Just War and Cyber Conflict
"Can there be an 'Ethical' Cyber War?"

George R Lucas, Jr.

Thank you, Col. Athens, and to members of the Naval Academy Class of 2014, our generous donors, dedicated faculty colleagues, ladies and gentlemen: good evening. Thanks for coming, although I realize many of you did not really have a choice in the matter. I'm aware of the fondness of midshipmen for mandatory weeknight formations for any reason! People tend to exact a subtle revenge when their choices are constrained. A few years ago I had the similar honor of being invited to deliver the annual Reiff Lecture on Ethics at the Air Force Academy. They, too, were a captive audience, so I tried my best to do a good job, but afterwards the Cadet Wing Commander came up on stage with the speaker's award, a beautifully-carved mahogany Falcon with a silver dedication plate. As he presented this lovely gift, the Cadet Commander remarked: "Sir, you gave us a lecture tonight. So now we would like to give you 'the Bird'!"

I. The Just War Tradition and Cyber Warfare

So tonight I'd like to discuss the topic you are currently studying in your ethics course, the so-called "just war tradition," and see whether that venerable historical tradition of moral reflection on the declaration and conduct of war that you are currently studying can help us understand the new moral challenges that we face in the domain of

cyber conflict. The specific question I would like to raise and address is, "Can there be such a thing as an Ethical, or a "Just" Cyber War?"

Now, at first, this might seem like a strange question to ask. In fact, we might reasonably wonder whether it even makes sense to talk about justice, "ethics," or morality in our present and future development and use of cyber weapons, or when engaging in cyber warfare – especially when adversary nations, organized crime, and terrorists are relentlessly engaged in attacking us, harming us, and stealing us blind without regard for either. The vulnerabilities, the threats posed, and the genuine harm already done are all very real. Would not a consideration of ethics at this point merely serve to hamper us by placing imaginary or idealistic constraints on our own ability to respond to these vulnerabilities, and thereby provide an unfair advantage to adversaries who give such matters absolutely no credence whatsoever?

In my presentation this evening, I want to argue that we, *and* our potential adversaries, just might benefit considerably by giving some thought to what diplomats and international relations experts term "governance:" that is, principles found in both morality and the law that might encourage all concerned with, or engaged in, cyber conflict to reflect more cogently and coherently upon the strategic goals that might be served by such conflict. An "ethical analysis" of cyber conflict simply invites all parties to it to think clearly about what we are doing, what we are willing (and perhaps

unwilling) to do, and why. That is, what is it we hope to accomplish through such conflict? In particular, I think that it is both appropriate and important to talk about what we ourselves in the U.S. can and should do in response to what appear to be a relentless barrage of cyber espionage and cyber attacks directed against military, commercial, and vital infrastructure targets in our nation by persons or entities unknown. We must also consider whether there are limits (of an ethical sort) on what we are willing to do in response, and finally about whether, just as in conventional or counterinsurgency conflict, it is really true, as it is so often asserted to be, that acknowledging and abiding by ethical principles in the midst of this or any kind of warfare automatically puts us at a disadvantage in our conflict with adversaries, enemies, and international criminals.

II. The Peculiar Nature of Cyber Conflict

That's the agenda: so, let's talk first about threats and vulnerabilities. Authors Richard A. Clark, Joel Brenner, and Mark Bowden (to name only a few) have all done a service by raising public awareness of the nature and significance of cyber conflict, pointing out the extensive risks and vulnerabilities we face, and by inviting us to think more carefully about how to respond to the threats and manage that risk.[1] At the same time, it is important not to move all the way from abject lack of concern (a fair

[1] Richard A. Clark and Robert K. *Knake, Cyber War: the Next Threat to National Security, and What to Do About It* (New York: HarperCollins, 2010); Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Books, 2011); and Mark Bowden, *Worm: the First Digital World War* (New York: Atlantic Monthly Press, 2011).

description, for example, of the U.S. Naval Service's attitude toward cyber conflict barely two or three years ago) to an exaggerated or hysterical assessment of our vulnerabilities.[2] Threat inflation is no more of use to us in thinking through these difficult questions than ignorance and avoidance.

