Virtual Patriots and a New American Cyber Strategy

Changing the Zero-Sum Game

Matthew Crosston

Most analyses on cyber deterrence draw a sharp distinction between the operational philosophy of the United States and that of authoritarian states like China and Russia. On the whole, they describe the difficulty of US efforts to maintain an effective cyber defense against brazenly offensive Chinese and Russian threats. This analysis takes an important contrarian position on this issue which has been relatively ignored: the cyber philosophy of China might offer the United States some useful insights. China's approach is more effective in ways that, for now, are apparently antithetical to the United States—amoral, overt, and proactive.

Whether Russian cyber nationalists or the Chinese Honkers Union, their guiding principles are clear: they are willing to defend their homeland through assertive and invasive techniques and will not limit their focus to defensive capabilities that only unevenly deter attacks. When defending the state from any perceived enemies—whether state, substate, or nonstate—establishing an offensive capability that instills fear is clearly a main agenda item within Russia and China. Part of this is based on their insecurities about a perceived kinetic imbalance with the United States and a willingness to be morally flexible when it comes to cyber-war norms. Arguably, the United States does not adopt a similar approach because of an apparent reluctance to mimic the policy of such distasteful regimes and an arrogance that does not concern itself with asymmetry. These stances undermine US national security.

First, for clarification, it is necessary to parse out the so-called rogue cyber behavior of China and Russia. There are significant differences in the manner and philosophy with which the two states approach their

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. He has authored two books, several book chapters, and nearly a dozen peer-reviewed articles on counterterrorism, corruption, democratization, radical Islam, and cyber deterrence.

cyber activities. China is seen as having a more "learnable" model that should creatively inspire the United States to alter and evolve its own cyber strategy to a level that would subsequently surpass the Chinese approach. Importantly, the purpose is not to copy Chinese cyber policy exactly, but rather to transform the characteristic of overt transparency into a US strategy of proactive cyber capability. This would infuse US security with a complex but capable new influence calculus where strategically overt means are used to further positive deterrence ends.

Ideally, this overt cyber strategy would create credibility in virtual weapons which employ disruptive cascading effects so powerful as to negate their use. The key would be in establishing plausible fear in the adversary. Some might argue there is limited utility in this approach because of the possibility that both China and Russia would fail to recognize the power of such a posture. Such logic subsequently declares virtual weapons do not have the same credibility as, say, nuclear weapons because the former have not achieved that level of credibility through actual usage or even testing. The efficacy evolution in cyber weaponry, however, helps support the main argument here. Given the recent revelations about Stuxnet and the effectiveness of the Duqu and Flame viruses—which quite possibly moved beyond the capabilities of Stuxnet—cyber weapons are rapidly obtaining that fearful reputation, and thus, deterrence via overt cyber strategy can no longer be considered pure fantasy.

This influence calculus turns current conventional wisdom on constraining norms within *jus in cyber bello* on its head. To date these constraints have shunned an overtly proactive US cyber strategy. A greater likelihood for peace across the global virtual commons is possible by using a strategy of facilitating restraint through fear. Please note, however, that *amoral* and *unethical* are not freely interchangeable in this analysis. For example, the Chinese may not view their cyber stances as unethical, while the United States does. The classically Machiavellian argument is that deep reflective discussions about morals and ethics should be suspended from the cyber domain if effective deterrence is to be achieved through overt strategy.

Finally, a cautious caveat: this is not an entreaty to abandon covert activities or secrecy. Rather, it is an important balancing argument for developing a fully encompassing strategy that allows both covert *and* overt US cyber power—an important evolution. It is not an argument against the need for classified operations. Simply, cyber strategy must be decoupled from a de facto zero-sum game. The building and elevating of overt cyber preemption does not take away from the relevance and reach of US covert cyber reactionary powers.

China and Russia: Cyber Cousins—Not Cyber Brothers

There seems to be a strong divergence in perception regarding China's desire to command cyberspace offensively. On the one hand is the assumption that this is a natural manifestation of its growing desire to achieve global superpower status. On the other hand is the counterargument that emphasizes China's own perception of its inability to operate effectively against the United States in a conventional military confrontation. Indeed, many Chinese writings suggest cyber warfare is considered an obvious asymmetric instrument for balancing overwhelming US power.[1] This latter argument is more compelling based on these stark military realities:

- In overall military spending, the United States spends between five and 10 times as much per year as China.
- Chinese forces are only now beginning to modernize. Just one-quarter of its naval surface fleet is considered modern in electronics, engines, and weaponry.
- In certain categories of weaponry, the Chinese do not compete. For instance, the US Navy has 11 nuclear-powered aircraft carrier battle groups. The Chinese navy only recently launched its first carrier, a refurbished Russian ship used solely for training.[2]
- In terms of military effectiveness (i.e., logistics, training, readiness), the difference between Chinese and US standards is not a gap but a chasm. The Chinese military took days to reach survivors after the devastating Sichuan earthquake in May of 2008 because it had so few helicopters and emergency vehicles.[3]

With this state of military affairs, China's perception of insecurity is not surprising. Even more logical is the Chinese resolve to grow its asymmetric cyber capabilities: such attacks are usually inexpensive and exceedingly difficult to precisely attribute. Attribution becomes even more complex for states where cyber attacks can be "launched" from neutral or allied countries.[4]

Given an authoritarian state's capacity for paranoia, it is illogical for China not to develop its offensive cyber capabilities. In this case, the weak conventional military strength is quite real. To that end, the People's

Republic has endeavored to create its own set of lopsided military advantages in the cyber domain. To wit:

- The Pentagon's annual assessment of Chinese military strength determined in 2009 that the People's Liberation Army (PLA) had established information warfare units to develop viruses to attack enemy computer systems and networks.
- The PLA has created a number of uniformed cyber warfare units, including the Technology Reconnaissance Department and the Electronic Countermeasures and Radar Department. These cyber units are engaged on a daily basis in developing and deploying a range of offensive cyber and information weapons.
- China is believed to be engaged in lacing the network-dependent US infrastructure with malicious code known as "logic bombs."[5]

The official newspaper of the PRC, the *Liberation Army Daily*, confirmed China's insecurity about potential confrontation with the United States in June 2011. The Chinese government proclaimed that "the US military is hastening to seize the commanding military heights on the Internet. . . . Their actions remind us that to protect the nation's Internet security we must accelerate Internet defense development and accelerate steps to make a strong Internet Army."[6] Clearly, the Chinese have sought to maximize their technological capacity in response to kinetic realities. This is not to say the United States is therefore guaranteed to be in an inferior position (information about US virtual capabilities at the moment remains largely classified), but the overt investment, recruitment, and development of Chinese virtual capabilities presents opportunities the United States should also be willing to entertain.

How does all of this compare and contrast with the Russian approach to the cyber domain? Anyone studying cyber conflict over the last five years is well aware of Russia's apparent willingness to engage in cyber offensives. The 2007 incident in which the Estonian government was attacked and the 2008 war with Georgia are universally considered examples of Russian cyber technology as the tip of their military spear. While it is true Russia actively encourages what has come to be known as "hacktivism" and lauds "patriotic nationalist" cyber vigilantism as part of one's "civic duty," there are still distinct differences with China.[7]

Much of Russia's cyber activity, when not in an open conflict, seems to be of the criminal variety and not necessarily tied directly into the state.

Indeed, Russia seems to utilize organized crime groups as a cyber conduit when necessary and then backs away, allowing said groups continued commercial domination. Russia, therefore, almost acts as a rentier state with criminal groups: cyber weapons are the natural resource, and the Russian government is the number one consumer. This produces a different structure, style, and governance model when compared to China.

Table 1. Parsing cyber rogues

Category Breakdown	China	Russia
Purpose	Protectionist	Predatory
Psychology	Long-term/Rational	Short-term/Cynical
Style	Strategic	Anarchic
Governance Model	State-centric	Crimino-Bureaucratic

Purpose

China's purpose in developing its cyber capability seems motivated by protectionist instincts based largely on the perception that it is not able to defend itself against the United States in a straight conventional military conflict. Russia's purpose seems utterly predatory. This is no doubt influenced by the fact that most of the power dominating cyber capability in the Russian Federation is organized and controlled by criminal groups, sometimes independently and sometimes in conjunction with governmental oversight.

Psychology

The operational mind-set of China seems to be both long-term and rational. Its strategies are based on future strategic objectives and its position within the global community. Most if not all of China's goals in the cyber domain can be clearly understood in terms of rational self-interest. Russia's cyber mind-set is dominated by short-term thinking, largely motivated by the pursuit of massive profit and wielding of inequitable political power. Analyzing just how much of Russian cyber activity is in fact controlled by the desire for wealth leads to an overall impression of state cynicism.

