World Gone Cyber MAD

How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence

Matthew D. Crosston

In the unseen reaches of cyberspace, our enemies are quietly taking the postmodern form of warfare we witnessed on September 11 to a new level: they are no longer just transnational—they are non-national, hiding and attacking in a world where there are no borders. They are no longer just stateless—they are place-less. And they are no longer virtually invisible—they are, well, virtual.

—Alan W. Dowd, *Fraser Forum* (2008)

Many cyber experts say the United States is woefully ill prepared for a sophisticated cyber attack and that each passing day brings it one step closer to a potential virtual Armageddon. While the problems hindering the development of an effective and comprehensive cyber deterrence policy are clear (threat measurement, attribution, information-sharing, legal codex development, and poor infrastructure, to name several), this article focuses on one aspect of the debate that heretofore has been relatively ignored: that the futility of governmental innovation in terms of defensive efficacy is a relatively constant and shared weakness across all modern great powers, whether the United States, China, Russia, or others. In other words, every state that is concerned about the cyber realm from a global security perspective is equally deficient and vulnerable to offensive attack; therefore, defensive cyber systems are likely to remain relatively impotent across the board.

The United States tends to view this problem as if it has a unique burden to bear. While smaller states that do not envision a global role for themselves fear a massive cyber attack far less than the United States, this is not necessarily true of the aforementioned states and others that wish to

---

Dr. Matthew Crosston is director of the International Security and Intelligence Studies Program and chair of political science at Bellevue University. A graduate of Colgate and Brown, he has specialized in issues of national security, especially in regards to democracy promotion, terrorism prevention, and new concepts in future conflict. He also works to promote interaction abroad between intelligence agencies that share common interests but are without channels of connectivity.

be important global players. As a consequence, the goal for major powers should not be the futile hope of developing a perfect defensive system of cyber deterrence, but rather the ability to instill deterrence based on a mutually shared fear of an offensive threat. The United States is better positioned by shifting to an open, transparent policy that seeks to infer deterrence from the efficacy of its offensive cyber capabilities. This strategy has greater probability of staying ahead of rival deterrence systems and establishing the perception amongst rivals that the United States would indeed have effective second-strike capabilities if attacked. True, the goal for any major power would be to achieve dominance over such capabilities (such is the way with great powers), but this would also result in the problem of cyber security morphing into a zero-sum game where one state's dominance increases the insecurity of all others. For this reason it is logically more stable and potentially peaceful to have a system of deterrence that is structured mutually across major powers, giving no one state the ability to disrupt cyber equilibrium.

If adopted, this policy shift could hold the same potential that made nuclear mutually assured destruction (MAD) so effective for so long without being physically challenged through global war. Nuclear deterrence initially built off of the expected second-strike capability of being able to survive an initial strike long enough to launch an equally devastating counterstrike. But over time—as the great nuclear powers continued to build up huge arsenals—the de facto effectiveness of nuclear deterrence was not so much based on the likelihood of a second-strike capability but rather on the acceptance by all players that engaging in the nuclear game would inevitably bring devastation to all. A logic of deterrence emerged from an admission of being defenseless.

Perhaps it could be so with this new cyber "MAD"—in an open and transparent offensive system of cyber threat, each major player in the global system would come to fear debilitation equally and therefore would not risk being the first-strike initiator. By capitalizing on this shared vulnerability to attack and propagandizing the open buildup of offensive capabilities, there would arguably be a greater system of cyber deterrence keeping the virtual commons safe. Though it may seem oxymoronic, the more effective defense in this new world of virtual danger is a daunting cyber-lethal offensive capability; not so much to actually use it, but rather to instill the fear of it being used. And while the anarchic chaos and freedom of the Internet will always be a haven for nonstate actors looking to inflict

damage upon state systems, an open and transparent cyber-MAD policy would systematically give major powers the second-strike capability to potentially influence and deter these nonstate actors as well. Presently, defensive cyber deterrence systems basically give these actors free reign.

