Duqu's Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyberwar

Matthew Crosston

The debate over the applicability or non-applicability of international law to cyberwar and the need for a cyber-specific international treaty might be irrelevant. Both camps, pro and con, argue about the need for cyberwar to have the Law of Armed Conflict (LOAC) or some new international legislation properly cover the cyber domain. Both camps, however, misread how the structure of the cyber domain precludes strategically "piggybacking" on conventional norms of war. International laws on conventional war are effective because of the ability to differentiate between civilian and military sectors. There is a civilian/military ambiguity in the cyber domain that makes such differentiation unlikely if not impossible well into the future.

Hence "Duqu's Dilemma": with the focus on establishing legitimate targets and setting limitations on allowable action, the United States and its allies expose themselves to vulnerabilities while engaging in a futile endeavor that does not lead to improved cyber control. The effort to establish cyber rules akin to conventional norms is fruitless since these rules are not enforceable or logical. They will simply handcuff lawful states. This signifies that greater effort should be expended on creating preemptive strategy that accepts the military/civilian ambiguity problem. The tendency of scholars and policymakers to strive for "sanitized" cyberwar by constraining targets during operations means that cyber strategy remains devoid of true deterring power.

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and Founder and Director of the International Security and Intelligence Studies (ISIS) program at Bellevue University.

Whether one believes LOAC can or cannot apply to the cyber domain, whether one pushes for an international cyber treaty or thinks such treaties will be meaningless, one aspect is constant: the desire for rules governing cyberwar behavior. The problem is in attempting to create a code of cyber conduct that demands a distinct separation between civilian and military sectors. The cyber domain is not amenable to this separation since the aforementioned fusion, where participants, facilities, and targets are hopelessly entangled between civilian and military institutions, has basically been a missing explanation as to why the global effort to enhance and clarify norms has remained uneven and inadequate.

The Ineffectiveness of International Law

Addressing the issue of cyber security, the East-West Institute stated in 2011, "There is an urgent need for international cooperation on this most strategic of issues. If we fail on this task, global stability could be as threatened as it would be by a nuclear exchange."[1] International norms established with the Geneva and Hague conventions were meant to be explicit lines of protection for civilian populations when states engaged in war. That respect for and preservation of civilian life is now held to be sacrosanct, regardless of what form or delivery method war takes. As such, there is an expectation that cyberspace can be subjected to the discipline of conventional norms.

Others argue that establishing these customary understandings in the cyber domain is one of the most important geopolitical battles today, going so far as to say that it is Ground Zero for global diplomacy, national security work, and intelligence.[2] The goal is to bring the principles of arms control into the cyber domain. Indeed, the most optimistic want voluntary agreements that impose constraints on the development of cyber capabilities and ostensibly ameliorate behavior in cyberspace. Some, however, have acknowledged that there are potential dangers in trying to achieve this. Stewart Baker, a former general counsel at the NSA and assistant secretary for policy at DHS under President George W. Bush, voiced the obvious fear: the United States and its allies would obey whatever was written down and agreed to while no adversaries would.[3]

There may be a larger problem, however, than non-compliance: conventional war has the distinct advantage, historically, of being fairly explicit about target classification. Most military networks that would

initiate and enact a cyber attack depend upon and work within countless numbers of civilian networks. In addition, many of the actors that are part of the planning, initiation, and deployment of cyber attacks are not necessarily formal military but rather civilian employees of government agencies. In other words, the world of cyber conflict and cyberwar is not a world that can achieve such explicit classification. In fact, future trends only show this fusion growing deeper and tighter in time. As such, any attempt to introduce norms and rules that are predicated upon knowledgeable differentiation will likely end up confused and ineffective.

This "ambiguity assertion," for lack of a better term, has so far been relatively ignored in the various cyber debates. The latter tend to revolve around how loose or rigid, how informal or formal, how international or local such codes of constraint should be. Many of these proposed codes aim to constrain cyber behavior so as to protect banking, power, and other critical infrastructure networks "except when nations are engaged in war."[4] Without addressing the ambiguity problem, however, states find themselves in a quandary: where are the lines of distinction between civilian and military drawn? Perhaps the biggest dilemma, therefore, is not the problem of figuring out attribution (who was the trigger man), but rather this futile attempt to clear up the inherent and purposeful ambiguity that characterizes the critical infrastructure used to house, develop, and utilize a state's cyber capabilities.