One glaring problem with how this problem is being discussed is something called "equivocation" (in which different parties to a dispute employ similar-sounding language in very different, often divergent, and frequently misleading ways).[3] Equivocation and conceptual confusion is an enormous obstacle to the clear analysis of military technologies generally, such as "drones" and robotics. But nowhere is this problem of confusion and equivocation more apparent than in the arena of cyber conflict. For example, Clarke and Brenner both offer chilling scenarios of a potential cyber "Pearl Harbor on Steroids," with dams bursting and flooding, trains derailing, planes falling from the sky, poison gases escaping from chemical storage plants in large cities, and the like. But most of the subsequent discussion of actual cyber conflict documents criminal activity, vandalism, theft, and acts of espionage. There is a heated debate in the literature about whether well-publicized cyber events in Estonia and Georgia and Iran (that we will

[2] 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).

[3] CDR Todd C. Huntley, USN complains of the problems of misuse of concepts and terminology as a fatal flaw in the analysis of cyber conflict and vulnerabilities: "Controlling the Use of Force in Cyber Space: the Application of the Law of Armed Conflict during a time of Fundamental Change in the Nature of Warfare," *Naval Law Review* LX (2010): 1-40. See especially his characterizations of cyber activity at p. 4.

turn to momentarily) even constituted cyber "attacks" at all, since (as the critics complain) no lives were lost or permanent harm done.[4] One skeptic on the television show "Intelligence Squared" derisively dismissed cyber "war" altogether as a fantasy, likening it to the Soviet Army having invaded the U.S., and then….stood in line to prevent U.S. citizens from renewing their drivers' licenses! All these debates frame difficult, and as yet unanswered questions, such as:

- What constitutes the "use of force" in the cyber realm?
- When, if ever, does such force rise to the level an "armed attack" of the sort envisioned in the United Nations Charter [e.g., Articles 2.4, 39, and 51], constituting a legitimate cause for war in self-defense?
- More generally, what is the nature of the "harm" or damage done through such attacks, when it is not explicitly kinetic or physical harm?
- When does the harm (on whatever account) done through relentless intrusion and invasion and theft of vital information and potential sabotage of vital infrastructure rise to a level that justifies retaliation, either in kind, or by means of kinetic reprisal?
- And finally, when formulating our strategies for cyber security and defense, what is the relation on one hand between privacy, and any right an individual citizen

[4] On such skeptic is Thomas Rid (University of London), who argues that all of the highly touted cyber "attacks" to date have constituted little more than conventional state and commercial espionage and criminal activity, none of which rises to the level of a military use of force or an "armed attack." See "Cyber War will Not Take Place," *Journal of Strategic Studies*, 35:1 (October 2011), 5-32. See also his exchange John Arquilla in *Foreign Policy*: "Think Again: Cyberwar," and Arquilla's rebuttal, "Cyber War is Already Upon Us," (March-April 2012): http://www.foreignpolicy.com/articles/2012/02/27/cyberwar; and http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us, respectively. I have argued in response that the concern for threat inflation, and confusion of true warfare with low-intensity conflict (espionage and covert action) is appropriate, but the author's definition of "harm," "use of force," and "armed attack" are simply too restrictive for this domain. See "Permissible Preventive Cyber Warfare," in Luciano Floridi and Mariarosaria Taddeo, eds. *Philosophy of Engineering and Technology* (UNESCO Conference on Ethics and Cyber Warfare, Unniversity of Hertfordshire, July 2011), forthcoming from Springer Verlag.

> may reasonably claim to such privacy, and to anonymity on the other? Are these really equivalent?

These are all questions about which we are still largely unclear, in part because the domain of cyber space appears to be so novel and unique,[5] and our history of backing into it until just a few years ago was so casual and largely unreflective.[6] Just as with earlier questions about the impact of emerging issues like private military contracting, or the advent of military robotics, on the military profession, ethics, and law, so too these problems and questions pertaining to cyber warfare have arisen, not through judicious pursuit of carefully formulated strategic policies, but largely through the unreflective evolution of behaviors, and through the gradual emergence of new possibilities and unanticipated prospects over the course of time, leaving us likewise to wonder about their impact on the military profession, ethics, and international law.