Style

Chinese cyber activity is strategic in style. The state strives to control the cyber environment and maintain influence over all groups in the interest of the state. The Russian cyber atmosphere, unfortunately, resembles anarchy. The state engages criminal groups through an authority structure that is blurred if even existent. Consequently, there is little confidence that the Russian government exclusively controls its cyber environment.

Governance Model

It is clear that China's cyber governance model is state-centric. This may not be ideal for democracy, but it shows China does not allow competing authorities or shadow power structures to interfere with its national interests. Russia's cyber governance model is crimino-bureaucratic. It is not so much that the state is completely absent from the cyber domain in Russia, but rather the ambiguity of power and authority define the cyber domain. Russia may enjoy claiming the allegiance of its patriotic nationalist hackers, but it does not in fact tightly control its own cyber netizens, at least not in comparison to China.

While neither Russia nor China is afraid to use offensive cyber weapons, there are dramatic structural, motivational, strategic, and philosophical differences. Russia seems to embody a criminal-governmental fusion that has permeated the entire state apparatus. The cyber domain there is used for temporary forays to achieve state objectives and then returns to more permanent criminal projects. As such, it is not truly state-controlled, is relatively anarchic, and cannot establish any deterring equilibrium. China, on the other hand, may be the first state to truly embrace the importance of tech-war; it has realistically assessed its own kinetic shortcomings and looked to cyber for compensation. In short, it has fused Sun Tzu with Machiavelli—better to quietly overcome an adversary's plans than to try to loudly overcome his armies.

This analysis paints Russia in a relatively stark strategic light. While these differences do not give rise to a trusted alliance with China, the manner in which it approaches its cyber domain presents interesting new ideas about how the United States should approach the global cyber commons. These ideas would be in contrast to both academic literature and journalism, as they offer two completely divergent responses. On the one hand, the United States is not appropriately meeting this challenge, and on the other hand, it remains second-to-none in cyber offense.

The United States invests heavily in cyber security, and members of the intelligence community work to create cyber weapons meant to preserve US military predominance. However, there are still missed opportunities and weaknesses that have not been addressed or overcome by covert strategy. Namely, emphasizing covert and opaque cyber initiatives hinders the emergence of a global cyber strategy that could compel constraint without actually engaging in cyber attacks. Recall this is not about developing overt at the expense of covert. Rather, it is about ending the zero-sum cyber game to the strategic benefit of the United States. Up to now American virtual patriots have not been used for maximum impact and effectiveness. It would be wise to position offensive cyber capabilities for strategic, overt, preemptive purposes rather than as solely logistical, covert, reactionary weapons. This is a dramatic shift in strategic mind-set, arguing for a yin-yang approach toward the covert and overt aspects of cyber rather than the present view as a zero-sum game.

New Technology but not New Thinking

In 2004, the Congressional Research Service (CRS) issued a report on information warfare and cyber war. It discussed public policy oversight issues Congress should consider, including whether the United States should

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities;
- modify US cyber-crime legislation to conform to international agreements that make it easier to track and find cyber attackers;
- engage in covert psychological operations affecting audiences within friendly nations;
- encourage or discourage the US military to rely on the civilian commercial infrastructure to support part of its communications, despite vulnerabilities to threats from possible high-altitude electromagnetic pulse (HEMP) or cyber attack;
- create new regulation to hasten improvements to computer security for the nation's privately-owned critical infrastructure; or
- prepare for possible legal issues should the effects of offensive US military cyberweapons or electromagnetic pulse weapons spread to accidentally disable critical civilian computer systems or disrupt systems located in other non-combatant countries.[8]

The CRS analysis focused on existing physical infrastructure and capacity. It did not explore new theoretical concepts that might achieve national interest more effectively. Most striking is the apparent assumption that the cyber domain will worsen in terms of political environment, as seen by the overreliance on cyber defensive systems. Such emphasis renders the US position reactive and late. The argument made here is for also pushing overt strategies based on devastating offensive capabilies that shift the US position into being more proactive, like China. Reactive policy simply *responds* to cyber attacks. Overt policy seeks to *deter* them.

The same CRS report highlighted the need for the Department of Defense (DoD) to achieve both decision and information superiority. This means a competitive advantage in the cognitive realm and one that enables the military to surprise an enemy.[9] Both of these advantages are best achieved with added frontend capability and not solely accomplished by reactionary policies. In short, there can be no dominant operational transfiguration without first a profound strategic transformation. An overt cyber strategy upfront makes proactive deterrence through fear more probable and gives the perception of decision and information superiority. Broadening the discussion to embrace a change in strategic mind-set greatly expands new potential deployment and deterrence options.