Many of the current cyber discussions are flawed by the manner in which they implicitly want to analogize conventional conflict with cyber conflict, to make cyber attacks equivalent to armed attacks. To do this, however, the conversation must turn to legal definitions and parameters: when does cyber conflict constitute the use of armed force or a formal act of war? What actions would constitute a war crime? How much damage does it take to trigger a necessary retaliatory response?[5] These questions are much more difficult to answer in the cyber realm because of the logistical nightmare provoked by the ambiguity assertion. This fact has not been emphasized appropriately to date, nor is it strategically addressed at all.

Up to now, questions have focused instead more on comparable lethality, damage estimates, and the aforementioned attribution problem. To an extent, however, all of these problems are enveloped by the civilian/military ambiguity issue. The inability to establish that separation means that lethality could be more extreme by being more than just military

casualties, damage could be more devastating by being more than just military facilities, and attribution might not even be relevant: defining the WHO of an attack does not solve the problem if the HOW behind the WHO is inextricably fused among government, military, and civilian properties and people. In other words, many assume that figuring out WHO in cyberwar will solve most problems. The ambiguity assertion reminds everyone to be careful what they wish for: in cyber war, the WHO will never be conveniently distinct because of the HOW.

International law clearly does not alleviate the problem of civilian/military ambiguity in cyber conflict. Whether the discussion extends to codes of conduct, treaties, or international laws writ large, none of these potential documents attempts to address the inherent structural problem of modern societies and how they currently organize, conduct, and develop their cyber capabilities. Further confirming this is the equal amount of time, effort, and frustration expended in the sister projects of establishing terms and defining parameters. Examining that frustration will illustrate how impactful the ambiguity assertion is when contemplating how the world should deal with the rules for cyberwar.

The Frustration of Setting Terms

Part of the problem in getting international law to cover cyberspace efficiently involves a longstanding failure to translate essential terms and parameters into something that would truly impact on the cyber domain. Progress in moving beyond this problem has been extremely limited. Indeed, even a cursory glance across the literature over the past decade attests to the fact that cyberwar does not fit perfectly into the already existing legal frameworks on war and use of force.[6] Despite this reality, these terminological and doctrinal difficulties have been continually investigated with the aim of forcefully coordinating existing terms and doctrines in the cyber arena. This article argues that the lack of success is attributable to the unwillingness to engage the civilian/military fusion.

The desire for explicit terms, parameters, definitions, laws, and treaties is based more on the worry that failure to produce such explicitness will leave cyberwar outside the boundaries of rules that currently govern conventional war. The consequences are considered stark: critical civilian infrastructure could be targeted, as could basic necessities such as agriculture, food, water, public health, emergency services, telecommunications, energy, banking

and finance, and so on. The ambiguity assertion, however, articulates the difficulty in obtaining such explicitness: most if not all of a state's cyber capability utilizes and depends upon critical civilian infrastructure that also provides many important civilian functions. No state to date has created a cyber operations capability that is wholly distinct and separate from civilian networks and civilian infrastructure. In other words, go after the "military" targets and you will also de facto be going after "civilian" targets. The literature to date seems to ignore this fact. Consequently, much of the literature engages in a false riddle, trying to impose a theoretically precise answer on an empirically ambiguous reality.

This is further confirmed by the number of respected scholars, diplomats, and policymakers who miss the relevance of the ambiguity assertion by demanding that the laws of cyberwar should actually *forbid* the targeting of purely civilian infrastructure, indicating that cyber actors should try to respect the Geneva Conventions as much as conventional actors do.[7] The problem, of course, is that in cyberwar, purely civilian infrastructure is a category of diminishing returns. Indeed, given the obvious trend that sees only intensification and deepening of the civilian/military fusion, purely civilian infrastructure will end up more myth than reality.

The failure to address this structural riddle has been matched by an over-emphasis on agency. This manifests itself mainly in the focus on limiting and controlling potential cyber actions from adversarial states. James Lewis of CSIS emphasizes how a state can reduce risks for everyone by imposing common standards, like moving from the Wild West to the rule of law.[8] Eugene Spafford concurred, citing how cyber security is a process, not a patch, requiring continual investment for the long term as well as the quick fix, without which states will always be applying solutions to problems too late.[9] These are some of the brightest and most respected names in the cyber discipline. Their warnings are not irrelevant, but the emphasis on state actor agency, while failing to recognize the impact and importance of inherent cyber structure, leaves a vulnerable gap in cyber strategic thinking. Indeed, the contemporary failure to create explicit norm coordination should be seen as a demand to consider new strategy that can accept this structural incompatibility as inherent and not something to "overcome." For structural ambiguity is not only intrinsic: states are purposely deepening the ambiguity for its strategic advantage

and economic efficiency. States, therefore, should not focus on how to force a distinct civilian/military separation, but should rather develop new strategic thinking that accepts the ambiguity problem as a logistical reality that must be accounted for.