These, of course, are questions that have begun to be addressed in the emerging cyber security strategy of the U.S., of which there are now two versions: the Department

---

[5] Randall Dipert calls attention to what he terms the "unique ontology" of cyber objects, events, and weapons as posing the greatest challenge to understanding both this new domain, and the application of conventional conceptions of military ethics, just war doctrine, and the Law of Armed Conflict (LOAC) to it. See Randall Dipert, "The Ethics of Cyber Warfare," *Journal of Military Ethics* 9, no. 4 (December 2010), 384-410. Michael Schmitt likewise calls attention to this puzzling feature of cyber events and objects as the principal source of difficulty in determining how to interpret and apply jus in bello and the black-letter provisions of international law to cyber conflict. See Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues," *U.S. Naval War College International Law Studies*, vol. 87 (2011), 89-110.

[6] As detailed, for example, in 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.

of Defense (DoD), and the Department of State/White House version.[7] The rhetoric of both is quite distinct and different, but both manage in their own way (in American humorist James Thurber's phrase) "to amuse with their pretensions." The latter, the State Department document, was largely drafted by a (former) doctoral student of colleagues at Oxford University's program in "Ethics & the Law of Armed Conflict" (ELOAC). It is visionary and aspirational, acknowledging the cyber security threats and vulnerabilities, to be sure, but focusing largely on the prospects for global peace and international prosperity that an open, transparent, universally accessible global Internet promises to yield.

I stopped in Oxford to lecture on this topic this past November, on my way home from teaching these subjects for new 2nd Lieutenants at the French Military Academy in Saint-Cyr. The ELOAC faculty were justifiably proud of the work of their recent graduate, but I confessed that, while I admired the document's visionary rhetoric, I thought their student's underlying policy recommendations were perhaps too sanguine, and too naïve concerning the security threats. By contrast, the DoD document, released finally in the summer of 2011, displays the protective paternalism one might expect from responsible military, intelligence and security forces: the document is chock full of threat

---

[7] "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," (Washington DC: Office of the President, 1 May 2011), 25 pp. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. "Department of Defense Strategy for Operating in Cyberspace" (Washington, DC: Department of Defense, 1 July 2011), 13 pp. http://www.defense.gov/news/d20110714cyber.pdf.

assessment, cognizant of the bewildering array of vulnerabilities, and fairly bristling with proposals for defensive and counter-offensive measures in response -- the cyber equivalent of barbed wire, steel, and land mines. One DoD official summed it up last May 30th for the *Wall Street Journal*, "if you shut down our power grid, maybe we will put a missile down one of your smokestacks!"[8]

This is the tough talk of deterrence, that might give pause to reasonable, self-interested adversaries. I'm less certain that criminals and terrorists will be dissuaded by it. In any case, I hope you will see that it immediately poses some hard questions: first, of course, *whose* smokestacks, given the difficult problem of what is termed "attribution" in the cyber domain. Perhaps just as important: *how many* missiles, down *how many* smokestacks? What cyber damage or harm would we need to sustain in order to provoke such a response? And the trick is, we'd need to have an answer, on the one hand, to inform our policy. But, as Martin Libicki at the RAND Corp points out,[9] we wouldn't want exactly to advertise what that answer was, or clarify it too vigorously, since adversaries invariably try to "game the system" and test the limits of any declared policy. In order for the desired deterrent effect to occur, it would be better to keep them guessing

---

[8] Military official quoted in Siobahn Gorman **a**nd Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal* (30 May 2011): http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[9] Martin Libicki, presentation at the Air Force Research Institute symposium, "Cyber Power: the Quest Towards a Common Ground" (Maxwell AFB, Alabama: October 26-27, 2011; proceedings forthcoming). See also his earlier, path-breaking work in this field, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Corporation, 2009); *Conquest in Cyberspace: National Security and Information Warfare,* (New York: Cambridge University Press, 2007).

and worrying. We need to remain deliberately vague about where those limits lie – just the sort of "double-deek" deception we used to practice w/the Soviets during the Cold War.