Many agencies within the US government have come close to espousing this transformation, only to fall short by demanding that US cyber capabilities remain exclusively covert. The National Security Agency has argued to better defend information networks by openly engaging both allies and adversaries in an open forum.[10] The Pentagon believes strongly in "active defense," which is quite simply, cyber offense. The problem is that both remain strategically focused on *responding* to a major cyber attack through covert means. In other words, the same flaw found in the CRS report nearly a decade earlier still applies; the limited innovation remains reactive. If the United States continues to view the overt and covert aspects of cyber strategy as a zero-sum game rather than as yin-yang symmetry, then it will fail to realize its true cyber dominance.

A more disconcerting aspect of the discussion—at least for those who envision the cyber domain as a venue for instigating deterrence, not provocation—is that a capability used exclusively for covert activity becomes just another weapon among weapons. The point of maintaining total secrecy is due to the lethality of actual deployment. Any preemptive deterring power, therefore, is lost when kept covert. Remember, the argument here is not to abandon secrecy altogether; it is not about showing all the cards but voluntarily revealing some cards for strategic purposes. If the desire is to expand a capability's impact, not just in terms of winning wars but in preventing them, then overt strategy is a valuable tool.

Recall where Chinese cyber policy found its fundamental motivation: China's original intent was to deter other nations from pursuing more-traditional coercive policies. It also wanted to develop an advanced cyber warfare capacity that would allow it to asymmetrically challenge any potential adversary.[11] One must see Chinese cyber offensive strategy as a rational solution that is not simply cheap, but potentially capable of giving the United States pause before a large-scale conventional military engagement.[12] This kind of policy in US hands, focused by an overt offensive strategy, could transcend national interests and provide a framework for achieving greater cyber restraint at the global level. Keeping the aforementioned influence calculus in mind, it elevates above Chinese parochialism for the greater, more responsible global good of overt US cyber dominance.

Note this is not an entreaty to copy or mimic Chinese cyber policy. China itself does not formally admit to an explicitly overt strategic policy over the cyber domain. It is, however, undoubtedly proactive and offensive. By strategically allowing general knowledge about the existence of an offensive program and spreading the perception that it is willing to proactively use it, the United States has the opportunity to increase the fear-hesitancy of potential adversaries beforehand. In other words, adopting China's proactive policy and mutating it into something more overt and explicit (combined with superior US technological innovation and rule of law) can expand US cyber capability beyond its current covert, reactive roles. This is not an argument to disband covert action or remove reactive capacity. Rather, it is an admission that these two latter spheres simply do not equip the United States with an effective deterring cyber capability. Adding a proactive, offensive, overt "third strategic wheel" to this domain might do so.

The importance of this issue was confirmed by the head of US Cyber Command, Gen Keith Alexander, testifying before the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities in 2011:

> We believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for

> destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are proliferating into national arsenals and possibly beyond. . . . Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.[13]

For those aware of the innate difficulty of cyber deterrence reactively keeping ahead of cyber attacks, this confession from General Alexander only makes it more compelling to allow discussion of a new overt mind-set in US cyber strategy that strives to prevent these deadly new weapons from being used. In some ways Alexander is close to this very conclusion but misses the final connection:

> We see frequent media reports on nations contemplating the creation of their own cyber commands. . . . *There is a rough, de facto deterrence at the strategic level of cyberspace. Although no one knows how a cyberwar would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way.* This concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects (emphasis added).[14]

In developing offensive cyber weapons for overt strategic use, states make it known how devastating and cost-punitive a potential cyber strike would be. In essence, it is simply adjusting the general's vision—by making the costs of cyber war overtly explicit, it becomes every state's self-interest to engage in cyber restraint. Alexander intimates that such restraint has already developed to a certain degree because of the unknown fear (but clearly perceived assumption) that an all-out cyber war would be disastrous. As such, the most logical path is to try to intensify that perception through overt cyber strategy and thus raise restraint even more. The argument here seeks to answer the "why it matters" question and begin changing the original strategic mind-set. With such an argument in place, it will then be appropriate to broaden and deepen the project into blazing potential "how to" trails. This in fact makes analytical sense; namely, there can be no relevant "game planning" if the strategic state mind-set remains unaltered.

