The Monroe Doctrine in Cyberspace

The following document expands upon remarks made by Mary Ann Davidson in testimony given on March 10, 2009 to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and. Technology.

The relevant section of testimony – one of three major points is included below for clarity:

A. Testimony Excerpt

3. We are in a conflict – some would say a war. Let's call it what it is.

Given the diversity of potentially hostile entities building cadres of cyberwarriors, probing our systems including our defense systems for weaknesses, infiltrating U.S. government networks and making similar attempts against American businesses and critical industries, is there any other conclusion to be reached? Whatever term we use, there are three obvious outgrowths from the above statement. One is that you do can't win a "conflict" – or war if you don't admit you are in one. The second is that nobody wins on defense. And the third is that we need a doctrine for how we intercede in cyberspace that covers both offense and defense and maps to existing legal and societal principles in the offline world. In short, Congress should consider developing a 21st century application of the Monroe Doctrine. The need for a framework to guide the government's role in response to foreign aggression is a point that Melissa Hathaway has already noted during her 60day interagency review of the Federal cybersecurity mission, and an area where this subcommittee can productively collaborate with the National Security Council.

For those a tad rusty on their US history, the Monroe Doctrine (introduced December 2, 1823) said that further efforts by European governments to interfere with states in the Americas – the Western hemisphere – would be viewed by the US as acts of aggression and the US would intervene. The Monroe Doctrine is one of our longest standing foreign policy tenets: invoked on multiple occasions by multiple presidents, including Teddy Roosevelt, Calvin Coolidge, Herbert Hoover and John Kennedy. We have, as the expression goes, sent in the Marines and the rest of our armed forces to support the Monroe Doctrine.

Note that the Monroe Doctrine did not detail the same intervention or even specific intervention for each perceived act of aggression, merely laid out "here is our turf; stay out or face the consequences" language that allowed great flexibility in terms of potential responses. Some may argue that cyberspace is "virtual" and unsuited to declared spheres of influence. But even Internet protocol (IP) addresses map to physical devices in physical locations we care about – critical infrastructures such as a server for a utility company in New York, for example, or a bank in California. By extension, any new U.S. government framework for cyberspace should also respect the global nature and shared ownership of cyberspace by mapping policies to existing legal and societal principles in the offline world.

The advantages of invoking a Monroe-like Doctrine in cyberspace would be to put the world on notice that the US has cyber "turf," (properly and narrowly scoped - we should not claim all cyberspace as our turf). And the second is that we will defend our turf. We need to do both. Now.

As I mentioned earlier, having a military response capability does not mean militarizing all elements of U.S. cyberspace any more than invoking the Monroe Doctrine meant necessarily creating permanent encampments throughout the Western hemisphere. Nor should a Cyber Monroe Doctrine lead to permanent government encampments in private networks, or become a mandate for unilateral intervention in all of cyberspace. With proper guidance, various government agencies and the private sector can find their natural role in guarding our cyber infrastructures in a framework similar to how we currently protect our real-world interests.

B. Discussion

1. The essential truth of invoking a Cyber Monroe Doctrine is that what we are seeing in cyberspace is no different from the kinds of real-world activities and threats our nation (and all nations) have been dealing with for years; we must stop thinking cyberspace falls outside of the existing system of how we currently deal with threats, aggressive acts and appropriate responses.

Referencing the Monroe Doctrine is meant to simplify the debate while highlighting its importance. The Monroe Doctrine became an organizing principle of US foreign policy. Through the concept of the Americas sphere of influence, it publicly identified an area of national interest for the US and clearly indicated a right to defend those interests without limiting the response. Today cyberspace requires such an organizing principle to assist in prioritization of US interest. While cyberspace by its name connotes virtual worlds, we should recall that cyberspace maps to places and physical assets we care about that are clearly within the US government's remit and interest.

Conceptually, how we manage the cyber threat should be no different than how we manage various real-world threats (from domestic crime to global terrorism and acts of aggression by hostile nation-states). Just as the Monroe Doctrine compelled the US government to prioritize intercontinental threats, a Cyber Monroe Doctrine also forces the US government to prioritize: simply put, some cyberassets are more important than others and we should prioritize protection of them accordingly. We do not treat the robbery of a corner liquor store with the same response (or same responders) as we treat an attempt to release a dirty bomb into a population center, for example. With this approach, policy makers also benefit from existing legal systems and frameworks that ensure actions are appropriate and that protect our civil liberties.

Similarly, not all European incursions into the Western hemisphere have warranted a response under the Monroe Doctrine. For example in 1831, Argentina, which claimed sovereignty over the Falkland Islands, seized three American schooners in a dispute over fishing rights. The US reacted by sending the USS Lexington, whose captain, Silas Duncan, "seized property taken from the American ships, released the American seamen,

spiked the fort's cannon, captured a number of Argentine colonists, and posted a decree that anyone interfering with American fishing rights would be considered a pirate"(The Savage Wars of Peace, Max Boot, page 46).