Finally, are "smoke stacks" and power grids the proper sorts of targets? Perhaps responding in kind to an enemy's cyber attack on vital infrastructure would be appropriate, but would we want to make such attacks on civilian infrastructure part of our offensive strategy? Would we be willing, for example, to use a sophisticated cyber weapon to take out the Three Gorges dam, and subject millions of ordinary farmers and citizens to drowning, starvation, and immiseration merely to counter an armed confrontation or military standoff in the Straits of Taiwan, or worse, over competing claims of regional states over mineral rights in the South China Sea (in which we, as a nation, have no claim or direct interest)?

III. Just war doctrine and the military profession

Those, then are some of the main puzzles, threats and vulnerabilities associated with cyber conflict. How are we to go about formulating policy in response to such questions and scenarios?

My view is that such questions drive us back to foundational resources for dealing with crisis response, resources and traditions that attempt to guide us in balancing important guiding principles and values against the lives and welfare of large numbers of

people who might be affected by such events. This is never an easy balancing act, but we do have resources, and experience in applying them to questions like these. We find these resources in the cardinal principles of international law, that, in turn, reflect centuries of philosophical evaluation of such moral dilemmas, known as the "Just War Tradition." That tradition, and the body of international law derived from it, counsels us in two respects. They advise us on (1) *when* are we entitled to use force, or engage in an armed attack against adversaries who have harmed, or threaten to harm us; and (2) on *how* we are to go about doing so. As you've learned in the past few class sessions, those two sets of questions and responses go under their Latin headings, which medieval lawyers originally coined as the idioms *jus ad bellum* and *jus in bello,* respectively.

In answer to the first set of questions, the so-called *jus ad bellum*: the use of force is justified in this tradition only reluctantly, in behalf of a grave or serious matter of state, and only after all reasonable attempts by duly constituted or "legitimate" authorities to resolve the conflict have failed. These three specific observations are known as "just cause," legitimate authority, and "last resort," respectively. There are some other concerns that also come into play in reaching our decision, such as what are the proper goals or intentions to pursue, and whether the harm done to us is sufficiently grave to justify war in its resolution (called "proportionality of ends"), and so forth.

When the resort to force is found necessary according to such criteria, moreover, the conventional responses to the second set of questions, the so-called *jus in bello*, declare that force must be employed only to the degree required to achieve legitimate military objectives, should be directed only against representatives of the military forces of the adversary, and never deliberately against third-parties or non-combatants. These guiding principles of just war doctrine are likewise the cardinal principles of the international law of armed conflict, known broadly by their philosophical names (more than by their specific legal expression) as: *proportionality of means* (or, the "economy of force"), *military necessity*, and the principle of *noncombatant immunity* or discrimination (or "distinction" in the law). In international humanitarian law, the principle of "proportionality of means" takes an addition form, in specific legislative prohibitions against weapons or uses of force that inflict cruel and unnecessary suffering.

Now here is the important feature of these principles: these cardinal principles or strictures of LOAC reflect a grudging moral consensus, achieved over centuries of state practice between rivals and adversaries, to attempt to limit the collateral damage of war (as we were reminded most recently in the Kosovo air campaign over a decade ago). We don't deliberately target civilians or civilian infrastructure, and we take reasonable care to limit the degree of force deployed in pursuit of a legitimate military objective in order to avoid disproportionate "collateral damage." In my own teaching and writing,

furthermore, I have attempted to show how such legal constraints emerge from the proper practice of the profession of arms, constituting its most sacred and fundamental moral values and professional principles.[10] They are thus not to understood as imposed externally, as "handcuffs" on military personnel, placing our military at a competitive disadvantage against ruthless and unprincipled adversaries. Rather, such norms and constraints on permissible action arise out of the reflection by military personnel on their experience of combat, their professional identify, and the underlying purpose of the military profession itself as a vital form of public service.[11]

IV. Just War doctrine and cyber conflict

The question we face presently is how, and perhaps even whether, such longstanding principles and traditions can offer any useful guidance in the cyber realm, or rightly constrain our efforts to respond to and resolve cyber conflict.