Interestingly, some states are clearly already adhering to this strategy, at least in the informal sense if not in explicit policy position—China's fervent support of "honkers" and the Russian Federation's frequent reliance upon "patriotic hackers" come to mind most readily. The United States certainly has the technological capability to equal Chinese and Russian virtual lethality. The formal lack of an open policy arguably indicates hesitancy on the part of the United States to develop a "weaponized virtual commons." Rather than an indication of infeasibility, this reluctance seems to be a nod to intelligence considerations, meaning the United States is arguably more satisfied developing its offensive capabilities in secret as part of more-covert operations than as a piece of overt policy. This article argues the emphasis on covert offensive capability rather than overt is an error that compromises the effectiveness of American cyber security.

The Need for a New Doctrine, New Questions, and New Answers

Institutional inertia and doctrinal rigidity are often major obstacles blocking policy reform and may even hinder the emergence of new policy ideas. However, in the cyber realm these blockades are not nearly as entrenched as other security issues/principles. For the past 10 years cyber security has become an increasingly important area of national interest; however, the cyber security context is a completely new era of thinking and dangers. It was not until late in the second term of Pres. George W. Bush that more definitive efforts were made across agencies to explicitly develop something akin to a national cyber doctrine (most vivid in this governmental newness was the 2009 creation of US Cyber Command). As analyst Mark Young recently argued,

> A national cyber doctrine is necessary. It is the link between strategy and the execution of the missions of the national security sector. Doctrine may traditionally be a military notion, but agencies are acknowledging the wisdom of establishing guiding principles. A national cyber doctrine can be a vehicle used to define the roles of departments and agencies for the entire U.S. government. In contrast to a presidential executive order or a National Security Council directive, a doctrine is developed in an openly collaborative fashion.[1]

This evidence attests to the absence of an open, overt, well-defined policy guiding long-term American interests over the issue of cyber security. Young rightly acknowledges that an explicit and well-defined cyber policy is essential to developing a comprehensive and effective cyber security system, largely because of the intense complexity inherent to cyber attacks and cyber deterrence. He continues,

> The nature of network attacks makes a well reviewed cyber doctrine particularly important, since national security leaders will have little time to consult with the National Security Council or the Commander in Chief when faced with an attack that could devastate the national economy, corrupt the flow of commerce, or disrupt military supply chains. Due to technical challenges, counterstrikes remain a time-consuming proposition. Disruption of a cyber attack is more easily achieved but may not be accomplished in time to protect critical data or national security systems.[2]

The main concern addressed by this article is that the debate to create a unified, explicit, and truly national cyber doctrine does not openly acknowledge the most basic axiom of the cyber realm: offense will always trump defense which, therefore, will not include all potential options and strategies.

To wit, the language cyber analysts and specialists use is inherently defensive—it is always about the problematic nature of counterstrikes, the technical challenges to disrupt an attack in progress, and lamenting the offensive advantage adversaries have over defensive specialists. These laments are real, but they inexplicably fail to lead the United States to the one potentially effective elephant sitting in the room that remains ignored or consistently talked around: the national cyber doctrine of the United States should not be based on defensive measures that are always going to hopelessly lag behind offensive measures, but rather on offensive capabilities that would give the explicit perception to potential adversaries that any aggressive maneuver will trigger debilitating retaliatory attacks more severe than any initial transgression—a true cyber-MAD policy, initially enshrining second-strike capability and, one would hope, institutionalizing the deterring admission of first-strike futility.

Some excellent work is already being done on the types of questions that need to be asked when considering cyber security options. While most of these questions presently address cyber deterrence from a purely defensive stance, the more important ones are still relevant for a cyber-MAD policy:

- Should the target reveal the cyber attack?

