa Monica, CA: RAND Corporation, 1999): 379-401. More recently, see “Conflict, Security, and Computer Ethics, in the *Cambridge Handbook of Information and Computer Ethics*, ed. Luciano Floridi (New York: Cambridge University Press, 2010): 133-149.

war theory.⁹ In keeping with what many other analysts concluded over the past decade with respect to the topics of terrorism, counterinsurgency, and irregular warfare, Dipert concludes likewise in the case of cyber conflict that the tactics and weapons of cyber warfare are such as to render traditional law and morality obsolete, or at least, largely inapplicable. His overall conclusion is that cyber conflict is so utterly unlike conventional war, and its weapons and tactics so novel and unprecedented, that an entirely new regime of governance is called for. He thus echoes, and indeed, fans the flames of public anxiety over this mode of conflict.

For my part, I do not doubt the gravity of the threat (as Arquilla described it over a decade ago, for example, in an interview for the PBS news program, *Frontline*), nor do I dispute the seriousness of the concerns that Randall Dipert now raises and discusses. I do think, however, that this topic presently suffers from a certain amount of confusion, hysteria, and threat inflation.¹⁰

It is certainly true that cyber conflict is, like IW and terrorism, a substantial challenge to our conventional thinking about war and armed conflict, and will certainly call for some disciplined and careful analysis, and some constructive efforts to meet the

⁹ Thus, see also Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *jus in bello*," *International Review of the Red Cross* 84, no. 846 (June 2002): 365-399.

¹⁰ See, for example, the treatments of this topic by highly respected journalists: James Fallows, "Cyber Warriors," *The Atlantic Monthly* (March 2010): 58-63; and Seymour M. Hersh, "The Online Threat," *The New Yorker* (1 November 2010), both of whom echo the concerns of Clarke and Knake, cited above (n.1). Since first writing and delivering this address at a UNESCO-sponsored conference on cyber security at the University of Hertfordshire (U.K.) on 1 July 2011, a very thoroughly documented and persuasively-written article by Thomas Rid of Kings College (London) has appeared in the *Journal of Strategic Studies* (5 October 2011), forcefully arguing similar points about conceptual equivocation and threat inflation in the discussion of cyber war: see "Cyber War Will Not Take Place," *Journal of Strategic Studies*, DOI:10.1080/01402390.2011.608939. Available at <http://dx.doi.org/10.1080/01402390.2011.608939> Rid goes even farther than I to claim that cyber "warfare," properly speaking, has never occurred and likely will not occur, and that what is being discussed (and "hyped") under that heading are actually internet versions of sabotage, espionage, and subversion. I think this view overly restrictive, in that it does not give credence to various forms of grave and serious harms that might be done to individuals and states that are nonetheless technically "non-lethal."

challenge of effective governance in the near future. The fear that we might unwittingly or inadvertently unleash a widespread and unrestrained, and highly destructive conflict in the cyber arena, in particular, as an act of war is a very real concern. But public discussions, including the essays I have cited, often fail to distinguish, or even attempt to distinguish with sufficient care, between different kinds of cyber conflict:

- (1) what might be called cyber *vandalism* (a hacker breaking into, and lurking in defense information systems);
- (2) acts of cyber *crime* (in which data are damaged or stolen, or services denied, for personal or corporate gain);
- (3) cyber espionage (what might be accurately described as acts of cyber vandalism and cyber crime carried out by states or commercial corporations);
- (4) cyber *terrorism* (in which all of the foregoing things, and also damage and destruction to physical infrastructure are inflicted by aggrieved non-state agents in order to sow fear and confusion, and inflict widespread physical suffering upon random victims); and
- (5) genuine acts of cyber *warfare*, in which the latter sorts of things (physical damage, causing death, destruction, and widespread physical suffering) are done deliberately, to specified adversaries, in pursuit of political objectives or conflict resolution by states, governments, and their military and intelligence forces.¹¹

In passing, let me quickly remark that I am of the opinion that *the threat of cyber terrorism, in particular, has been vastly overblown*. Unlike IW and conventional acts of terrorism generally, genuine cyber *warfare* turns out to be a very expensive, labor intensive, and therefore remains a highly state-centric enterprise. Terrorists can engage in vandalism and crime, and have used the internet to great advantage for the purposes of conventional propaganda and disinformation. But they cannot easily develop true cyber weapons, or engage in acts of cyber warfare – nor have they yet been detected as doing so, or even trying to do so. To be blunt: neither the 14-year old hacker in the next-door