For empirical confirmation of the futility of trying to address these problems of conventional norms and explicit parameters, look no further than the United States military over the past half-dozen years. It is easy to produce a laundry list of frustration and unfulfilled hopes: General Alexander of US Cyber Command mentioned that progress was being made, but that the risks were nonetheless growing faster than the progress at present;[10] Vice Admiral Michael Rogers, commander of the US Navy's fleet cyber command, admitted to Congress that no agreement had been reached amongst the various commands on ironing out the rules of cyber conflict, but hoped that there would be positive developments "at some point in the near term";[11] and even the Pentagon produced a cyber document that ultimately stated that the laws of armed conflict apply in cyberspace as in traditional warfare, even while admitting that the basic terms "act of war" and "use of force" were still somewhat *ill-defined* in the cyber domain.[12] This shows the real term effects that the lack of new strategic thinking has when states do not address the ambiguity of civilian/military fusion.

Turf Wars and Tightropes: Military Discussion on Cyber Parameters

Just as with scholars, policymakers, and diplomats, the military has been steadfastly committed to establishing strict rules of cyber engagement that are akin to the conventional rules of war.[13] For several years, there has been a pending revision of the military's standing rules of engagement in the cyber realm.[14] It seems that while the military hoped that the scholarly and diplomatic communities would be able to help define much of the needed clarification, the two latter communities were themselves hoping to see the military lead the way with its revision. This obfuscation of responsibility, however, is not as relevant as many observers and analysts might think: failure to address these issues is not so much a case of one community trying to pass the buck on to another, but rather testimony to the confusion created when the ambiguity assertion about civilian/military fusion is not addressed.

General Alexander stated that in debating the rules of conflict in cyber operations, the United States was trying to do the job right.[15] Those debates, however, constantly oscillate back and forth between positions that do not address the primary innate structural concerns of the cyber domain. Consequently, the military has spent a half-dozen years promising imminent progress that does not materialize. The Pentagon's official report was itself described as "ducking" a series of important fundamental questions, including defining such basic terms as "war," "force," and "appropriate response."[16] This is pointed out not to poke fun at the military. Quite to the contrary, this article makes the argument that given the reluctance of all parties concerned to engage the ambiguity assertion, with an eye to developing new strategy that embraces it rather than hopelessly using old strategy to overcome it, the military has had no real chance of making substantive progress to define the parameters of cyber action concisely.

It is no coincidence that the American military has sincerely worked on issues such as administrative network control, cyber organization, force composition, and cyber intelligence/operation differentiation, in addition to basic terminology parameters, without any major questions being considered definitively and comprehensively closed.[17] How, for example, can USCYBERCOM be expected to connect all the dots and be the competent arbiter in determining a case for action when it readily admits difficulty in even articulating who exactly comprises the fraternity of cyber warriors operating and defending home networks?[18] If the issues at hand were neither so serious nor so far-reaching on the future of cyber conflict, it would be almost comical. Only recently has it seemed possible that relevant military bodies have started to reach the epiphany discussed here:

> Although there are some noteworthy first steps toward establishing an international set of cyber norms – evident in bodies such as the Convention on Cybercrime – any global framework governing military response actions in cyberspace will surely materialize at an onerous pace. After all, how can the rules of war, built upon the tactile presence of combatants and weapons and sovereign territory, be retooled for a world where 'troops' can be dispatched in milliseconds from a multitude of states?[19]

At least the above quote begins to frame the discussion around the innate incompatibility between how war in cyberspace would likely be conducted and how that compares to all previous wars. It is still, however, emphasizing agency over structure: establishing an international set of cyber norms mainly to hallmark the division between civilian and military assets and mitigate action already undertaken. This might help explain why formal strategic documents concerning cyberspace end up being nothing but simple platitudes about how the United States intends to protect itself. Take for example the Department of Defense's (DoD) Strategy for Operating in Cyberspace, released in mid-2011 and consisting of five "strategic initiatives":

> *Strategic Initiative 1*: Treat cyberspace as an operational domain to organize, train, and equip so that the DoD can take full advantage of cyberspace's potential.
> *Strategic Initiative 2*: Employ new defense operating concepts to protect domestic networks and systems.
> *Strategic Initiative 3*: Partner with other US government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
> *Strategic Initiative 4*: Build robust relationships with US allies and international partners to strengthen collective cyber security.
> *Strategic Initiative 5*: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Take full advantage; employ new concepts; partner with others; build robust relationships; leverage ingenuity. All of these phrases are wonderful slogans, but they are not accompanied by any explicit new strategic thinking that could hope to actually institute said initiatives. Trying to adapt conventional strategy slightly and then force the cyber domain into it is likely to remain a project bearing little fruit. Examining that conventional strategy and proposing new strategy that engages the structural dilemma is the final section of this paper.