- When should attribution be announced?
- Should cyber retaliation be obvious?
- Is retaliation better late than never?
- Can there be confrontation without retaliation?[3]

All of these questions are incredibly important but have decidedly different answers, depending on what type of cyber-security system is being built. A purely defensive system rooted in intelligence secrecy produces ineffective answers that leave gaps in the national security infrastructure. Answers provided by an open, transparent, and offensive cyber-MAD policy would be aggressive and explicit enough to close these gaps by capitalizing on the logic and efficacy of nuclear deterrence. Openness and transparency render the "dilemma" of revealing targets and attribution problems moot, while a focus on offensive capability not only gives stronger teeth to retaliation but also creates the possibility of effective confrontation without retaliation and, ultimately, the avoidance of engagement outright. This was arguably the true legacy of peace left by nuclear deterrence. Could a cyber-MAD policy not produce the same hope?

One counterargument would answer no to that question: it is still impractical and unrealistic to think a cyber-MAD system can be effectively developed. There are simply too many problems in developing and guaranteeing that "mutually assured debilitation" can be achieved and, even if achieved, guaranteeing it can bring about the necessary threat deterrent to prevent or limit cyber attacks. In this case scholarship must be careful not to become purely academic and simply policy curmudgeons—stating that the cyber realm is a hopelessly offensive arena where deterrence based on defensive techniques cannot be effective, while also stating that a cyber deterrence system based on offensive technologies is equally impractical and ineffective. In other words, there is a tendency to declare that defense does not work *and* offense does not work simultaneously. This creates a scholarly and policy dead end, hopelessly charging intellectual windmills and getting nowhere.

Russian Rumors

The near virtual shutdown of Estonia in 2007 coincided with the Estonian government's decision to move a Soviet-era war memorial. In essence, the entire virtual framework within Estonia was inundated and overwhelmed

with "junk" for a period of three weeks. This essentially compromised if not temporarily crippled the Estonian communications network, as newspapers, mobile phones, emergency response systems, and the state's largest bank were all targeted. In addition, a concentrated attack effort was aimed at the offices of the president, prime minister, parliament, and the foreign ministry.[4]

The relevance of this attack, however, highlights some of the problems for developing an effective cyber deterrence system: even though Estonia intimated that it was able to trace some of the attacks to Russian government offices, it did not in fact establish any direct governmental links. Russia always maintained that the attacks came from renegade cyber nationalists, acting according to their own sense of warped patriotism but not on the orders of any official government office or agency. It is more a testimony to the state of global public perception that no one today believes the Russian version of the attacks and takes for granted the Estonian version—there never was a definitive "smoking gun" piece of evidence proving formal Russian governmental policy as the chief culprit in the Estonian attacks.

This is a perfect real-world example of the attribution problem often theorized by cyber specialists: it is often too difficult to accurately trace a cyber attack to its origin. Perhaps worse still, in cases where an origination point can at least be compellingly argued, there is still no definitive way of proving just who was "at the trigger point" launching the attack. Solving both of these issues would be essential for the development of a truly effective cyber deterrence system. An inability to prove culpability severely hampers any efforts to enact defensive measures. It really is as simple as "how do you know who to retaliate against if you cannot be sure who threw the virtual punch?" You cannot, and as a consequence any effort to build an effective cyber deterrence system emerges already deeply compromised.

Chinese Reality

Perhaps the only other state associated with cyber attacks and cyber espionage today as much as the Russian Federation is China. As early as the late 1990s the United States accused China of attacking various governmental agencies and attempting to infiltrate American nuclear facilities. Around the time Estonia was being attacked and accusing Russia, Germany had several infiltrations into governmental agencies and placed blame on China. Just as with the Estonian case, both the United States and Germany,

despite their adamant conviction of knowing who to blame, did not in fact have any real evidence linking the Chinese government to the detected incursions.[5]

This is no small matter and not an issue of blame semantics. The international community's response to evidence of direct governmental involvement in a cyber attack against another state could very easily be to consider it an act of war, even if at the moment a war of lesser degree. Accurate attribution, therefore, is of highest importance, as it could lead to the commitment of military forces and expose a state to the most serious of consequences—battlefield casualties. Any cyber deterrence system must therefore be capable of overcoming the attribution problem to be relevant in the most important issue of all—state security. It is clear that the world, not just the United States, is currently incapable of devising a system that can overcome this problem.