¹¹ Thomas Rid (preceding note) defines cyber war as “potentially lethal, instrumental, and political act of force conducted through malicious code.” Once again, however, what requires further explication is the nature of harm that can be suffered in a cyber attack, and whether forms of such harm that are technically non-lethal are still of sufficient gravity to warrant classification as acts of war (given that acts of sabotage are currently understood to constitute acts of war).

neighbor's upstairs bedroom, nor the two- or three-person al Qaeda cell plotting from a tiny flat in Hamburg, are going to bring down the Glen Canyon and Hoover Dams. And that offers occasion for modest hope.

II.

For the moment, I want to make a somewhat provocative case that *there are acceptable forms of cyber conflict and cyber warfare* that can be justified from the standpoint of just war theory. Indeed, such cyber conflict (as Neil Rowe has allowed) may in some instances be preferable to conventional war, and even to alternative forms of conflict resolution (such as economic sanctions), if properly conducted.¹² I also want to remark that our actual experience of cyber warfare to date (and there have been several military strikes by governments), has not been all that bad, and is likewise such as to offer hope that the worst fears regarding cyber conflict may be somewhat exaggerated. Indeed, I think it is possible on the basis of experience to distinguish between morally justified and unjustified forms of cyber conflict, and to discern, quite remarkably, that those cyber strikes that have been conducted within the current constraints of law and morality (e.g., with respect to the prevailing principles of the law of armed conflict) have also, to date, proven more effective than those that potentially represent the commission of war crimes.

Let me begin with two cyber attacks of military significance, at least one of which may illustrate indiscriminate and disproportionate targeting of civilian infrastructure.

¹² See Neil C. Rowe, "Towards Reversible Cyberattacks" (unpublished draft: available on the website of the Consortium for Emerging Technologies, Military Operations, and National Security (CETMONS): http://cetmons.org/files/documents/library/thrust5_cyberattacks.pdf. [accessed 15 July 2011])

These two attacks were presumably unleashed by the Russian Federation against nearby adversaries in Estonia (in April, 2007) and once again in Georgia (in July-August, 2008). The first instance was basically a “distributed denial of service” (DDOS), overwhelming and shutting down virtually all internet-based services in a sophisticated country dominated by paperless government and heavy reliance upon internet financial transactions.¹³ A DDOS attack began around 20 July 2008 in Georgia, when “botnets” from all over the world began blasting Georgian computer services and networks with enormous amounts of useless data, much of which was eventually traced back to the RBN (Russian Business Network), an organized crime unit of Russian mafia. This was a prelude to conventional bombing and perhaps also intended as a prelude to full scale cyber-war (that was not carried through). The attribution of cyber attacks is, of course, a well –known problem, and no official source in Russia has ever admitted complicity in either case. What is significant, however, is that both strikes were acts of preemptive aggression, in that both were apparently responses to ordinary political actions by the eventual victim or target state that did not rise to the accepted level of *causus belli* in international law. Even more significantly, the Estonian strikes relied almost exclusively on targeting civilians and civilian infrastructure, while the prelude attack in Georgia targeted primarily government offices and military defense systems, effectively shutting

¹³ An excellent summary of the circumstances leading up to the attack on Estonia and its consequences can be found in Episode 2, Season 1 of the PBS program, “Wired Science” from shortly after the incident in 2007, entitled, “Technology: World War 2.0” at http://xfinitytv.comcast.net/tv/Wired-Science/95583/770190466/Technology%3A-World-War-2.0/videos?skipTo=189&cmpid=FCST_hero_tv. See also Charles Clover, “Kremlin-backed group behind Estonia cyber blitz,” *Financial Times* (London: 11 March 2009), and Tim Espiner, “Estonia’s Cyberattacks: Lessons learned a year on,” *ZD NET UK* (1 May 2008). For an analysis of the attack against Georgia, see E Tikk, K. Kaska, K. Rünneri, M. Kert, A-M. Talihärm, and L. Vihui, “Cyber Attacks Against Georgia: Legal Lessons Identified” (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2008); and the United States Cyber Consequences Unit (US-CCU), “Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008”, US-CCU Special Report (August, 2009), available at: www.usccu.org.

down coordination between the government and its military in Georgia. In neither case was extensive permanent or long-term damage done, nor injuries sustained, nor to my knowledge were lives directly lost as a result.

