War and Peace

The Cyber Edition

— BY NEAL POLLARD

On May 26, 2011, President Obama released his administration's International Strategy for Cyberspace, which stated that, as a last resort, the United States reserves the right to respond to cyber attacks with conventional military force. Additionally, the Defense Department's new strategy for cyber security reportedly will consider that computer sabotage coming from another country can constitute an act of war. A military official was even quoted saying, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks." Since these reports, pundits have opined on how unprecedented this is, how things have changed, what should or could possibly constitute an act of war, and even that a state of war currently exists between the United States and other nations.

But there is little new here from a security perspective. The notion the president will use the military, if need be, to protect the nation from hostility is as old as the nation itself, and the advent of cyber conflict does not change that basic fact. Even Obama's declaratory policy, while novel at the pPresidential level, has some precedent: in 1998 testimony to the Senate Government Affairs Committee, Lt. Gen. Ken Minihan, then-Director of the National Security Agency, suggested that a large-scale cyber-attack by a foreign government against U.S. computers could be considered a weapon of mass destruction, saying "we perhaps ought to consider adding information infrastructure threats to our definition of weapons of mass destruction." [2] What is new, however, is a requirement now, for a new policy and operational framework that raises the military's unique capabilities in cyberspace to the level of a national resource, bridging the gap between military cyber capabilities, and those of civilian agencies and the private sector, clarifying when and how that gap should close.

Legally speaking, the United States has an inherent right to self-defense, and the president is obligated to use all instruments of national power, including the military, to defend the nation from all attacks, including cyber attacks. Politically speaking, the United States is in a state of war when – and only when – the president or the Congress says it is. Practically speaking, there is a finite set of circumstances in which a cyber attack would be widespread and threatening enough that only the military has the unique capabilities necessary to prevent or respond.

In these circumstances, such an attack would also likely take place in a geopolitical context, where something else is going on in the "real" world, probably related to the cyber event. The attacks against Georgian networks in summer 2008 are an example, when cyber events occurred roughly the same time Russia invaded Georgia.

The issue at hand is not what kind of cyber attacks should be considered an act of war demanding a conventional military response. It is neither necessary nor desirable for the president to stipulate what he would consider a cyber act of war. Drawing boundaries eliminates options – rarely a good thing for a president – and even in cyberspace there is value in Thomas Schelling's notion that ambiguity strengthens deterrence by the "threat that leaves something to chance."

If the United States is at war, then the military is clearly the lead federal agency, even in a cyber war.

Rather the issue at hand is gaining a deeper understanding of, and creating an interagency planning framework around, what kind of cyber events – intentional or accidental – would necessarily involve the military in a lead or supporting role, how the military should make the best use of its full set of capabilities as a national resource, and how it can support the lead of civilian agencies and the private sector in securing cyberspace, establishing trust, and responding to failures. Here, there are two sets of circumstances to consider: when the military would be the lead agency for response, and when it would be in support of civilian authorities. Drawing even that distinction is not easy.

If the United States is at war, then the military is clearly the lead federal agency, even in a cyber war, as the president has made clear. The military can expect a lead role in conducting cyber operations from a political perspective – the Commander-in-Chief so orders it – or from the perspective of perpetrators or consequences of cyber events. Clear involvement of a state in a cyber event, societal-level damage such as national power grid failure, or loss of life and physical damage, would likely see the military leading the response, as would specific targeting of military systems that degrade the nation's ability to defend itself, or insertion of malicious software in the cyber-supply chain of weapons programs. But theft of information, even widespread, is at worst espionage, and is neither an act of war nor an incident calling for the unique capabilities of the military. Sabotage is a gray area, but again, it is not a new concept – the president would consider the response based on the attributed perpetrator, intentions, and effects of the attack, as well as the broader costs, benefits, and consequences of possible response options.