Is US Cyber Command already blazing that trail on its own? When considering the five strategic initiatives below, as detailed by General Alexander, it seems clear that it is not:

1. Treat cyberspace as a domain for the purposes of organizing, training, and equipping, so the DoD can take full advantage of its potential in military, intelligence, and business operations;
2. Employ new defense operating concepts to protect DoD networks and systems;

3. Partner closely with other US governmental departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cybersecurity;
4. Build robust relationships with US allies and international partners to enable information sharing and strengthen collective security; and
5. Leverage the nation's ingenuity by recruiting and retaining an exceptional cyber work force and enable rapid technological innovation.[15]

There is nothing faulty or inappropriate with the above strategies. The issue is that the United States is not fully considering all the strategies available. US cyber policy remains too wedded to reactive defensive measures. When it considers proactive offensive measures more akin to Chinese strategy, they remain within covert operations. This is fine to facilitate the two goals of USCYBERCOM—to protect US freedom of action in cyberspace and to deny freedom of action in cyberspace to all adversaries—but it is not enough as a holistic strategy to achieve the desired change in the global cyber mind-set, where the use of cyber weapons becomes as abhorrent as using nuclear weapons.

The focus on possible cyber improvements should be strategic. Not all cyber initiatives must be reacted to in kind. Theoretically, it will always be possible to react to a cyber attack with, for example, a drone strike. Logistically, however, such reactions might be worse than the initial action. As such, while answering cyber with cyber should not be considered inevitable and exclusive, it could be the best strategic response in the end. This would be a loose inspiration from the Chinese example, where cyber often seems a preferred initiative over direct military maneuvers.

Perhaps partial explanation for this strategic flaw is that the United States does not have a healthy fear of kinetic asymmetry like China and Russia. Viewing kinetic asymmetry as "everyone else's problem," the United States could actually fall behind other states in terms of innovative cyber strategy. China's concern over conventional asymmetry clearly led to greater investment in proactive and offensive cyber measures. Since the United States does not worry about such asymmetry, it seems stuck on measures that are reactive, covert, and defensive. This overconfidence limits the potential reach and deterrent impact of a new US overt cyber strategy.

Leading cyber states excel at increasing the effectiveness of covert virtual weapons. The United States in fact is the prime leader. But it remains a poor representative in pushing forward an agenda of overt strategic cyber transparency where cyber becomes more about preemption and deterrence rather than inferior surprise and reaction.

Zero-Sum Game, Part I
The Strategic Power of Overt Transparency

The potential risks in cyberspace have always been on policymakers' minds. The stakes were made clear in the president's *National Cyberspace Policy Review*:

> With the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations . . . and individual rights. The government has a responsibility to address the strategic vulnerabilities to ensure that the US . . . together with the larger community of nations, can realize the full potential of the information technology revolution.[16]

Clearly, a constructive cyber environment—globally expansive in its positive conformity while limiting free riders and violators—is essential. Alas, the drive to create such an environment seems based on idealistic beliefs that do not conform to the real world. As stated by Mikko Hypponen at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2009, "in the end, it is just about good versus evil." The United States will not co-opt through paramilitary structures, like China, nor will it coerce through shadowy criminal networks, like Russia. So how does it motivate global cyber netizens to positive behavior? Apparently, this seems to rest on creating enough trust in states "doing the right thing."[17] Given the counterculture ethos of the cyber domain, this goal seems hyper-idealistic, if not outright irresponsible.

If the choice is between a system of deterrence based on idealistic governmental altruism or on a realist fear of retaliatory punishment and strategic first-strike restraint, the latter (again, loosely inspired by Chinese strategic thinking) is not only more easily achievable but also more effective. It would appear, however, that contemporary conventional wisdom does not agree. This is partially based on an attempt to force just war theory unchanged into the cyber domain and to misread what the rules of strategic cyber deterrence ought to be, as Randall Dipert notes:

> It is also true that Just War Theory, having been endorsed by most industrial democracies and in international law, has acquired the status of damage-minimizing convention. However, the increasing number of nations, especially non-Western ones, who show no serious effort to endorse or follow this convention—and the

> unwillingness of other nations to force compliance—means that the advantage of a widely accepted convention is lost; it merely handicaps nations with the developed public sense of morality and prevents them from moral intervention.[18]

This public sense of morality handicaps well-meaning nations, because they are trying to create compliance on the backend of a process, reactively and covertly, when such compliance is more likely when accompanied by an equal strategy on the frontend, proactively and overtly. Focusing on ethics, morals, and trust to motivate compliance in the cyber domain is irrational at the very least because of how easy it is to attack anonymously. Flipping this process and inverting the motivational stimuli produces a system of compliance independent of goodwill and ethical behavior: not purely defense, but offense; not purely covert, but overt; not purely reactive, but proactive; not hoping to inspire trust, but forcibly compelling fear. The cyber domain is not so different that the guiding principle of international relations cannot apply—fear plus self-interest equals peace. It is simply about realizing that covert and overt cyber activity function best not as zero-sum, but as yin-yang.