Unlike Russia, which has always been extremely secretive about its cyber activities and steadfast in its denial of engaging in any state-sponsored cyber attacks, China has been surprisingly open about its belief in the need and appropriateness of establishing an army of cyber warriors. China actively recruits and facilitates support of some of its more brilliant, locally developed hackers, called "honkers." Unabashed in their virtual patriotism, honkers espouse a philosophy that "the best defense is a capable offense." They do not consider themselves necessarily employees of the government or members of the Chinese intelligence community; they simply believe that China needs to be protected from adversaries. If it is brought to their attention that another state or corporation is initiating harmful maneuvers against their country, then it is their obligation to respond in kind. Note that responding in kind is not simply stopping a cyber attack but rather formulating a retaliatory cyber strike that is in fact more intense and more comprehensive than the initial strike.

In some ways this reality gives argument to the possibility of cyber war existing above and beyond conventional war; not because conventional war will ever be obsolete or be a state's most supreme form of security, but rather cyber war can be seen by many states as a less confrontational and more results-oriented maneuver. Effective hacking and strategic cyber attacks at the moment still hold many more opportunities for hiding participation while successfully gaining economic, political, diplomatic, and military secrets. In simple cost-benefit calculations, cyber war is much more cost effective than conventional war, so it is arguable that its popularity

over time will grow exponentially. When considering the impotence of defensive systems tasked with stopping such efforts, cyber war as a concept is fundamentally complex, convoluted, and diffused by design. These characteristics would at least be challenged by an open and transparent cyber-MAD system in ways present cyber deterrence methods do not.

At the moment it is fair to assume that Chinese honkers are not explicitly attempting to create a cyber version of the nuclear-MAD theory, but this does not mean they have not created such a policy in their de facto actions. What seems inarguable is that China has decided there are no ethical considerations in the cyber realm. In fact, it is easy to see how a state could make the counterargument—if cyber war will not necessarily involve immediate and direct bloodshed due to the cyber attacks, then ethical handcuffs can be freely removed from state considerations. More importantly, China has given the rest of the world a theoretical blueprint justifying such a policy—the honkers' offensive philosophy is not based on any sense of vindictive bloodlust, but rather a careful calculation of what is truly effective in the cyber realm: defensive capabilities are hopelessly compromised; therefore, only offensive threats have the potential to deter enemy initiatives.

In some ways this thought process has already been supported by none other than the current vice-chairman of the Joint Chiefs of Staff, Gen James Cartwright, who argued in 2007 before the Strategic Forces Subcommittee of the Senate Armed Forces Committee that it was "time to apply the principles of warfare to the cyber domain . . . and the defense of the nation is better served by capabilities *enabling us to take the fight to our adversaries* when necessary to deter actions detrimental to our interests."[6] Cyber deterrence as it is currently being envisioned does not carry this capability and does not enable the United States to take the fight to adversaries. This is not an attempt to beat the reader incessantly with a dead cyber horse, but is rather the necessary emphasis on how the United States clings to defense. It seems determined to fit this square peg into a round hole, even if to its own security detriment. As politically uncomfortable as it may be to model something important to US national security after Chinese hackers, it is clear at the moment honkers are more openly and successfully applying the principles of warfare to the cyber domain. The United States, meanwhile, refuses to transparently engage and develop its own possibilities and capabilities and therefore remains the more vulnerable cyber target.