Consider, for example, that by far the greatest areas of vulnerability are not hardened, encrypted, and securely-firewalled military and security targets (although these

[10] See, for example, G.R. Lucas, " 'This is Not Your Father's War': Confronting the Moral Challenges of 'Unconventional' War," *Journal of National Security Law and Policy*, 3, no. 2 (2009), 331-342; "'Forgetful warriors' – neglected lessons on leadership from Plato"s Republic," *The Ashgate Research Companion to Modern Warfare*, eds. George Kassimeris and John Buckley. London: Ashgate Press, 2010; and the treatment of military ethics as professional ethics in *Anthropologists in Arms: the Ethics of Military Anthropology* (Lanham, MD: AltaMira Press, 2009).

[11] This somewhat novel approach to just war doctrine as a manifestation of professional ethics in a military context infuses the textbook presently used in this course, and in similar courses at the Air Force Academy and Naval ROTC capstone courses, and constitutes the reason that this text is sub-titled "The Moral Foundations of Leadership." See George R. Lucas, Jr. and W. R. Rubel, eds., *Ethics and the Military Profession: the Moral Foundations of Leadership*, 3rd edition (New York: Pearson, 2010).

are still surprisingly and disturbingly vulnerable). Rather, as in nuclear conflict, the areas of greatest vulnerability are civilian populations, civilian objects, and vital public infrastructure. Accordingly, most cyber weapons, and many scenarios for cyber warfare, have been focused upon such targets, in apparent violation of the most fundamental principles of international humanitarian law and the just war tradition.[12] Critics of both, however, have offered these facts as demonstration that these approaches are antiquated, outmoded, and useless, and ought not to be invoked in the analysis and evaluation of cyber conflict, especially when the "harm" done appears to involve little or no loss of life or destruction of property.[13]

I dissent from, and object to that dismissal of the relevance of international law and the just war tradition to cyber conflict.[14] The principles of just war and law of armed conflict are central to that tradition, so I would be reluctant to toss them out now, largely because the insights stemming from conventional or traditional just war doctrine, and

---

[12] This complaint has been lodged most forcefully by computer scientist Neil C. Rowe: "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.

[13] E.g., in the works by Randall and Rid, cited above.

[14] Midshipmen forced to listen to this mandatory lecture as part of their ethics class might think, "Of course he does, because he and CAPT Rubel co-authored the textbook and put that stuff in, so naturally they want to defend its relevance." In fact, that is mistaken. We did not co-*author*, we merely co-*edited* the textbook, which meant that it was really a huge collaboration between civilian academics and senior military personnel, who argued for over a decade on what should be included. But when all was said and done, it was a great honor to listen to and help senior military personnel develop a fuller understanding of their own professional experience and core professional values, and to try our best to enshrine their important insights in this text and in the Naval Academy's core ethics course.

lying at the philosophical and juridical core of present international law, constitute the only resources we have to bring to bear upon such questions. We must, at least, attempt (as human beings invariably are driven to do whenever faced with a set of novel circumstances) to extrapolate from the known to the unknown, by means of analogy, comparison, and interpretation. At least we must make the attempt, and explore the intuitive soundness of the results, before abandoning such resources altogether.

When attempting this interpretive extrapolation based upon "professional ethics," we are immediately confronted with an interesting discovery concerning the cultural context or background of cyber conflict: it is "information warfare," and so reflects the tolerated and traditional practices of the professional communities most deeply engaged in ISR: the clandestine services and intelligence communities. These communities are neither identical to, nor uniformly coextensive with, the community of professional military practice. In international espionage, for example, the name of the game is usually thought to be dirty tricks and deception: to steal more information from them than they do from us, and in the ensuing conflict to "do unto them, before they do unto you."