This idealistic normative thinking is even more dubious when the limitations of a so-called cyber cold war are supposedly elaborated:

> It is relatively clear what the reasonable (and thus moral) constraints on Cyber Cold War would be. There should be little targeting of strictly defensive computer control systems. There should be no attacks that disable or panic global financial or economic systems. There should be no power interference in the vital economic and security interests of a major power.[19]

These proposed behavioral rules about *jus in cyber bello* are paradoxical: with so many constraints on allowable action, the underlying motivational framework of fear—so essential in the original Cold War in moderating behavior—becomes nonexistent. Indeed, if the above parameters were observed, then a state could arguably be *more* motivated to attack. Remove the civilian population and domestic infrastructure from cyber attack, and you have sanitized cyber war to a point where there is no fear of engagement.

> A Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private companies or even individuals or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic and constitutionally free countries, which national governments can easily rein in these potential corporate and individual cyber attackers.[20]

The problem with this formulation is that it envisions a so-called cyber cold war beholden to apparently *voluntary* parameters of constraint. The parameters elaborated, however, do not honor but corrupt the true deterring force that existed in the Cold War. If an overt strategy of credible cyber debilitation were allowed to openly develop, then most of the problems mentioned above would be inconsequential to the proper functioning of the virtual global commons—multilateral or bilateral, individuals or groups, national governments or private corporations, clearly defined adversaries or anonymous, nonattributable attacks. A system that does not rely on arbitrary good behavior and instead proactively establishes overt cyber-weaponization strategies alongside continued covert capabilities creates an environment where the futility of first-strike efficacy and perceived retaliatory devastation reigns in behavior globally.

The United States tends to be obsessive about keeping its technological capabilities classified. This is partially explained by the need to maintain effective surprise in retaliation to an attack rather than striving to prevent an attack initially. Yet, it is also explained by the US attempt to be the leading voice for liberally idealistic global cyber norms. This was confirmed in 2008 when former intelligence official Suzanne Spaulding testified before the House Cybersecurity Subcommittee.

> My concern is that (the Department of Defense) has been so vocal about the development and deployment of [classified] cyber-warfare capabilities that it will be very difficult for that department *to develop and sustain the trust necessary to undertake essential collaboration on defensive cybersecurity efforts* with the private sector and with international stakeholders. . . . There is significant risk that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal (emphasis added).[21]

There are two problems with the above quote. On the one hand, policymakers continue to focus on apparent voluntary trust in a domain that is not typified by such behavior. On the other hand, the DoD remains steadfast in its worship of clandestine capability and thus loses the preemptive deterrence of overt strategy which can compel cooperation as opposed to just hoping for it. These are not small problems, as trust and collaboration between dangerous actors work when there is an element of consequence to poor action. An overt strategy of offensive cyber capability—revealing some cards while not revealing all, with no nod to ethical considerations that demand targeting constraints and a focus purely on the efficacy of preemptive deterrence—arguably has a chance to shine a light of consequence into the shadowy anarchy of cyber. This is how the United States, as mentioned at the beginning of this article, could be inspired by the essence of Chinese cyber strategy, but it must ultimately elevate to a higher capability and competence.

Further hindering this evolution, the academic community has remained too enamored with trying to connect ethical theories into the cyber domain to create a liberal, idealistic governing code. Many scholars have acknowledged that these theories, whether utilitarianism, Kantian theory, or natural rights theory, have cast relatively little new light into the cyber domain.[22] Despite such sincere if misguided efforts, the best possibility for preemptive cyber deterrence might be old-school strategic realism and not new-school ethical liberalism.

As awkward as it may be to admit publicly, the Chinese might have something for the United States to truly consider. A fusion of Sun Tzu's pragmatism with Machiavelli's overt strategic amorality carries the potential to deter negative cyber action before it ever begins. As Sun Tzu asserted, the highest realization of warfare is to attack the enemy's plans; next is to attack its alliances; next to attack the army; and the lowest is to attack its fortified cities. Machiavelli made it clear that if an injury has to be done to a man, it should be so severe that his vengeance need not be feared. This overt, amoral offensive fusion has one purpose: not to *logistically* conduct war but to *strategically* avoid it. At the present time there is no current discussion of US cyber strategy broaching these subjects, and subsequently, the zero-sum cyber game remains unchanged.