It is difficult to gauge the effectiveness of the Estonian attacks, which certainly seemed to constitute some sort of retaliation for the government's decision to move a Russian war memorial statute from the center of the capital to a less prominent military cemetery, and to be further undertaken in support of the massive demonstrations and arrests of Russians living in Estonia that followed. The tensions gradually subsided. The Georgian attacks, by contrast, seem to have constituted more a prelude or warm-up for conventional armed intervention: the first time, according to a NATO Cyber Defense study, that a conventional attack was deliberately preceded by a cyber attack,¹⁴ which apparently served to prepare the way for Russia's subsequent conventional armed intervention in South Ossetia. Both attacks, from a political perspective, caused a great deal of resentment, and inflamed hostilities, making a political solution to either conflict relatively unlikely.

In light of the widespread and witheringly indiscriminate attack on civilians and civilian institutions, Estonia requested at the time that NATO recognize a violation of sovereignty, so as to trigger the collective self-defense provision of the NATO treaty. Interestingly, that suggestion was rejected at the time on the grounds that "a cyber attack is not a clear military action."¹⁵ In the second case, somewhat in contrast, the preparatory

¹⁴ E Tikk, K. Kaska, K. Rünneri, M. Kert, A-M. Talihärm, and L. Vihui, "Cyber Attacks Against Georgia: Legal Lessons Identified" (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2008): 5. The apparent Israeli attack on a Syrian nuclear facility in the fall of 2007, however, predates this event, and likewise constituted the coordination of cyber and conventional weapons.

¹⁵ Major Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64, no. 121 (2009): 144-145. Quoted in Steven G. Bradbury, "The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal*

cyber attack on government offices and military installations assuredly aided the success of the conventional intervention and occupation. In neither of these known cases did the cyber strategy address, alter, or otherwise remedy or resolve the underlying political conflict. I would accordingly be inclined to describe the indiscriminate and disproportionate attack on Estonia as an “unjust” cyber attack, in that it both lacked a sufficiently grave “just cause” (*causus belli*), and directly targeted civilians and civilian institutions indiscriminately and disproportionately, in violation of the international law of armed conflict. By contrast, the cyber attack on Georgia was part of a legitimate political disagreement between two sovereign nations over control of territory deemed important to both, conventionally taken to be a legitimate cause for the use of force when attempts at diplomatic solutions are unsuccessful. Moreover, the cyber attack was aimed primarily at disabling the opposing government’s military capacities of command and control. No explicitly civilian infrastructure (nor civilians themselves) were deliberately targeted. This strikes me as a justifiable use of cyber weapons in accordance with the constraints of LOAC as conventionally understood.

Israel apparently likewise preceded its devastating F-15 air strikes against a secret Syrian nuclear facility near Dayr az-Zawr on 6 September 2007 with a full-scale cyber attack that managed to completely disable Syria’s extensive, Russian-made anti-aircraft defense system, though once again the details are murky, and formal attribution has never been made or acknowledged. In this case, as in the Georgian case, the preemptive cyber strikes were directed entirely against military targets: radar and air defense systems, much as a conventional attack might have been, enabling Israeli fighters to penetrate

(forthcoming). Keynote address for the annual Harvard National Security Journal Symposium, “Cybersecurity: Law, Privacy, and Warfare in a Digital World” (4 March 2011).

deeply into Syrian airspace with little resistance. Unlike the conventional attacks that followed (in which several persons, allegedly including a number of North Koreans, were killed), however, the cyber attack attained the military objective of rendering defensive forces helpless, without widespread destruction of property or loss of life on either side.¹⁶ Especially because it was clearly a preemptive cyber (and conventional) attack, the extent of its justification depends heavily on the nature and imminence of the threat of harm (which was likely considerable), and the extent to which appropriate diplomatic means were first tried and exhausted. On the basis of the historical and political considerations at stake in otherwise permitting Syria and North Korea to engage in a clandestine violation of the international nuclear non-proliferation treaty, I am inclined to judge that this focused attack on an adversary's illicit military installation was justified.

III.