Military involvement does not necessarily presuppose armed aggression, kinetic response, or even an intentional failure. There are circumstances today in which civilian agencies lack the capabilities to respond to natural or manmade crises, and must request military action in a supporting role. Here the issue is, what is the policy, operational and legal framework for the Defense Department – especially the National Security Agency – to support civilian authorities such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), or even the private sector, in responding to significant cyber events? Are there such circumstances, well short of armed conflict or societal grid failure, in which DHS or FBI will lack the technical capabilities to respond, and will require the support of the military, similar to how DHS requires the support of the military via Northern Command in Colorado, in responding to natural disasters or catastrophic physical events? It is comparably easy to draw a border around a real-world disaster zone, where governors request Federal assistance, statutes such as the Stafford Act make routine Defense support to civilian authorities, and military capabilities support DHS. However, in the event of a cyber failure, how does one draw the disaster zone boundary, who is the "governor" or indeed any government official requesting federal assistance, when will military capabilities be required, and what are the appropriate statutory and operational frameworks by which DOD will support Federal civilian authorities, let alone the private sector? Or, should the United States replicate the cyber capabilities of the DOD within DHS, and what are the resource implications of that? What are the respective expectations and assumptions among FBI and the Departments of Homeland Security and Defense, for when the military will be involved and in what capacity, and how are those expectations and assumptions reflected in departmental strategies, plans, and resources?

The creation of U.S. Cyber Command (USCYBERCOM) in 2010 provided a military combatant command authority and structure, analogous to U.S. Northern Command, but it is less clear how this structure would support military integration with civilian authorities, and under what circumstances. Although DHS co-locates cyber personnel with USCYBERCOM, the commander of USCYBERCOM (a combatant command) is also the Director of the National Security Agency (an intelligence agency). The director of an intelligence agency directing cyber activities on U.S. infrastructures or in support of U.S. companies implicates numerous legal and operational issues. Unless, and until, DHS replicates the military's capabilities, legal, policy, and process issues will remain, and will present even more of a response challenge than an obvious act of war in cyberspace.

Even a potential kinetic response to cyber threats poses challenges beyond speculation of what constitutes an act of war. The White House should be commended on announcing its policy. Cyber is a unique domain that challenges traditional international legal concepts like necessity, proportionality, and attribution in responding to attacks. Cyber attacks that are used to preclude or prevent a war might not look different from a preemptive attack. Concerns about disclosing our intelligence capabilities to deconstruct and attribute a cyber attack might undermine our ability to make a compelling legal case for a kinetic response. These issues do not, however, require defining what constitutes an act of war. Even attribution, while a technical challenge, will be mitigated by the current geopolitical context and political judgment. The president need not be held to judicial standards of proof in attribution, and indeed the United States has been to war over less.

What is important is that planners consider how to position the Defense Department – especially USCYBERCOM and the NSA – as national resources, to provide their unique capabilities and technical skills for attack detection and characterization, response, and foreign intelligence insights to protect civilian government and private-sector critical infrastructure networks. This requires first characterizing the circumstances in which military capabilities would truly be required, the range of possible responses to such events if they appear intentional, and how different agencies' capabilities work in tandem to respond across the spectrum of the cyber failure –prevention, detection, attribution, response, and recovery. In this respect, definitions and plans are less important than the planning process that produces them, as this will be the process that enables the United States to stay proactive in the event of a crisis. U.S. behavior in response to a cyber attack will set an important precedent, both in international law and in cyber operations for armed conflict among allies and adversaries. It would be best if this response is carefully considered in advance and guided by deliberate planning, rather than, ad hoc, reactive, and driven by crisis.

Toward this end the nation would benefit from a new policy and operational framework, led by the White House, that provides guidance, structure, and authorities for when military capabilities are uniquely necessary to respond to cyber attacks and events, under what circumstances, and how they should be used, especially in support of civilian authorities and the private sector. This framework would provide a means to implement the president's strategy for cyberspace, as well as a mechanism for integrating and coordinating the respective cyber strategies of the Departments of Defense, Homeland Security, and Commerce. In support of strategy integration, this process would also help set expectations and assumptions, and facilitate decisions and resource planning, on when the military should be in the leading or supporting roles of response. This framework would also highlight for the Congress legislative authorities still required to meet national strategic requirements for cyber security. This framework would enable operational concepts and planning to streamline military response and support to civilian authorities and the private sector, in the event of severe crises or attacks in cyberspace. Finally, this framework will establish a foundation for predictability and expectations, for both the Departments of Defense and Homeland Security as well as the private sector, for when and how the military will play an active role in responding to national-level events in cyberspace, while balancing the multiple public policy imperatives of security, economic viability, civil liberties, and public/private partnership. By providing these benefits to the nation's security, economy, and social vitality, this framework would help the U.S. government meet the president's stated national values for cyber space.

