Many cyber experts state that the United States is woefully ill-prepared for a sophisticated cyber-attack and that each passing day brings us 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 piece 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 that be the United States, China, Russia, Iran, India, Great Britain, France, etc). 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 and therefore defensive cyber systems are likely to remain relatively impotent across the board. Like the nuclear realm before it, a cyber M.A.D. doctrine (in this case, ‘mutually assured debilitation’) may be scary but it also may produce more peaceful behavior from all sides.

The United States tends to view this problem as if it has a unique burden to bear. While it is true smaller states that do not envision a global role for themselves fear being the victim of a massive cyber-attack far less than America, this is not necessarily accurate when considering the aforementioned states and others that see themselves as 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 for major powers to instill deterrence based on a mutually shared fear of offensive threat. This strategy has greater probability of staying ahead of rival deterrence systems and at least establishing the perception amongst rivals that the United States would indeed have effective second-strike capabilities in the event of an attack. 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 problems 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 at least logically more stable and potentially peaceful having a system of deterrence that is structurally mutual across major powers, giving no one state the ability to disrupt cyber equilibrium. If adopted this policy shift could ultimately hold the same potential that made nuclear M.A.D. so effective for so long without being physically challenged through global war: at first nuclear deterrence builds off of the expected second-strike capability, of being able to survive an initial strike long enough to launch an equally devastating counter-strike. 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 survivable second-strike capability but rather on the obvious acceptance by all players that engaging in the nuclear game would inevitably bring about devastation to all. A logic of deterrence emerged from an admission of being defenseless.

Perhaps it could be so with this new cyber M.A.D. – 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 build-up 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 measure of defense in this new world of virtual danger is to have a daunting cyber-lethal offensive capability. Not so much as to actually use it, but rather to instill the fear of it being used. And while the anarchical chaos and freedom of the internet will always be a haven for non-state actors looking to inflict damage upon state systems, an open and transparent cyber M.A.D. policy would at least systematically give major powers the second-strike capability to potentially influence and deter these non-state actors as well. Defensive cyber deterrence systems basically give these actors free reign presently.

Interestingly, there are clearly states already adhering to this strategy, at least in the informal sense if not in explicit policy position (China and its fervent support of ‘honkers’ and the Russian Federation’s frequent reliance upon ‘patriotic hackers’ come to mind most readily). The United States most certainly has the same 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 being an indication of unfeasibility, 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 rather 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.

While this article testifies to the famous problem of attribution in the cyber domain (ie, not being to truly determine who was responsible for an attack), 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 figuring out who to launch missiles against, but rather enforcing the perception of massive technological/infrastructural debilitation if just the suspicion of an attack is determined and attributed. Nuclear M.A.D. was successful not because various states actually did launch 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 of an attack far outweighed any potential benefits. A cyber M.A.D. model has to operate on this same principle, only with virtual weapons rather than real-time ones. If done successfully, essentially weaponizing the cyber global community, then it becomes prohibitively expensive for an adversary to risk an attack.

Keep in mind that in the 21st century, cyberspace is no lesser space to guard – it is true that news agencies 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. While this article by no means ends the debate about how we should police the virtual commons and how we should develop our individual state cyber policies, it is hoped that an argument has been produced here that will force a place at the table for a cyber-position that can ensure greater general security by proposing ‘mutually assured debilitation’ for all. We still have to address important issues of asymmetry in the cyber domain, where states like the US might indeed be sincerely worried about its own vulnerabilities but other states around the globe need to be concerned about American power applied to cyber action and their own inabilities to off-set or countermand such actions. Would the above ideas/philosophy be an answer to such asymmetry? For now it is hard to say as so few engage formally in the ideas listed above. But one thing seems clear: it would certainly be a step towards greater overall global security simply because it shifts states’ thinking from being anarchically secretive, covert, and virtually violent with its capabilities to being more caution-oriented and unmotivated to risk using such power. And any such shift would help all states in an asymmetrical system of cyber power as the true objective becomes not one of dominance but one of deterrence.
Dr. Matthew Crosston is Professor of Political Science and Director of the International Security and Intelligence Studies program at Bellevue University, exclusively for the online magazine “New Eastern Outlook”.