The territorial dispute ended in 1833 when Great Britain sent a landing party of Royal Marines to seize the Falklands. In this instance the US specifically did not respond by invoking the Monroe Doctrine; the Falklands were deemed of insufficient importance to risk a crisis with London.

2. The initial and longstanding value of the Monroe Doctrine was that it sent a signal to foreign powers that the US had a territorial sphere of influence and that incursions would be met with a response. Precisely because we did not specify all possible responses in advance, the Monroe Doctrine proved very flexible (e.g., it was 1later modified to support other objectives).[1]

It is understandable that the United States would have concerns about ensuring the safety of the 85% of US critical (cyber) infrastructure that is in private hands given that much of this critical infrastructure (if attacked or brought down) has a direct link to the economic well-being of the United States in addition to other damage that might result. That said, declaring a national security interest in such critical infrastructure should not mean militarizing all of it or placing it under military or other governmental control any more than the Monroe Doctrine led to colonization ("planting the flag") or militarization (military occupation and/or permanent bases) of all of the Western hemisphere.[2] Similarly, the US should not make a cyberspace "land grab" for the Western hemisphere, or even our domestic cyber-infrastructure.

A 21st century Cyber Monroe Doctrine would have the same primary value as the original Monroe Doctrine - a signal to others of our national interests and a readiness to action in defense of those interests. Importantly, any consideration of our cyber interests must be evaluated within the larger view of our national security concerns and our freedoms. For example, it is clear where the defacement of a government website ranks in comparison to a weapons of mass destruction (WMD) attack on a major city. All cyber-risks are not created equal nor should they have a precisely "equal" response.

Another reason to embrace a Cyber Monroe Doctrine (and the innate flexibility it engendered) is the fact that cyberspace represents a potentially "liquid battlefield."

---

[1] The government of the Dominican Republic stopped payment on debts of more than $32 million to various nations, which caused President Theodore Roosevelt to invoke (and expand upon) the Monroe Doctrine to avoid having European powers come to the Western Hemisphere for the purpose of collecting debts. This expansion of the Monroe Doctrine became known as the Roosevelt Corollary.

[2] As Max Boot notes in The Savage Wars of Peace, most of America's wars have been small wars, not large set pieces in which we have "sent in the Marines" (or other armed forces) in response to specific provocation and for specific purposes. In most cases, we had a military presence in a country for a period of time that varied depending upon what the stated goal was and how long it took to achieve it. Today, we have no permanent military presence in Haiti, the Dominican Republic, Venezuela, Mexico, China, the Marquesas, and other countries in which we have had military engagements – "small wars" – during our history (note: not all the above were the result of invocations of the Monroe Doctrine).

Traditionally, wars have been fought for fixed territory whose battlefields did not dramatically expand overnight (e.g., the attack by Imperial Japan on Pearl Harbor did not overnight morph into an attack on San Francisco, Kansas City and New York City). By contrast, in cyberspace there is no "fixed" territory and thus the boundaries of what is attacked are fluid. For a hostile entity, almost any potential cybertarget is 20 microseconds away.

A Cyber Monroe Doctrine must also accommodate the fundamental architecture of the Internet. Since the value of the Internet is driven by network effects, policies that decrease the value of the Internet through (real or perceived) balkanization will harm all participants. While a Cyber Monroe Doctrine can identify specific critical cyber infrastructure of interest to the U.S., parts of the cyber infrastructure are critical to all global stakeholders. In short, even as the United States may have a cybersphere of influence, there are nonetheless cybercommons. This is all the more true as attacks or attackers move through or use the infrastructure of those cybercommons. Therefore, the US must find mechanisms to be *inclusive* rather than exclusive when it comes to stewardship and defense of our cybercommons.

3. Placing the critical assets we care about within a framework that maps to existing legal, policy and social structures/institutions is the shortest path to success.
For example, military bases are protected by the military, and a nation-state attack (physical or cyber) against a military base or military cyberassets should fit within a framework that can offer appropriate and proportionate responses (ranging from State Department harassment of the local embassy official, to application of kinetic force). Critical national assets (power plants, financial systems) require similar flexibility, but through engagement of the respective front-line institutions in a manner that permits escalation appropriate to the nature of the attack.

C. Challenges

There are a number of challenges in applying a Cyber Monroe Doctrine. Below is a representative but by no means exhaustive list of them.

1. Credibility

A deterrence strategy needs teeth in it to be credible. Merely telling attackers "we are drawing a line in the sand, step over it at your peril," without being able to back it up with an actual and proportionate response is the equivalent of moving the line in the sand repeatedly in an attempt to appear fierce while actually doing nothing. (The Chinese would rightly call such posturers "paper tigers.") Mere words without at least the possibility of a full range of supporting actions is no deterrent at all. A credible deterrent can be established through non-military options as well - for some a sharply worded public rebuke may change behavior as much as if we were sending in the Marines.