Countercyberspace

A fascinating development, perhaps inspired by the admonishment of General Cartwright, comes with the concept of *countercyberspace*, defined as "a function consisting of operations to attain and maintain a desired degree of cyberspace superiority by the destruction, degradation, or disruption of an enemy's capabilities to use cyberspace."[7] This work comes from a new conceptualization of Air Force basic doctrine and is an admission of the need to produce new thinking (though arguably through the application of tried and true old-war ideas) to the realm of cyberspace and its defense. The issue at hand is of course trying to establish "cyberspace superiority," which AF Doctrine Document 2-11, "Cyberspace Operations," draft version defined as "the degree of advantage possessed by one force over another that permits the conduct of operations in cyberspace at a given time and place without prohibitive interference by the opposing force."[8] When taking these concepts and definitions into consideration, it becomes starkly clear how ineffective cyber deterrence will always be as long as it is a system constructed from defensive priorities. In the cyber realm a defensive system by default puts a state back on its governmental heels and does not contain the potential to conduct operations without prohibitive interference. America's cyber doctrine must achieve this capability.

In May 2007, President Bush ordered the National Security Agency (NSA) to conduct a cyber attack against cell phones and computer networks that Iraqi insurgents had used or intended to use in roadside bombings. The NSA complied, and its subsequent success essentially knocked out what was up to then an effective insurgent communications network. Many military analysts credit that effort with being monumental in turning the tide of the war.[9] It is true a cyber MAD cannot be exactly like nuclear MAD. It is not semantics when destruction is replaced by debilitation. So, while the analogy may not match up perfectly, it does work effectively, based on the fact that war in the twenty-first century has arguably moved away from being global and apocalyptic to something more regional and temporarily damaging. As such, the weapons in a cyber-MAD policy do not destroy states to sand and glass but simply cripple and incapacitate them across realms that are crucial to their effective functioning and governance. Such damage is not insignificant.

Clearly, the United States has the technical capability and the strategic aggressiveness to conduct such operations. It must now conceptualize an offensive mind-set to begin defending cyberspace. The problem to this

point has been its relatively limited sphere of utilization—the Iraqi example was a case of open and explicit war aimed at a target that was actively and aggressively attacking American military personnel. Granted, this may not be as politically clean, but it can be dramatically more effective in limiting adversaries who are motivated to attack the United States or other countries across the virtual commons. Keep in mind that in the twenty-first century, cyberspace is no lesser space to guard. It is true news media will not be able to show body counts or bloody battlefields when a country is victim to a massive cyber attack, but the devastation and destruction of such an attack in many ways can be more comprehensive and far-reaching.

Lacking Infrastructure

The logical arguments for a cyber-MAD policy become even more compelling when the technical obstacles facing a true defensive cyber deterrence are examined in full. For the past 10 years the United States has invested heavily in cyber-security technologies. Despite this commitment and investment, major problems remain across the most fundamental areas. There is still no large-scale deployment of security technology capable of comprehensively protecting vital American infrastructure.[10] The need for new security technologies is essential, but to date the best developments have only been in the small-to-medium-scale private research facilities. What would be required to make rapid, large-scale advances in new network security mechanisms is daunting:

- development of large-scale security test beds, combined with new frameworks and standards for testing and benchmarking;
- overcoming current deficiencies and impediments to evaluating network security mechanisms, which to date suffer from a lack of rigor;
- relevant and representative network data;
- adequate models of defense mechanisms; and
- adequate models of the network and for background and attack traffic data.

Most of these issues are problematic because of the severe complexity of interactions between traffic, topology, and protocols.[11] In short, it is simply easier to attack than to defend in the cyber realm, and the innate com-

plexities of infrastructure preparedness make it seem likely this is not just an estimation of current affairs but rather an axiom that will stand across eras. Hackers will always trump defenders. The United States must not waste time attacking the virtual windmill when it already has the technology, talent, and capability to create a different policy path.