Zero-Sum Game, Part II
Cyber Domain and International Law: Can Fear Be the Duty to Assist?

Unlike cyber crime, the international community has not achieved an agreed-upon consensus for cyber rules. This leaves existing international law no choice but to try to apply by analogy. While the application is not perfect, there are at least three general prescriptions to state conduct in cyberspace, according to law professor Duncan Hollis.

1. States must not launch a cyber attack that qualifies as a use of force absent UN Security Council authorization or pursuant to a state's inherent right to self-defense.

2. States must not employ cyber attacks within armed conflicts that violate the laws of war. States must avoid cyber attacks that target civilian objects, cause indiscriminate harm, or violate the rights of neutral states.
3. States must respect the sovereignty of other states in responding to any cyber attacks that do not constitute a use of force. . . . States cannot respond to cyber attacks directly if it would interfere with the sovereignty of another state.[23]

The most controversial argument here is the idea to purposely and openly violate the above three precepts, or at least create believability that such violation will occur, to instill the compelling credibility of fear. Such overt strategy can create compliance improvement when considering the duty to assist (DTA), as Hollis suggests, using a rescue-at-sea analogy.

> International law needs a new norm for cybersecurity: a duty to assist, or DTA. . . . As yet, there is no DTA for the Internet. But an SOS for cyberspace, an e-SOS, could both regulate *and* deter the most severe cyber threats. Unlike proscriptive approaches, a DTA would not require attribution to function effectively; those facing harm would not need to know if it came from a cyber-attack, let alone who launched it. A DTA would seek to redress unwanted harms directly, whatever their cause. It would do so by marshaling sufficient resources to avoid or at least mitigate that harm. If it does so effectively, attackers may think twice about whether it is worth the effort to attack at all (emphasis in original).[24]

The overall purpose of the DTA is correct: to deter the worst potential cyber behavior. It is by no means a false deterrence ploy; it is the rightful obligation of states to assist in an investigation not only to help, but also to improve their own trustworthiness and remove suspicion of complicity. The flaw, once again, comes in focusing on the backend of the process, seeking to reactively reduce harm. It uses the terms *deter* and *avoid*, but in actuality the DTA is truly centered on the terms *redress* and *mitigate*. An overt proactive cyber strategy is about deterrence and avoidance, which would make issues of redress and mitigation less necessary.

Hollis wanted to legally establish an e-SOS that would better deter cyber attacks by rendering states more resilient in the face of threats.[25] He is accurate in diagnosing the problem but is unable to connect to truly new strategy because of moralistic hand-wringing that restricts discussion to reactive and defensive measures of mitigation. In other words, the intellectual community has focused so exclusively on the aftermath of an attack that it basically does not consider the potential promise in overt, proactive strategies that might preempt attacks.

This becomes obvious when considering two concepts used in the law of armed conflict, reflecting the fundamental differentiation between principles that govern the legal decision to use force in international relations (*jus ad bellum*) and conduct/behavior during times of war (*jus in bello*).[26] Trying to seamlessly apply these principles to the cyber domain has proven consistently thorny.

> Both traditional elements of deterrence seem to be considered unsatisfactory for the purposes of cyber deterrence. . . . *Whilst cyber deterrence does not abandon the approach based on influencing potential adversaries' mind-sets, it will most likely have to rely on different methods to achieve this desired effect* (emphasis added).[27]

Changing the strategic mind-set of cyber thinkers requires one to recognize it is easier to leverage influence *before* conflict takes place than *after* hostilities have begun. The flaw is in the failure to connect higher-purpose ethical considerations to a harder strategic core; the argument is not that the United States must *never* consider the parameters and limitations in cyber war once underway. Rather it is about the need to address these concerns by enacting an overt strategy that can prevent cyber attacks. Perhaps one other reason this bridge-building has not been attempted is because of the general consensus that cyber weapons cannot be used for coercive purposes or do not instill fear as easily as nuclear weapons. But in reality, this might not matter.

Cyber Deterrence: Voodoo Magic or Simple Classic Realism?