These three cases, the details of which are by now reasonably well established in the public (non-classified) record, together offer an important set of evaluations that I want to take up with respect to some of the core criteria of just war theory. Specifically, I want to invoke the key criteria of “just cause” and “last resort” with respect to the justification of war (*jus ad bellum*), together with “proportionality” and “discrimination” (or, in international law, the principle of “distinction”), as these latter two criteria are understood with respect to the conduct of hostilities and specific applications of force (*jus*

¹⁶ Uzi Mahnaimi and Sarah Baster, “Israelis seized Nuclear Material in Syrian raid,” *The Sunday Times* (London: 23 September 2007): http://www.timesonline.co.uk/tol/news/world/middle_east/article2512380.ece. [accessed 15 July 2011]. For a summary of the cyber war elements of this strike, see David A. Fulghum, Robert Wall, and Amy Butler, “Israel Shows Electronic Prowess,” *Aviation Week* (25 November 2007): <http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&channel=defense>. [accessed 15 July 2011] See also “Cyberwarfare Technology: Is too much Secrecy Bad?” *Airforce-technology.com* (9 April 2008): <http://www.airforce-technology.com/features/feature1708/>. [accessed 15 July 2011]

in bello). From the perspective of *jus ad bellum*, I would like to argue that the first of the two (presumed) Russian cyber attacks lacked a sufficient just cause and was not undertaken in any meaningful sense as a last resort. Moreover, from the perspective of the just conduct of hostilities (*jus in bello*), the first of the two Russian attacks was utterly indiscriminate, and likewise disproportionate in its threat of harm, at least, when compared either to the harm Russia or Russian citizens allegedly were suffering, or any legitimate military objective that might have otherwise been under consideration.

It bears mention that the Russian government has a long history of making too ready, indiscriminate, and disproportionate resort to force even when they have a legitimate objective whether in domestic or international situations (as in the October 2002 siege of a Moscow theater by Chechen rebels).¹⁷ The Estonian attack seems to illustrate this tendency, although the subsequent attack in Georgia appeared to exercise appropriate restraint. The same is true, by comparison, in the (presumed) Israeli preemptive military cyber attack on Syria, preceding its conventional strike against their nuclear facilities. A conventional strike had been continuously threatened in the event that Syria pursued development of a nuclear weapons program. There was arguably adequate justification leading up to the conventional attack, and thus also justification for the preparatory cyber attack. Importantly, both the cyber and conventional military actions were undertaken only after reasonable diplomatic efforts (including embargoes of illegal shipments of materials from North Korea) had failed to halt the Syrian collaboration with North Korean agents. The targets of cyber strikes were entirely

¹⁷ 23 October 2002, in which the Russian security forces' "disastrous response" resulted in the death of all 39 Chechen attackers and 129 of the estimated 800 hostages taken. See Rebecca Leung, "Terror in Moscow," CBS News "60 Minutes" (11 February 2009): <http://www.cbsnews.com/stories/2003/10/24/60minutes/main579840.shtml>. [accessed 15 July 2011]

military, and the overall damage inflicted as a result rather minimal, and arguably proportional to the harm threatened, the wrong done, and the military objective in question.

If I am right, this suggests (in marked contrast to Dipert's conclusions) that not all cyber conflict escapes the analytical framework of classical or conventional just war theory, and vice versa, that consideration of just war doctrine may effectively guide the conduct of cyber war, even as it attempts to do for conventional and irregular warfare. In the latter case, one of the most controversial topics in the past decade has been the justification of preventive war, undertaken against an enemy who has, as yet, done no actual harm, but represents a future threat of harm. Modern and contemporary just war doctrine rejects the legitimacy of a cause for war that does not involve the actual (rather than merely threatened) infliction of harm through an act of aggression. And yet this does not seem (at least in my view) to address adequately, for example, the menace of rogue states, or the dilemma of terrorist ongoing *preparations* for attacks that have the aspects of an international criminal conspiracy not yet fully consummated.

In this regard, I think it is instructive to consider a fourth, most recent case: that of Stuxnet, which the *New York Times* in January of 2011 described as “the most sophisticated cyber weapon ever deployed.”¹⁸ Once again, the problem of attribution is vexed: no nation or coalition has come forward to claim credit, or accept blame, for having engaged in what has gradually come to be identified as an act of preventive warfare.¹⁹ Suspicion falls heavily on those who stood to gain the most from the attack,

¹⁸ William J. Borad, John Markoff & David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times* (15 January 2011): http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

and perhaps on those who smile the most broadly, without comment, when the event is cited. The details are by now likely familiar to most readers, so let me simply summarize the key points of this act of war.