There are other long-term steps the U.S. government can take, looking toward the future. In the context of cyber conflict, the United States is truly at a stage analogous to the 1950s and the advent of nuclear weapons – not comparable to the destructive capability of nuclear weapons, but rather to basic questions of strategy, planning, organization, and doctrine. How should the U.S. military organize, recruit, train, and equip around cyber capabilities? What does the resultant force structure look like? What is the difference – in technology, operations, law and policy – in offensive and defensive capabilities, or in intelligence and military operations, and what are the consequent implications for force organization and command? While it might be difficult, and even undesirable, to parse civilian vs. military "targets," are there concepts comparable to "counterforce" vs. "countervalue" calculations, that have merit in cyber conflict planning? Is it possible, or desirable, to orient arms control policies or mechanisms around certain classes or uses of cyber technology, e.g., selling or bundling of zero-day exploits? What do escalation ladders and "confidence-building measures" look like? How intrusive can "active defense" options be, what are the operational or legal constraints (international and domestic) of specific options (and under what circumstances), and how do traditional notions of sovereignty hold up against active defense?

The creation of USCYBERCOM and Service components such as the 24th U.S. Air Force represent a step to adapt the current military command structure around cyber operations. However, USCYBERCOM's subordination under U.S. Strategic Command (USSTRATCOM) – also the command responsible for the nation's strategic nuclear forces – poses basic issues for how the commander of USCYBERCOM reconciles his dual reporting to both the commander of Strategic Command and the director of the office of National Intelligence, let along the questions of strategy outlined above. Yet the placement of USCYBERCOM under USSTRATCOM holds many long-term implications about the unique nature of cyber conflict, in that USSTRATCOM is the lead command, and wields the weaponry for, only two types of conflict: nuclear and cyber. These implications ought to be explored in a deliberate enterprise, not ad hoc and in the heat of a crisis, and preferably outside the bounds of the "Washington Beltway," where the urgent and tactical frequently drowns out the important and strategic.

How should the U.S. military organize, recruit, train, and equip around cyber capabilities?

In the early 1950s, the RAND Corporation rose to answer very similar questions, also focused on the business of USSTRATCOM – to wit: how should the United States conduct warfare in the nuclear age? RAND's work offered answers at multiple levels, from how nuclear weapons fit within the order of battle, to high questions of nuclear strategy, including deterrence, containment, the doctrine of Mutually Assured Destruction, and Herman Kahn's *On Thermonuclear War*. It was intellectually and geographically located outside the din of the Washington Beltway, and it made an indelible impact on how the United States considered the role of nuclear technology in its military capabilities and doctrine, organization, policy, diplomacy, and national security strategy.

There might be value today in the U.S. government creating a new research and development think-tank, devoted to the long-term study of the role of cyber technology and operations within military and geopolitical strategy. Like with RAND, located in Santa Monica, California, any such endeavor should be located outside of Washington, D.C. – perhaps Palo Alto, California; Newport, Rhode Island; or Austin, Texas. Its mandate and research effort should be unbothered by current buzz of technological fads and what they mean for security, convenience, or communication, but rather focused on long-term trends, how they can be shaped, and what they mean for strategy. Technological innovation can be a driver of strategy development, given intellectual distance from the "tyranny of the inbox." This is more so, and more important, when crafting long-term strategy around capabilities, whose underlying technology can change dramatically within a single governmental budget cycle. Within four years a social networking platform—Facebook—went from connecting college students across the Ivy League to connecting reformers and protesters that changed the political landscape across the Arab world, possibly beyond. The United States defense community has the mission to avoid technological surprise. That imperative should continue in cyberspace. ■

Neal Pollard is an Adjunct Senior Fellow for Cyber Policy at FAS and a principal at PRTM Management Consultants, where he focuses on strategic cyber security, risk management and resilience, homeland security, and bio-defense in PRTM's Global Public Sector practice." Pollard is the author of the forthcoming book Strategic Cyber Security and Conflict: A Primer for Policymakers in an Age of Anxiety.