One counterargument to this rejects that the cyber realm will remain inherently dominated by offensive capabilities. The most often praised defensive measures that are allegedly catching up to offensive threats (IPV-6 and gateway technologies) are unfortunately a bit of an overstatement, as the cyber arena is never static—whatever defensive countermeasures are developed, one can rest assured there will be answers to those measures. And offensive answers so far have always outpaced the defensive "improvements." There is nothing in the foreseeable future that seems to truly challenge this basic reality. The United States should indeed continue to develop, improve, and refine its defensive technologies. But it should not be so naïve as to think it will ever be capable of developing a defensive deterrence that will continuously and routinely outwork and outmaneuver offensive threats. It simply does not seem that the structure of the cyber realm will allow this reality to emerge.

The Asymmetric Nature of Cyber Warfare

The United States' failure to enter the cyber arena offensively, as a reflection of open and transparent policy (or even to create the perception of willingness to offensively engage), has only exacerbated the asymmetric nature of cyber attacks. The commercialization, standardization, and low cost of high technology around the globe make waging cyber campaigns dramatically more simplistic than defending against them. Quite literally a dozen determined programmers are capable of threatening the US logistics network, stealing operational plans, blinding intelligence capabilities, or hindering the ability to deliver weapons on target.[12] This was never more obvious than in 2008, when the Department of Defense suffered a significant intrusion into its supposedly secured military networks. An infected flash drive was inserted into a military laptop in the Middle East. Placed there by a foreign intelligence agency, the drive succeeded in releasing malicious computer code that was able to spread so far and so deep into classified and unclassified information that it was considered akin to establishing a "digital beachhead."[13]

These examples perfectly illustrate the potential nastiness and futility of fighting against asymmetry. This is an innate structural problem that cannot be overcome, because of the nature of technology and the free market. The Internet was designed to be open and accessible, not only for ease of use among the most basic of consumers but also to encourage and foster low barriers to innovation. As a consequence, offense will always have the upper hand.[14] But instead of letting the logic of this reality lead America into a new conceptualization of "offensive defense," the thinking of the United States is entrenched in a defensive mind-set that can only result in a compromised system of deterrence.

Though asymmetry makes staying ahead of attacking adversaries highly doubtful, Lynn argues that this only emphasizes the need for the United States to be more adaptable to constantly adjust and improve its defenses. He even says that old, Cold War traditions of deterrence (models of assured retaliation) will *not* work in cyberspace due to the aforementioned attribution problem, making it nearly impossible to know just who to retaliate against. Therefore, deterrence is supposed to be about successfully denying the benefits to an attacker, rather than trying to impose costs through aggressive retaliation.[15]

While this article testifies to the problem of attribution, this does not lead to an argument for moving away from old models of retaliatory deterrence but actually the reverse: a retaliatory cyber model would not be about who to launch missiles against, but rather enforcing the perception of massive technological/infrastructural debilitation if even the suspicion of an attack is determined and attributed. Nuclear MAD was successful not because various states actually launched nuclear weapons; it succeeded because of the conviction across all parties that an attack of this nature would be so universally destructive that the cost far outweighed any potential benefits. A cyber-MAD model has to operate on this same principle, only with virtual weapons rather than kinetic ones. If done successfully, essentially weaponizing the cyber doctrine of the United States, then it becomes prohibitively expensive for an adversary to risk an attack.

This is not in fact arguing for the creation of some cyber variant of a Dr. Strangelove doomsday machine, the repercussions of which would solve the attribution problem. Taken to its extreme extrapolation, a cyber-MAD policy does deter as nuclear MAD—the perception of realistic virtual devastation via retaliatory strike does induce fear of action, thereby rendering the global system safe through dangerous, but stable, equilibrium. Just as

with nuclear weapons, the ability to universally destroy the virtual commons cannot be the ultimate hope for peace across the system. This is not an argument for giving the president a choice between surrender or hacking the modern world into the Middle Ages. Rather, a cyber-MAD policy—by being open, transparent, mutual, and offensive—would have enough new deterrents built into it structurally to not only provide more options but also give pause to rogue behavior that might probe its edges.