Although the work of Martin Libicki is extremely well-known among cyber experts, a relatively little-emphasized point in a recent article that discussed the ability (or inability) of cyber war to have strategic impact is crucial here:

> If cyber war is going to assume strategic importance, it must be able to generate effects that are at least comparable to, and preferably more impressive than, those available from conventional warfare. . . . More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to the leaders—so frightening that the aggressors can actually read some gains from the reaction or concession of their targets. . . . It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the *threat* to use cyber weapons may be similarly unimpressive. . . . Nuclear

> arms fostered fear, but there was not a great deal of doubt or uncertainty in their applications. Cyber may be the opposite—incapable of inducing real fear directly, but putatively capable of raising the specter of doubt and uncertainty (emphasis in original).[28]

Libicki is right in how the fundamental debate is framed. So how can a new strategic line of thinking answer some of his concerns? Perhaps the inability of cyber to achieve true strategic importance is not based on its inability to instill fear, but rather the policy community's reluctance to cross the ethical Rubicon and consider a system whose aim is to achieve credibility in using real-time cyber lethality overtly. The goal is not to turn cyber weapons into some sort of voodoo magic. Rather, it is to fuse cyber weapons with classical realism, whether through propaganda or public testing. If the perception of a first cyber strike becomes irrational because of a "proven" retaliatory capability, then Libicki's legitimate concern about the credibility of cyber lethality will be surmounted. Overcoming this concern is essential, as it brings the deterring equilibrium of fear without having to engage in actual cyber war.

With a system that can at times overtly advertise these requisite skills, the United States would no longer need to convince adversaries of its omniscience or magic. Adversaries would only need to believe in rational self-interest that good behavior will avoid debilitation and bad behavior carries severe consequences. Ironic as it may seem, perhaps the key to developing this overt cyber strategy of preemptive deterrence, ensuring more reliable behavior across the virtual commons, comes about by being creatively inspired by an authoritarian state like China and adopting more strategically amoral rules of conduct in cyber war that so far have been relatively forbidden by the American scholarly community.

This is not to say the United States should do away with defensive efforts or covert weapons or cyber spies. Rather, it is an entreaty to allow American virtual patriots to employ offensive cyber capabilities for strategically overt preemptive purposes rather than solely as logistically covert reactionary weapons. This is not an argument against the relevance of the latter, but it is an explanation of how the former might lessen their need. The overt and covert aspects of US cyber strategy are better understood as yin and yang. They are not zero-sum. Change that strategic mind-set in the uniquely American ways discussed here, and US cyber dominance will be unchallenged for a long time to come.

Notes

1. Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 1–24.

2. China's First Aircraft Carrier Enters Service," *BBC*, 25 September 2012, http://www.bbc.co.uk/news/world-asia-china-19710040.

3. James Fallows, "Cyber Warriors," *Atlantic* 305, no. 2 (March 2010).

4. Gunter Ollman, "Asymmetrical Warfare: Challenges and Strategies for Countering Botnets," in *Proceedings of ICIW 2010: The 5th International Conference on Information-Warfare & Security*, 509–14 (Reading, UK: Academic Conferences International, 2010).

5. George Patterson Manson, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict, *Comparative Strategy* 30 (April–June 2011): 122–33.

6. Don Reisenger, "Chinese Military Warns of US Cyber Threat," *cnet.com*, 16 June 2011, http://news.cnet.com/8301-13506_3-20071553-17/chinese-military-warns-of-u.s-cyberwar-threat.

7. Scott D. Applegate, "Cyber Militias and Political Hackers—Use of Irregular Forces in Cyberwarfare," *Security & Privacy* 9, no. 5 (September/October 2011): 16–22, http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6029351.

8. Clay Wilson, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues* (Washington: CRS, 19 July 2004), "Summary."

9. Ibid., 3.

10. Fallows, "Cyber Warriors."

11. Manson, "Cyberwar."

12. Hjortdal, "China's Use of Cyber Warfare."

13. Gen Keith Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 5.

14. Ibid., 7.

15. Ibid., 8.

16. Quoted in Col James Cook, "Cyberation and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics* 9, no. 4 (December 2010): 411–23.

17. Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February/March 2011): 41–60.

18. Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 394.

19. Ibid., 403.

20. Ibid.

21. Suzanne Spaulding, quoted in Shaun Waterman, "US Needs Cyber-offensive," *Space War*, 29 September 2008.

22. Giles Trendle, Cyberwars: The Coming Arab E-Jihad, *Middle East*, issue 322, April 2002.

23. Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (Summer 2011): 393–95.

24. Ibid., 378.

25. Ibid., 426–29.

26. Ulf Haeussler, "Cyber Strategy and the Law of Armed Conflict," in *Proceedings of ICIW 2011: The 6th International Conference on Information-Warfare & Security*, 99–105 (Reading, UK: Academic Conferences International, 2011).

27. Ibid.

28. Martin Libicki, "Cyberwar as Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 135–37.