The Stuxnet²⁰ virus is a cyber “worm” of unknown origin, apparently developed and released in a number of countries in 2009. By July 2010, it was known to have infected computers all over the world, seeming at first to pose an ominous and generalized threat to “programmable logic controllers” (PLCs), small computers that control everything from measuring filling for sandwich crème cookies to changing traffic lights, water flow valves on municipal systems, and the rate of spin of nuclear centrifuges. It gradually became apparent that nearly 60% of infected systems were located in Iran (although others ranged from India, Pakistan, Indonesia and Azerbaijan to the U.S. and Europe), and so after some initial confusion, Stuxnet was assumed to be a cyber weapon targeted at Iran, that had subsequently failed in its primary purpose and run amok, spreading uncontrollably to unintended targets all over the world, and thus demonstrating how indiscriminate and destructive cyber weapons were likely to be.²¹

¹⁹ Michael J. Gross described this as “A Declaration of Cyber-War,” in *Vanity Fair*. Condé Nast. <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>. [Accessed 3 March 2011]. For an equally thorough, but more recent account of the entire Stuxnet affair, see also Kim Zetter, “How Digital Detectives Deciphered Stuxnet, the most Menacing Malware in History,” *Wired Magazine* (11 July 2011): <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1>. [Accessed 15 July 2011]

²⁰ This nickname for the worm was coined by Microsoft security experts, an amalgam of two files found in the virus’s code.

²¹ A study of the spread of Stuxnet was undertaken by a number of international computer security firms, including Symantec Corporation. Their report, “W32.Stuxnet Dossier,” compiled by veteran computer security experts Nicholas Falliere, Liam O Murchu and Eric Chien, and released in February 2011, showed that the main countries affected during the early days of the infection were Iran, Indonesia and India: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

This was the assessment of Stuxnet offered, for example, in a footnote in Professor Dipert’s essay (Dipert 2010: p. 407, n. 3; *supra* n. 2).

What was a reasonable assessment at the time, however, turned out to be woefully incorrect. Unlike most malware, Stuxnet did no discernable harm to infected computers and networks that do not meet specific configuration requirements. "The attackers took great care to make sure that only their designated targets were hit...It was a marksman’s job."²² While the worm is promiscuous, it renders itself inert if Siemens software is not found on infected computers, and contains safeguards to prevent each infected computer from spreading the worm to more than three others. All copies of the virus are apparently set to erase themselves on 24 June 2012.

Why Siemens software? The virus attacks and destroys nuclear centrifuges manufactured by Siemens, overriding the proprietary software and overloading the centrifuges themselves until they self-destruct. It does so cleverly, in the manner of the Hollywood film, *Ocean’s Thirteen*, by running a second sub-routine (known as a “man in the middle”) that disguised the damage in progress from operators and overseers until too late to reverse. One line of code restricts this damage, however, only to an array or “cascade” of centrifuges of a specific size (an array of 984 centrifuges, to be exact). In

Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%

²² Comment of Ralph Langner, a computer security expert in Hamburg, Germany, quoted in the *New York Times* article [fn 16, *supra*].

sum, unless one happens to be running a large array of exactly 984 Siemens centrifuges simultaneously, there is nothing to fear from this worm. It is an extremely sophisticated weapon: estimates are that it must have been months, if not years in development, with large teams of experts and access to highly restricted and classified information and equipment. This is not something a terrorist group, or even likely a well-organized and funded criminal organization could have undertaken (and certainly not a single 14 year-old hacker!). The investment of time and resources and expertise were simply beyond any but a well-positioned state or coalition to effect. The damage was done exclusively to a cascade of centrifuges, illegally obtained and operated in an otherwise highly protected site at Natanz, in Iran, in explicit violation of the 1970 nuclear non-proliferation treaty. The damage sustained within Iran to its clandestine and internationally-denounced nuclear program was subsequently deemed as “substantial,” and thought to have put its nuclear weapons development program off track for several years.²³

In keeping with our discussions of previous cyber conflicts cited above: there was a good and justifiable reason, reluctantly sanctioned in the international community, to undertake military action against Iran’s nuclear weapons program. Famously, diplomatic efforts and other, non-military measures have been undertaken for years without success. The harm is serious, but it is future harm, threatened rather than as-yet inflicted, so this was clearly a preventive attack. The target was wholly military, and damage confined to the targets identified. There was no collateral damage of any meaningful or significant sort to lives or property: civilian personnel and infrastructure were apparently neither targeted nor affected. Most importantly, when compared against

²³ Scarcely a year later, however, that optimism has vanished as a report from the International Nuclear Regulatory Commission, released in November 2011, appears to show the nuclear weapons program back on track and fully recovered from the cyber damage to its cascade of nuclear centrifuges.