Recall that mutuality not only builds fear but this same fear also allows the possibility of trust through repeated engagement. Up to now the dynamic nature of the cyber realm too heavily favored those who would do damage against it. Cyber MAD would finally put some of that dynamism in the hands of major powers with a mutual interest in rules, regulations, and stability.

Cyberwar, Cyber Deterrence, and Political Complexity

Trying to study the consequences of the cyber realm's impact on war and conflict is a hornet's nest of political complications. Even when trying to develop a purely defensive, non-attacking system of protection, there is a preponderance of complex considerations. How can one be sure of the attacker? Can assets be held at risk when under suspicion of a cyber attack? Does retaliation send the right message to the defending side? Should there be a threshold for a response? How do you avoid escalation?[16] All of these questions pose problems not just because they are complicated but because the nature of a defensive cyber system exacerbates the flaws within such policy rather than eliminating them, and yet other questions arguably emerge only because of these inherent flaws in a defensive mind-set.

Complexity is reduced when considering the development of a cyber-MAD policy, but admittedly it may place the United States in an uncomfortable political position at first. Consider just war theory. In the first instance, jus ad bellum, when states may lawfully consider going from peace to war, there are at least three immediate criteria most states would prefer to have on their side: right purpose, duly constituted authority, and last resort.[17] A cyber-MAD policy would be especially harsh on each criterion: the policy does not operate on only going to war in self-defense, since the nature of cyber security precludes any real notion of being able to effectively defend against a massive cyber attack; there is also the risk of cyber MAD circumventing proper governmental notification because total

debilitation would depend in large part on the element of surprise, which works against premeditated transparency and openness; and finally, cyber MAD by its very nature is the antithesis of last resort—the effectiveness of the position comes from not being purely retaliatory but potentially preemptive, indicating a willingness to use virtual weapons in more than just desperate circumstances.

Many would argue that from a purely political/diplomatic perspective these positions appear somewhat untenable. This would be true if cyber MAD were set up structurally so that the United States dominates these offensive capabilities alone and de facto, becoming a virtual tyrant vis-à-vis the other great powers. But as argued earlier, the inherent structure of the cyber realm makes such a goal, even if logical for a great power, highly unlikely and nearly impossible. Therefore, all states pursuing cyber MAD would be relatively equal in their weaponization efforts. This allows for the possibility over time for the perception of equal debilitation to take effect and arguably create similar deterrence stimuli as nuclear MAD.

The initial political and diplomatic discomfort associated with cyber MAD does not improve when considering jus in bello, or the desire to have states maintain principles of justice while in war. Again, three main criteria can be highlighted: noncombatant immunity, proportionality, and more good than harm.[18] A cyber-MAD policy would still have the major benefit of any cyber defense system: that it is relatively bloodless. However, the benefit does start to become more ambiguous under cyber MAD; a massive strike against a state's infrastructure, debilitating important societal mechanisms and functions, would almost certainly result in noncombatant suffering and thereby not guarantee immunity in the most formal sense. Proportionality clearly cannot be met simply because the point of a cyber-MAD policy would be to secure defense through retaliatory second-strike *nonproportionality.* It would be the guarantee of that nonproportional response/strike that would bring about the deterring impulse. Finally, the criterion of more good than harm under cyber MAD really would be, in the end, a completely arbitrary interpretation based on which side and whose security goals were being considered.

Little work has been done to date on an explicit conceptualization of an offensive and transparent cyber strategy to heighten national security. What has been done achieves a general consensus that there are three obvious ways a state could create the capability to inflict damage on another state or nonstate adversary via cyber attack. The first option is simply creating

the capability through one's own forces and technologies. The second is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the supporting government. The third option is to outsource at least parts of the problem to other governments, commercial entities, or criminal underworld organizations in a quasi-mercenary model.[19] Each option clearly carries its own flaws.