Engaging Ambiguity: Strategic Thinking for the Civilian/Military Cyber Fusion

The need for a new strategic approach is best illustrated when the arguments of two highly respected strategic thinkers – one military and

one legal, who happen to fall on opposite sides of the LOAC cyber debate – ignore the problem of civilian/military structural cyber fusion. Dunlap, while accepting the need for improvement, believes the tenets of the law of armed conflict to be sufficient to address the most important issues of cyberwar.[20] The concern for distinguishing between legitimate military and civilian targets does not seem to bother Dunlap in its impact on the applicability of LOAC:

> LOAC tolerates "incidental losses" of civilians and civilian objects so long as they are "not excessive in relation to the concrete and direct military advantage anticipated." In determining the incidental losses, cyber strategists are required to consider those that may be reasonably foreseeable to be directly caused by the attack. Assessing second- and third-order "reverberating" effects may be a wise policy consideration, but it does not appear LOAC currently requires such further analysis.[21]

Dunlap's distinction is actually quite important given the current intellectual climate: he has introduced some much-needed realism into the debates by reminding people that LOAC has never been a flawless strategy that provides perfect protection for civilians and civilian objects. The problem highlighted here, however, is that his concerns over military/civilian differentiation are misplaced.

These pro-LOAC arguments are effectively built around the fact that cyberwar does not have to have a perfect record in delineating and then protecting civilians because LOAC does not, either. But these arguments assume that such delineation is generally possible. The future of cyberwar is unlikely to be able to create such possibility because it has long been established how many of the military's critical functions, assets, service providers, and supply chains all rely heavily on civilian traffic and networks.[22] As such, new strategy needs to be positioned so as to prevent the use of cyber weapons in general, because once they are used, the likelihood of incurring civilian risk, damage, and casualties will be de facto. "Sanitizing" the impact of cyber weapons once they are used by trying to constrain targeting choices will not work.

The anti-LOAC camp makes the same mistake when discussing why the law of armed conflict does not bring clarity to cyberwar:

> The laws of war are in place to ensure that parties to a conflict target combatants rather than civilians, and, if civilians are targeted, to ensure that such individuals have forfeited their protected status. To determine whether cyber-attacks properly distinguish between civilian and military targets, one must understand [the] distinction.[23]

The opposition camp fails in the belief that such a distinction can in fact be created in the cyber realm. This camp does not see the strategic influence of the ambiguity assertion, focusing rather on the deficiencies within LOAC and other contemporary norms and treaties: in short, make better laws and the cyber world will come to heel. As such, this camp is even further from cyber reality, ignoring a problem that is only going to deepen and intensify over time. The opposition camp, in essence, is a more liberal approach to conflict because the end goal is to create an atmosphere of trust that can minimize higher levels of violence and treachery.[24] This flies even more in the face of the current and future structure of cyberwar.

Both of these camps believe in being able to monitor and regulate and circumscribe cyberwar after it has begun, as happens successfully with conventional war. This is a false hope. The ability to monitor, regulate, and circumscribe cyber action is best done through strategy that can inculcate preemptive fear and thereby induce caution and hesitation. Current conventional strategies that aim for trust, target distinction, and minimizing noncombatant impact are simply inexplicably ignoring how cyberwar is organized, structured, and operationalized.

Liberal thinking also dominates the legal community, which is heavily leaned upon for law projects and the strategic thinking that purportedly infuses said projects for the cyber domain:

> [An effective solution to the global challenge of cyber attacks] cannot be achieved by individual states acting alone. It will require global cooperation. We therefore outlined the key elements of the cyber treaty – namely, codifying clear definitions of cyber warfare and cyber-attack and providing guidelines for international cooperation on evidence collection and criminal prosecution – that would provide a more comprehensive and long-term solution to the emerging threat of cyber-attacks.[25]

The only thing left to add here is to note yet another camp focusing on mitigating risk and limiting damage in the cyber domain ex post facto. Regardless of philosophical standing, political agendas, or theoretical acumen, every camp that examines the problem of parameters and definitions in the cyber domain seems to exclude considerations of preemptive strategies built upon fear and inducing reluctance to action. General Alexander of US Cyber Command cited the need to establish the lanes of the road for what governments can and cannot pursue and asserted that establishing those lanes was the necessary first step to addressing the challenge of cyber attacks.[26] What all of the camps examined here have in common is a tendency to give lip-service to strategy, but then really focus exclusively on ex post facto operations to establish progress. If the focus continues to be on agency action rather than on structural deficiency, then progress will not simply remain slow: it will become non-existent.

