2011

Foreword, Strategic Insights

Clarke, Richard

Strategic Insights, Vol. 10, Issue 1 (Spring 2011)
http://hdl.handle.net/10945/29625

Foreword

Richard Clarke

"As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare…it has become just as critical to military operations as land, sea, air, and space." These words, written by Deputy Secretary of Defense William Lynn last fall in *Foreign Affairs*, cemented the status of cyberspace as a domain of warfare like all others, and coincided nicely with US Cyber Command reaching its full operational capacity. Yet, suggestions of a strategy in the pages of this article and subsequent publications from Cyber Command and its four-star commander, Keith Alexander, belie the fundamental fact that the United States military, government, private sector, and citizenry are all seriously vulnerable to cyber attack and that we have no coherent plan to protect America. "Active defense," by which Cyber Command means going offensive first, is not a strategy that will protect this nation. If anything is clear, it is that we have a remarkably well-developed offensive capability, but no commensurately serious commitment to defense. There is neither a plan nor any capability to defend America's civilian infrastructure, from banking to telecoms to aviation. Perhaps the most important thing Americans can do to make us safer from cyber war is to discuss it, openly, in academic journals, to debate aspects of cyber war in Congress, and to educate the public and the world through mass media. Thus, this volume by the Naval Postgraduate School is an important step in improving our security as a nation.

Given the central importance of net-centric warfare to our current military doctrine, I fear that this lack of clear thinking with regards to defense in cyberspace leaves not only our military, but our society as a whole, highly vulnerable to cyber attack. It will not be the first time that initial adopters of a new military technology, overcome with inertia or overconfident in the weapons they love and consider supreme, fail to defend effectively against that which they have just created. Thus it was that while American Colonel Billy Mitchell was the first to recognize the capability of small aircraft to destroy battleships, it was the Japanese Imperial Navy that most effectively harnessed this knowledge and nearly defeated the Americans in the Pacific during World War II. Great Britain invented the modern tank and a French Colonel, Charles de Gaulle, developed the first tactics of rapid attack with massed tanks supported by air and artillery. However, it was the Germans that perfected the tank design during the interwar period and employed de Gaulle's tactics with horrific efficiency in what they referred to as blitzkrieg. I fear that we may be on the precipice of a similar situation in cyber war, one that may leave the American military hamstrung and the US civilian infrastructure shredded.

Unlike the conventional examples from history, however, the threat to the United States in cyberspace will very likely not come from an adversary developing superior offensive capabilities. Rather it will be from one who can most effectively exploit the inherently asymmetrical nature of cyber war. While the notion of asymmetry in warfare is as old as the profession itself, its implications have rarely been so great as they are when placed in the context of cyber. To confront the United States military in conventional terms is a losing proposition; no other military today can surpass its capabilities on a tactical or strategic level. Yet, the conventional supremacy of the Americans is predicated upon a highly vulnerable foundation, its complete reliance upon information technology. Computers and networks enable all elements of the defense apparatus to function. From units in the field to procurement officers to strategic planners, all communications pass through various computer networks. Navigational and weapons systems aboard planes and ships depend on highly

sophisticated networked hardware and software, to say nothing of the thousands of satellites that provide imagery of nearly every inch of the earth. While this high degree of networking has brought unprecedented levels of productivity and efficiency, they also expose the entire operation to serious vulnerabilities. From the insider threat, as demonstrated by the WikiLeaks incidents, to the attacks that compromised the classified SIPRNet, to the hacking of Secretary of Defense Robert Gates' personal computer, the examples of the vulnerabilities in cyberspace to our military abound. For this simple reason, the single most effective way to prevent units from communicating, procurements from taking place, or F-16s from properly acquiring targets, is to compromise chips and software in order to attack the network infrastructure and advanced weaponry of the net-centric giant.