What has happened, inadvertently, is that, without our full awareness, cyber conflict has blurred the heretofore sharp, traditional boundaries between espionage, covert action, and ongoing low intensity inter-state conflict and competition on the one

hand, and full-scale kinetic conflict and armed combat on the other. Those kinds of conflict were heretofore carried out by the members of two distinct professional communities, with their own set of rules, laws, and core values. So, in a sense, some of the debate about ethics and cyber war represents the debate between two different professional communities concerning how conflict of whatever sort is best handled.[15] It is important to realize this, and to wonder how the boundaries between the two communities may have moved. How have the resulting rules and conventions pertaining to conflict changed, if at all? Are we speaking metaphorically, or literally, when we describe cyber "attacks" and cyber "warfare"? (We don't normally, for example, label a massive breach of security by enemy espionage agents as an "armed attack," or classify our response as constituting "warfare.")

V. Emerging Norms of Cyber Conflict

When we find ourselves venturing into a new area of relatively unfamiliar terrain like this, the usual advice is to proceed with caution, speak and think carefully, and observe as closely as possible the sorts of behaviors that are actually taking place, and are found to test the limits of minimally acceptable conduct. In international law, this is

[15] This is so, I have insisted elsewhere, 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).

known as the search for "emerging norms" of state behavior. Here, I have argued in my own writings and presentations on cyber conflict, that we've begun to have enough experience with this relatively new domain to begin to discern, both as individuals and as nations, what we would like to see transpire there, and what kinds of behaviors we would like to condemn and discourage.[16] That international norms have begun to crystalize in the conduct of cyber conflict may be demonstrated by considering four recent instances of such conflict with which the general public is now reasonably familiar: Russia versus Estonia (2007), Russia versus Georgia (2008), Israel versus Syria (2007), and Stuxnet (2010).[17]

---

[16] See, for example: "Permissible Preventive Cyber Warfare," in Luciano Floridi and Mariarosaria Taddeo, eds. *Philosophy of Engineering and Technology* (UNESCO Conference on Ethics and Cyber Warfare, Unniversity of Hertfordshire, 1 July 2011), forthcoming from Springer Verlag.

[17] There are a plethora of reliable sources for accounts of each. A very succinct and dramatic description of all four cyber conflicts is offered by Richard A. Clark and Robert K. Knake in *Cyber War: the Next Threat to National Security, and What to Do About It* (New York: HarperCollins, 2010). 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. Rünnimeri, 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.

In the Syrian case, see 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. 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. See also "Cyberwarfare Technology: Is too much Secrecy Bad?" *Airforce-technology.com* (9 April 2008): http://www.airforce-technology.com/features/feature1708/.

Of course, no one has taken "credit" for Stuxnet, although allegations have flown since its initial discovery (by German cyber security expert, Ralph Langner) in 2009-2010. The usual default is to credit those who smile the most broadly, cough gently, and decline to comment for the record. Likewise the Russians and Israelis either deny, or refuse to discuss responsibility for the other altercations.

Here I've come to believe that the so-called "attribution problem" is neither all that big nor all that unprecedented. Cyber forensics has taken enormous strides in the detection of crime and the origins of inter-state cyber conflict, for one thing. For another, when in doubt, forget about "Asimov's laws" of robotics, and apply instead mystery writer Agatha Christy's principle: namely, ignore the background distractions, and focus upon who stands to benefit most from the deed in question. Nine times out of ten, you've

---

Finally, for Stuxnet, see 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. Michael J. Gross, "A Declaration of Cyber-War," in *Vanity Fair*. Condé Nast. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104. 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. This nickname for the worm was coined by Microsoft security experts, an amalgam of two files found in the virus's code. A study of the spread of Stuxnet was undertaken by a number of international computer security firms, including Symantec Corporation. Their report, "W32.Stuxnet Dosssier," compiled by noted 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. Despite its apparent success as a cyber weapon, concerns have been raised about proliferation and cloning of the design by third parties (e.g., terrorists). 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).

got your perpetrator, and 90% certainty is probably close enough for government work. An accused government may respond (as Russia did in the Estonian case) that it can't be held responsible for the actions of "patriots, criminals, or outraged vigilantes" within its borders, but that defense is nonsense. It didn't work for the Taliban in disclaiming responsibility for what Al Qaeda did "beyond its control" but within its sovereign borders, and it probably shouldn't be allowed to work here, either.