“Operation Babylon,” the conventional Israeli air raid against Iraq’s nuclear program at Osirik on June 7, 1981, this cyber strike involved far less damage, harm, and risk of either for all concerned.

Still there are concerns raised that the promiscuous spread of the worm has now made this destructive weapon available to users all over the world, who might tweak it and release other versions.²⁴ This concern about Stuxnet as an “open-source weapon” available for downloading by anyone, demonstrates a fundamental misunderstanding of the nature of individual cyber “weapons,” to which Neil Rowe has called attention in his work (*supra*, n.6). They are not like nuclear warheads or RPGs, simply obtainable and re-useable by anyone. Rather, they are “one off” weapons: once used, their structure and function becomes readily apparent to security experts, anti-virus and security protections are quickly developed, and the original weapon is seldom ever reused, or usefully replicable.

IV.

In his path-breaking article, “The Ethics of Information Warfare” (1999) over a decade ago, John Arquilla outlined what I take to be an argument for permissible preventive cyber attack. Though obviously not as familiar with the broader range of classical JW doctrine as Dipert and subsequent just war/ethics experts, Arquilla nonetheless homed in on precisely the most relevant features of morally-justified conflict: a grave and morally sufficient reason or just cause for war, a record of prior good faith

²⁴ This concern is voiced explicitly in the online “infographic” documentary, “Stuxnet: Anatomy of a Computer Virus” by Patrick Clair (2011): <http://vimeo.com/25118844>. See also Ralph Langner’s cyber security blog: “What Stuxnet is all about,” *The Last Line of Cyber Defense* (10 January 2011); “A Declaration of Bankruptcy for US Critical Infrastructure Protection,” *The Last Line of Cyber Defense* (3 June 2011).

attempts to resolve the conflict short of armed attack that made such war a necessary “last resort,” and, in the targeting and tactics, a focus solely on threatening and strategic military targets, with the likely prospect of confining harm almost entirely to those targets, and entailing no risk to, let alone deliberate targeting of, civilian personnel or infrastructure. Under such severe constraints, Arquilla concluded, a cyber strike might be morally justified (*supra*, n. 7, pp. 392-393). And I would add: morally justified, even though it might constitute a preventive attack.

Stuxnet conforms almost perfectly to Arquilla’s constraints – so closely, in fact, as to raise suspicion that its perpetrators had read his article, and followed his own outline of the relevant moral constraints virtually to the letter! For my part, I’m inclined to agree that the circumstances warranted such a preemptive attack, and that, as designed and carried out, Stuxnet was an effective and morally justified military cyber attack. It shows that cyber war can be an effective alternative to conventional war, when less drastic forms of conflict resolution have been tried in good faith, and have failed. And, contrary to the fears of Dipert and others, such weapons and tactics can be designed to be effective, discriminate, and to inflict proportionate damage on their targets – far more so than conventional attacks.

Finally, I mentioned in passing above that this sophisticated weapon, and effective cyber weapons and strategy generally, were still expensive, skilled, labor-intensive, and therefore state-centric enterprises. No terrorist could, nor has, attempted anything like this. An effective weapon of cyber warfare like Stuxnet, at least at present, simply outstrips the intellectual, organizational, and personnel capacities of even the most well-funded and well-organized terrorist organization, as well as those of even the most

sophisticated international criminal enterprises. If one is going to bring down hydro-electric generators, nuclear centrifuges, and air traffic control systems, then one needs direct access to such devices or systems and the software that operates them, as well as an intimate knowledge of their operations. The 14-year old neighbor, in particular, who skipped (and subsequently flunked) physics and engineering classes to concentrate on his social networking skills lacks the requisite knowledge, as well as the access to the relevant hardware. If he succeeds in hacking into a defense department computer, he won't have a clue of what to do there, other than the cyber equivalent of spray-painting artistic graffiti on subway cars. Centrifuges and hydro-electric generators, for their part, do not fit neatly into terrorist apartments in Hamburg, or sadly, even into the most well-equipped public high school laboratory.²⁵

That is moderately encouraging news. In addition, I believe our experience of states as entities with political interests, unlike the usual case of terrorists and non-state actors, makes these activities amenable to good governance. In the Stuxnet case, we have an example of what good governance could license. In the other instances, we have examples of less justifiable actions (such as the indiscriminate and wonton targeting of civilians and civilian infrastructure) that might reasonably be renounced by all sides, without any discernable loss of political advantage.