Both China and Russia formally and informally dabble with options one and two. States like Iran, North Korea, and Nigeria have been at least cursorily connected to option three. Perhaps this is the largest difficulty impacting the politics of American policymaking—it seems plausible that the United States is simply reluctant to consider a shift in policy that would so clearly associate it with this group of countries, no matter what the advantages. Of the three options, option one has the best chance of consideration by the United States, as this homegrown policy would at least be arguably controllable and explicitly defined by American democratic institutions with their inherent checks and balances informed by principles of transparency and accountability.

The United States does indeed have the capability of developing cadres assigned to the task of developing a weaponized cyber realm. But where this has been done so far has been on a small scale and in highly classified areas. These characteristics make it an obvious *attacking* capability structured most effectively for use in the context of open aggression and war rather than as it is ultimately needed—as a *deterring* capability meant to prevent said aggression from occurring during times of peace. Again, the greatest advantage with cyber MAD is not in truly achieving a *usable* second-strike capability but in creating over time the believability in such retaliation so the second strike is never required.

The other two options afford no such chance of a truly governable, accountable policy and are not likely to be considered by the United States. This article does not challenge the premise that initially a cyber-MAD policy would place the United States in some rather awkward political positions. Rather, it takes the more quintessentially Machiavellian position that national security is best managed by efficacy and control, even at the expense of diplomatic image and public perceptions of righteousness.

Conclusion

Most analysts, military specialists, and government officials admit that life in the twenty-first century will include cyber attacks. There is no vision of a world free from such attacks. This simple admission undermines the efficacy of a cyber deterrence system whose reason for being is the prevention of such attacks. This article is not so contrarian as to argue anarchically for abandonment of the effort to achieve real cyber security. Rather it asks that certain structural realities finally be given equal intellectual space at the discussion table and allow that space to entertain new options and possibilities. There are two structural realities in particular that should be emphasized. First, in the cyber realm offense always dominates and always will. It is structural and axiomatic. Second, the capabilities, technology, and talent already exist to institute this system within the United States. What is needed is a change in mind-set and encouraging new ideas and policies—transparently. Not easy by any means, but still achievable.

The imposition of a cyber-MAD policy could prove more effective, even though it may make the United States uncomfortable politically and diplomatically. The debate continues and the argument remains: greater cyber security can be achieved by mutually assured debilitation for all. SSQ

Notes

1. Mark Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law and Policy* 4, no. 1 (2010): 173–96.
2. Ibid.
3. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).
4. Arthur Bright, "Estonia Accuses Russia of Cyberattack," *Christian Science Monitor*, 17 May 2007, http://www.csmonitor.com/2007/0517/p99s01-duts.html.
5. Alan W. Dowd, "Are We Ready for WWI?" *Fraser Forum,* September 2009, 12–14.
6. James Cartwright, "Statement before the Strategic Forces Subcommittee of the Senate Armed Services Committee," 28 March 2007.
7. Eric D. Trias and Bryan M Bell, "Cyber This, Cyber That . . . So What?" *Air and Space Power Journal* 24, no. 1 (Spring 2010): 90–100.
8. Ibid.
9. Ibid.
10. Ruzena Bajcsy et al., "Cyber Defense Technology Networking and Evaluation," *Communications of the Association of Computing Machinery* 47, no. 3 (March 2004): 58–61.
11. Ibid.
12. William J. Lynn, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010).
13. Ibid.
14. Ibid.

15. Ibid.

16. Libicki, *Cyberdeterrence and Cyberwar.*

17. Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," *Proceedings of the 9th European Conference on Information Warfare and Security* (Reading, UK: Academic Publishing, Ltd., 2010), 177–82.

18. Ibid.

19. Rain Ottis, "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability," *Proceedings of the 8th European Conference on Information Warfare and Security* (Reading, UK: Academic Publishing, Ltd., 2009), 177–82.