Our response should be the same in cyber as in conventional conflict: "either you stop the illegal actors, arrest them or throw them out, and take responsibility for what goes on within your borders, or we will regard you as complicit in these acts." That declaration moves us from the realm of international criminal law alone, to that of inter-state conflict and LOAC.[18] That, coupled with effective cyber forensics and the "Agatha Christy principle" probably is enough to counter cyber subterfuge and take care of the

[18] This is a contested point that, for the most part, exceeds the scope of this paper. Scholars and practitioners of international law are far from unanimous on this point. Although in the past, States have successfully resisted imputing to themselves collectively the responsibility for criminal activities within their borders, that customary practice appears to have changed dramatically in the past decade. The International Convention on Cybercrime (Council of Europe, "Convention on Cybercrime" (Budapest: November 23, 2001): http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm) explicitly charges states with the responsibility for cyber crimes that occur within their sovereign borders, and the United Nations Security Council has increasingly demanded that member States own up to this responsibility. An authoritative interpretation of the current status of international law on this topic, supporting the position I adopt in this lecture, is offered by Col. David E. Graham, U.S. Army (retired), "Cyber Threats and the Law of War," *Journal of National Security Law and Policy*, 4 (2010): 87-102. See also the considerable body of work by Michael N. Schmitt on this problem, including: "Cyber Operations in International Law: the Use of force, Collective Security, Self Defense, and Armed Conflicts," in Herbert Lin, et al, *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, DC: The National Academies of Science, Engineering, and Medicine Press, 2010): 151-178. For his part Graham argues that a State's duty to prevent cyber attacks generates and indirect or attributed responsibility for such attacks that can be traced to sources or persons acting within the State's borders. He and Schmitt seem to agree that a combination of these factors is sufficient to attribute responsibility for an attack, and even to initiate a retaliation that may rise to the level of a justified "belligerent reprisal" under conventional international law.

attribution problem. (Besides, denials, disclaimers of responsibility, and non-attribution are nothing new in warfare: the Italians denied their small flotilla of submarines were responsible for sinking or damaging British supply ships near Gibralter early in WWII. When the British threatened to bomb the Italian peninsula into the Stone Age unless the attacks ceased, however, they mysteriously ceased!)

So let's move to cyber weapons, tactics and targeting. Estonia represents a wholesale and indiscriminate assault on civilians and civilian (and government non-military) infrastructure almost exclusively. There were no military targets, and more important, no reasonable military objectives served by the attacks. Moving a war memorial from one place of honor to another within one's sovereign borders may be cause for annoyance or even diplomatic protest, but hardly for war, and certainly not for an indiscriminate and disproportionate assault on noncombatants.

Stuxnet resides at the opposite extreme. The targets were purely military. No one was killed, no civilians or civilian infrastructure were deliberately targeted. The damage done and harm suffered was surely proportionate to the threat of harm posed by the target itself, and most importantly, every conceivable effort short of attack was undertaken to persuade the adversary to cease and desist. I'll come back to this in a moment, to wrap up. But I want you to notice how what in ethics and law we call "new norms" of inter-state conduct are already emerging from these instances.