Rowe, for his part, has suggested a plausible procedure for cyber weapon attribution that, like the nuclear-era red-phone "hot line" between Washington and Moscow, would help nations avoid accidentally precipitating a kinetic escalation of

²⁵ N.b.: The air traffic control scenario is a more plausible and ominous case, from the standpoint of both terrorism and even "vandalism," but would at minimum require the leadership or assistance of a disaffected ATC with years of experience and fairly robust security clearances.

hostilities in the case of mistaken suspicion.²⁶ Arquilla, in turn, recommended the wisdom of adopting a “declaratory doctrine of ‘no first use’ of information warfare against largely civilian targets,” a straightforward step that would address a principal concern of cyber critics, like Dipert and Rowe, that the core strategies of cyber war and weapons are premised on the illegal targeting of civilians and civilian infrastructure,²⁷ while still allowing for strikes against military targets (operations centers, logistics, and command and control nodes; *supra*, n. 8, p. 396). And, he adds, this policy still allows for retaliatory strikes in the event that one’s own civilian targets are attacked.

Finally, Stephen Bradbury, while echoing the current U.S. opposition to any new international conventions or cyber arms control agreements,²⁸ argues that the accepted norms and limitations in the cyber arena will develop through the practice of leading nations restricting their behavior in conformance with the established rules and customs of warfare. I believe we can now discern the norms emerging through the foregoing examples of practices, both good and bad, sufficient to move ahead with such discussions

²⁶ See “Towards Reversible Cyberattacks” (unpublished draft: available on the website of the Consortium for Emerging Technologies, Military Operations, and National Security (CETMONS): http://cetmons.org/files/documents/library/thrust5_cyberattacks.pdf. [accessed 15 July 2011]

²⁷ I have argued elsewhere that this tendency to target civilians in cyber conflict stems from the overwhelming influence of intelligence and espionage, or clandestine services communities in the formulation of strategy and development of weapons, as contrasted with the conventional war-fighting community, even though a preponderance of the participants, from General Keith Alexander and VADM William McCollough on down, wear (or wore) military uniforms. In espionage, covert action, and “psych ops,” there is no restriction on targeting civilians, although this has begun to be questioned in the intelligence community’s own discussions of professional ethics: See Jan Goldman, ed, *The Ethics of Spying: A Reader for the Intelligence Professional*, vols I & II (Lanham, MD: Scarecrow Press, 2005/2009); David Perry, *Partly Cloudy: The Ethics of Espionage, Covert Action, and Interrogation* (Lanham, MD: Scarecrow Press, 2009).

²⁸ The opposition to formal governance measures is beginning to decrease in the U.S. as a formal cyber strategy begins to take shape. At the same time, acknowledging that cyber conflict is likely to resemble features of the nuclear era and the cold war, a decided preference is expressed for bi-lateral and multi-lateral forms of “soft law,” such as Arquilla’s proposal for a declaration of “no first use” against civilian targets. See William J. Lynn III, “Defending a New Domain: the Pentagon’s Cyberstrategy,” *Foreign Affairs* 89, no. 5 (September/October 2010): <http://www.ciaonet.org/journals/fa/v89i5/08.html>. [restricted site, accessed 11 February 2011] VADM Mike McConnell, “To win the cyber-war, look to the Cold War,” *The Washington Post Outlook* (Sunday 28 February 2010): B1. Ellen Nakashima, “NSA Chief faces questions about new Cyber-command,” *The Washington Post* (Thursday 15 April 2010): A19.

and the formulations of relevant treaties and protocols, and to put to rest some of the more extreme, hysterical, and unfounded fears about cyber conflict. Outlawing indiscriminate destruction, and deliberate civilian targeting, would constitute a good beginning, and the foregoing cases show that such measures would not rob states of their abilities to conduct political conflict effectively within the accepted bounds of law and morality.