Nevertheless, for all of the potentially devastating implications for the United States military in a cyber war, such a war is probably not imminent. What ought to be of far greater importance not only to the United States, but to all industrialized nations, are the consequences of the current pandemic of economic cyber espionage. Economic warfare, which takes the shape of espionage conducted on an industrial scale against private corporations in all sectors across the globe, is happening every day. Intellectual property, proprietary information, bid and financial data – anything that comprises competitive knowledge in the digital global economy – is a potential target. The risks associated with such large-scale intellectual property theft pose an existential threat to the foundations of a state's economic leadership, competitiveness, and well-being. In our inter-connected world mutual dependencies among states abound, and thus, it would be in the long-term interest of few states to seek conventional war that could easily disrupt the delicate architecture of the global village. However, as the global competition for economic primacy intensifies in a knowledge-based global competition, the value of intellectual property, from research and development to biotech formulas to engineering designs, will only increase. China, among other nations, is systematically stealing terabytes of data at low cost, financially and diplomatically, and passing that data to its own companies. Private firms, limited by finite resources and obligations to maximize profits, will always lose against state-backed hackers unbound by such concerns. Governments, in the interest of maintaining economic stability, must therefore protect private industry and start the process of establishing an arms control regime in cyberspace.

Arms control for cyber war is too often summarily dismissed with the question of attribution. Critics assert that if you cannot definitively determine who committed an attack, you cannot hold anyone accountable for violating an agreement. Definitely establishing the origin of cyber attacks is extremely difficult post facto, and in nearly all cases one only ends up with an educated guess. What the argument essentially says is that arms control in cyber war cannot work because it would be too hard to establish. This is a refrain that I encountered multiple times over the course of my career at the Pentagon, State Department, and White House. Whether it was conventional force reduction in Europe, nuclear weapons limitation and reduction with the Soviets, or international agreements on chemical and biological weapons, the initial reaction invoked, without fail, the "it's too hard" argument. Yet we did, after long negotiations, draw down troop levels in Europe, and limit and reduce the numbers of nuclear weapons in our arsenal and ban chemical and biological weapons. With persistence, there are solutions. A way around the attribution problem may be to include in an international agreement on cyber arms control an Obligation to Assist clause. Such a clause would require states party to share information on attacks as they were taking place, and would require that states cut off computers engaged in malicious activity, as confirmed by other parties and an international monitor. Such a convention obviates the attribution issue. The responsibility for malicious traffic rests with the state in which the malicious traffic originates, regardless of whether the actual attacker is located within its borders. I concede that this proposition is not perfect, but it

is perhaps the basis of a discussion that must begin now, because the risks are too grave and despite the associated difficulties, there is a great potential for good.

Given the gravity of the implications of activities in this new domain of war fighting, it is vital that our national strategy be comprehensive, serious, and reflective of an open and frank debate, not just within the corridors of the Pentagon, but with academia and the broader public. Though the new Defense Department documents may suggest otherwise, "active defense" and "going first" do not constitute such a strategy. Again, I find myself reminded of historical precedent. In the early days of nuclear strategy, the Pentagon refused to share information regarding policies governing the use of nuclear weapons with anyone, let alone university professors. Yet as it became clear that the military's plan to strike first with the entire nuclear arsenal was not an optimal strategy, civilian officials began to see the value of having academics like Bill Kauffman and Herman Khan dissect and analyze this all too important topic. Those whom Fred Kaplan has called "wizards of Armageddon" brought a much-needed critical eye to the nuclear strategy debate, and slowly backed the nation away from the dangers of a policy governed by a hair trigger. We need a similar debate today regarding cyber war. Should the US government keep secret its knowledge about software vulnerabilities that put the US economic infrastructure at risk? We do not know can who initiate cyber operations against a foreign entity, nor do we know how we would respond if we were the victims of a cyber attack. At what point would we respond kinetically? When does the response require presidential approval? These are but a small fraction of the number of critical, yet unanswered, questions about the national cyber strategy that need to be addressed. Fortunately, this journal and others like it are beginning to explore precisely these kinds of questions and analyze the issues associated with cyber war, work that will undoubtedly ultimately contribute to making us all safer.