Duqu's Dilemma: Why It Matters

This analysis has pinpointed flaws in the current thinking and efforts to establish clear definitions and parameters governing the rules and operations within cyberwar. The emphasis placed here on inherent structural difficulties, namely, the innate cyber civilian/military fusion, has shown the likely damaging and deadly consequences to societies when strategies do not focus on the effort to stop cyber action preemptively, focusing instead on operational considerations after conflict has begun.

Only now are isolated legal analyses highlighting these problems beginning to emerge:

> It is unlikely that a state such as the United States could take precautions against the effect of attacks on military objectives by separating military objectives from civilians and civilian objects in cyberspace. This is because of the interconnectedness of US government and civilian systems in the near complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities... Proportionality assessments likely will prove particularly precarious in cyberspace, where outcomes are more difficult to predict than in the physical world: physical attacks at least have the advantage of physics and chemistry to work with. Because, say, the blast radius of a thousand pound bomb is fairly well understood, one can predict what

> definitely lies outside the blast radius and what definitely lies inside. Error bands and cyber-attacks are much wider and less well-known... [Most reports do not explain how] these public-private partnerships could be constituted in a manner that adequately considers laws of war issues nor do [they] address the likely use of active defenses by the private sector.[27]

As illustrated above, this structural issue is more than just semantics. It literally covers who engages cyberwar, what can be destroyed in cyberwar, who can be a victim during cyberwar, even the philosophical and ethical questions meant to be asked about cyberwar itself. Duqu's Dilemma is an entreaty to move away from unattainable goals and idealistic dreams in a futile hope to create sanitized cyberwar. Cyberwar will never be sanitized. Consequently, contemporary strategic thinking about the cyber domain must start treating the ambiguity assertion with the same gravity that the more famous attribution problem receives.

Notes

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict," *Cybersecurity Policy Report*, February 14, 2011.
2 Tom Gjelten, "Shadow Wars: Debating Cyber Disarmament," *World Affairs* 173, no. 4 (2010): 33-42.
3 Ibid.
4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar," *National* Journal, June 10, 2011.
5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory," *European Conference on Information Warfare and Security* 177-XI (July 2010).
6 Vida Anatolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?" *Naval Law Review* 51, no. 132 (2005): 1-34.
7 Don Tennant, "The Fog of (CYBER) War," *Computerworld* 43, April 27, 2009, pp. 28, 30-32.
8 James Fallows, "Cyber Warriors," *Atlantic Monthly* 305 (March 2010): 58-60, 62-63.
9 Ibid.
10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials Say," *Cybersecurity Policy* Report, March 26, 2012.
11 Lolita Baldor, "Cyber Warriors," *Army Times*, August 6, 2012, p. 23.
12 Siobhan Gorman and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack," *The Australian,* June 1, 2011.

13 Anonymous, "Military Ponders Cyberwar Rules," *Los Angeles* Times, April 7, 2008.
14 Ellen Nakashima, "Pentagon Seeks to Expand Rules of Engagement in Cyber War," *Washington Post*, August 10, 2012.
15 Ibid.
16 Ellen Nakashima, "Cyber Offense Part of Strategy," *Washington Post*, November 16, 2011.
17 Wesley Andrues, "What US Cyber Command Must Do," *Joint Forces Quarterly* JFQ 59 (Fourth Quarter 2010): 115-20.
18 Ibid.
19 Ibid., p. 120.
20 Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011): 81-99.
21 Ibid., p. 90.
22 Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review* 68 (2012): 167-206.
23 Michael Gervais, "Cyber Attacks and the Laws of War," *Journal of Law and Cyber Warfare* 30, no. 2 (2012): 525-79.
24 Ibid., p. 561.
25 Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review, Inc* (2012): 817-85.
26 Ibid., p. 884.
27 Hannah Lobel, "Cyberwar Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas International Law Journal* 47, no. 3 (2012): 617-40.