The middle ground is occupied by the Georgian and Syrian cases. Here the Russians (or whomever) showed both discrimination and restraint, employing cyber tactics to destroy or disrupt the adversarial governments and military's command and control preceding a conventional attack, limited in turn to forcing a resolution of the specific issue in dispute (the status of breakaway province of Ossetia, and fate of Russian citizens living there). This is a perfectly acceptable wartime tactic.[19] We may choose to side with our NATO allies in Georgia in that dispute, but it is a legitimate inter-state conflict, a difference of opinion with reasonable claims on both sides. Clausewitz might scold us that this is what wars are designed to solve. The same holds true in the case of the alleged Israeli bombing attack on the Syrian nuclear facility apparently under construction (with technical assistance from North Korea) at Dayr al Zawr . A cyber attack utterly dismantled Syrian air defenses, permitting a conventional bombing raid on an illicit nuclear weapons facility, undertaken at night when deaths and collateral damage might be reasonably minimized, and presumably after diplomatic initiatives to cease and desist had utterly failed.

Notice that in these cases, I'm deliberately trying not to interpose my judgment of the merits of each side's dispute: only how they came to resort to war, and how they

[19] Michael Schmitt's analysis of this conflict in "Cyber Operations and the *Jus in Bello*, *op. cit.*, along with a majority of the sources he cites, support this interpretation of the legality of the cyber component of this attack, and also of its general conformity to the restrictions of LOAC.

conducted their conflict with cyber weapons and tactics. Here, I think, we can identify the following norms of acceptable behavior. A cyber attack is morally justified, and should perhaps be legally sanctioned, whenever the following conditions are met:

(1) the underlying issue in conflict is sufficient grave to serve as a *causus belli*

(2) only the adversary's military assets are targeted, and the harm inflicted (kinetic or cyber) is proportionate and reasonable in light of the threat posed by the targeted assets

(3) civilian lives and infrastructure are not the intended object of attack, and every effort is made to avoid or minimize damage to same; and finally

(4) every effort has been made short of war to resolve the dispute in question.

I think that is a pretty substantive set of conclusions to draw from these examples, and constitutes a good beginning for the ethics of cyber warfare. It both sorts the examples into acceptable and unacceptable modes of conduct, and seems to explain our different responses to each, independent of which side we politically favor in the dispute, and so offer a reasonable guide for action in the future.[20]

[20] 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 John Arquilla's proposal for a declaration of "no first use" against

Interestingly, as the case of Stuxnet suggests, these norms seem to permit even a *preemptive or preventive* cyber strike, as well as guide our thinking about retaliation for an unacceptable strike on our own assets. That is, the guidelines seem to work for both offense and defense.[21]

In fact, something like this list of criteria can be discovered in an interesting and path-breaking article on ethics and information warfare authored over a decade ago by Professor John Arquilla, Chairman of the Department of Defense Analysis at the Naval Postgraduate School (Monterey, CA). It was buried in an obscure Rand Corporation report issued in the late 1990s.[22] Arquilla, who is quite eminent in international relations, (but not in ethics), and you'll find his work throughout the pages of Foreign Policy and Foreign Affairs. Interesting, when he turned to ethics issues in this new area, he based his analysis almost entirely on his previous collegiate understanding of traditional just war doctrine.

---

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.

[21] See my forthcoming article from the UNESCO cyber security symposium (1 July 2011), "Permissible Preventive Cyberwarfare," *loc. cit.*

[22] John Arquilla, "Ethics and Information Warfare," in *The Changing Role of Information in Warfare*, eds. Z. Khalilzad, J. White, and A. Marshall (Santa Monica, CA: RAND Corporation, 1999): 379-401. Arquilla literally coined to term "cyber warfare" to currency, and is one of its leading analysists. I have cited some of his more recent work, above. See also "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.

Our team of resident Stockdale fellows was working on the Stuxnet case a year or so ago, when Col. Ed Barrett, our research director, first discovered this article. After reading it, I contacted John to introduce myself and ask him to speak to a consortium of engineers, scientists, lawyers and ethicists with whom we routinely collaborate on military operations and national security. I pointed out the coincidence and remarked: "John, it sure seems to me as if whoever developed this incredibly sophisticated weapon not only read your article, but followed its resulting ethical guidelines to the letter!"

He smiled broadly, coughed gently. . .and declined to comment for the record.

Thanks for listening, and I'll be happy myself to comment *for* the record, if there are any questions or comments.