Because the Monroe Doctrine did not detail all potential responses to provocation in advance, the United States was able to respond as it saw fit to perceived infractions of the

Monroe Doctrine on multiple occasions and over much of our history. The response was measured and flexible, but there was a response.

2. Invocation Scenarios

To bolster credibility, the "teeth" part of a cyber doctrine should include a potential escalation framework and some "for instances" in which a Cyber Monroe Doctrine would be invoked. This planning activity can take place in the think tank realm, the cyber exercise realm, or a combination thereof.

We know how to do this. Specifically, military strategists routinely look at possible future war scenarios.[3] In fact, it is not possible to do adequate military planning by waiting for an incident and only then deciding if you have the right tools, war plans, and defense capabilities to meet it, if for no other reason than military training and procurement take years and not days to implement.

Similarly, "changing the battlefield" could be one supporting activity for a Cyber Monroe Doctrine. For example, it has been argued that the United States only developed a strong Navy (and the centralized government that enabled it) as a result of the wars of the Barbary pirates. Similarly, the fabric of our military may change and likely will change in support of a Cyber Monroe Doctrine and that could include not only fielding new "troops" – the Marines first made a name for themselves by invading Tripoli – but new technologies to support a changed mission.[4] One would similarly expect that a Cyber Monroe Doctrine as a policy construct would be supported by specific planning exercises instead of "shoot from the hip" responses.

3. Attribution

A complicating factor in cybersecurity is that an attack - especially if it involves infiltration/exfiltration and not a "frontal assault" (e.g., denial of service attack) - and the perpetrator of it may not be obvious. Thus two of the many challenges of cybersecurity are detecting attacks or breaches in the first place, and attributing them correctly in the second place. No one would want to initiate a response to a cyber attack if one cannot correctly target the adversary. In particular, highly reliable attribution is critical in cyberoffense, since the goal is to take out attackers or stop the attacks, not necessarily to create collateral damage by taking down systems being hijacked by attackers. Notwithstanding this challenge, "just enough attribution" may be sufficient for purposes of "shot over the bow warnings," even if it would be insufficient for escalated forms of retaliation.

For example, in cybersecurity circles last year there were a number of discussions about the types of activities that occur when one takes electronic devices overseas (e.g., hard

[3] For example, 7 Deadly Scenarios, A Military Futurist Explores War in the 21st Century by Andrew Krepinevich includes a description of a future cyberattack.

[4] Very credibly in Power, Faith and Fantasy, America in The Middle East 1776 to the Present, by Michael Oren

drives being imaged, cell phones being remotely turned on an used as listening devices) and the precautions that one should take to minimize risk. While specific countries were not singled out on one such draft document (outlining the risks and the potential mitigation of those risks), the discussion included whether such warnings should be released in advance of the Beijing Olympics. Some expressed a reluctance to issue such warnings because of the concern that it would cause China to "lose face."

Ultimately, the concern was rendered moot since Joel Brenner, a national counterintelligence executive in the Bush Administration, otherwise made the topic public.[5] It seems ludicrous in hindsight that the concern over making a government "feel bad" about activities that they were widely acknowledged to be doing should be greater than protecting people who did not know about those risks. (Do we warn people against walking through high crime areas at night, or are we worried that criminals might be offended if we did so?) Even when we choose to exercise diplomacy instead of countermeasures, diplomacy inevitably includes some element of "you are doing X, we'd prefer that you not do so," if not an actual "cease and desist" signal.

The difficulty of proper attribution of non-state actors deserves specific attention because of the need for multi-stakeholder cooperation in order to identify and eliminate the threat. When an attacker resides in one location, uses resources distributed around the world, and targets a victim in yet another country, the authorities and individuals responsible for finding out who (or what) is behind the attack may only have portions of the information or resources needed to properly carry out their job. Taking a unilateral approach will at times be simply impossible, and may not offer the quickest path to success. However, working collaboratively with other governments and stakeholders not only builds our collective capacity to defend critical infrastructures around the world, but also ensures that our weakest links do not become havens for cyber criminals or terrorists.

While it can be at times harder in cyberspace to distinguish what kind of foe we face, a Cyber Monroe Doctrine will work best when we can clearly distinguish who is conducting an attack so that we can deliver the appropriate response. This is not an easy task, and will require new skill sets across the entire government to ensure cyber threats are properly categorized.

D. Sources

1. The Savage Wars of Peace: Small Wars And The Rise Of American Power by Max Boot

http://www.amazon.com/Savage-Wars-Peace-Small-American/dp/0465007201

2. 7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century by Andrew Krepinovich

http://www.randomhouse.com/catalog/display.pperl/9780553805390.html

[5] http://blogs.computerworld.com/slurping_and_other_cyberspying_expected_at_olympics

3. Power, Faith and Fantasy: America in the Middle East: 1776 to the Present by Michael Oren

http://www.amazon.com/Power-Faith-Fantasy-America-Present/dp/0393058263