A "New Monroe Doctrine" for the Law of Armed Conflict (LOAC) and the Use of Force in Cyberspace: Colonial Interests, US & Russian Expansionism, and The United States Doctrine

Susanna Cox | CX7
2022.04.05

In the early 2000s, as the world was beginning to understand the implications of “paperless” societies and the world wide web, many nations remained largely underprepared for the threats that cyber actions could pose to national security. After the historic 2007 cyberattacks against Estonia proved the potentially destructive capabilities that a tech savvy actor (or group of actors) could wield against even a well defended nation, governments scrambled to assemble comprehensive–and cohesive–cybersecurity policy.

The United States Doctrine on the use of force in cyberspace derives largely from a speech given in September 2012 by then-legal advisor Harold Koh under the Obama administration (U.S. Congressional Research Service, “Use of Force in Cyberspace”). However it is possible that the doctrinal underpinnings are traceable to administration positions dating at least as far back as 2009, as evidenced in remarks given by Mary Ann Davidson to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology (Hathaway and Obama, n.d.), and expanded on in later documents. One such archived document from the Obama administration titled “The Monroe Doctrine in Cyberspace” references the 1823 policy tenet laid out in a speech by US President James Monroe, and arguably shaped considerably by then-Secretary of State John Quincy Adams, articulating US stances against 19th century European colonization of the Western Hemisphere and policies of intervention in the case of such colonization, which the US would view as an act of aggression.

The Obama administration’s referencing of the Monroe doctrine is layered; the historical tenet’s introduction was precipitated in part by deteriorating 19th century US-Russian relations (nakajima, 2007) as the United States grappled with fears of Russian expansionism in what the US considered to be its colonial claims. Although Russian territories are often thought of as contiguous and exclusive of North America, Russian interests on the continent were at one time significant. It is impossible to make sense of modern US-Russian relations without a foundational understanding of the history of North American colonization.

On 8 July 1799, Russia’s first ever joint-stock company was founded in St. Petersburg, with the purpose of establishing a presence in the Alaskan fur trade market. The company, called Под высочайшим Его Императорского Величества покровительством Российская-Американская Компания (*Pod vysochayshim Yego Imperatorskogo Velichestva pokrovitelstvom Rossiyskaya-Amerikanskaya Kompaniya),* or *The Russian-American Company Under the High Patronage of His Imperial Majesty*, is often referred to simply as The

Russian-American Company. While Russian fur traders had already begun to colonize the Pacific Northwest, The Russian-American Company began expansion of North American trade settlements in earnest.

Russian colonization of Pacific North America was not kinder to Indigenous peoples than that of the British or Americans. Borrowing a page from contemporary US policies towards Indigenous populations in North America, Russian colonists forcibly conscripted Native and so-called "mixed blood" individuals from groups across the Pacific Northwest to labor in the fur trade, often by holding their spouses and children hostage and demanding furs or labor as ransom (Lightfoot, 2003). These Indigenous people were enslaved due to their extraordinary skill (*ibid*). In addition, infectious diseases brought by Russian colonists decimated local populations. The impact of diseases brought by the Russians is significant enough to be measurable in skeletal remains of Indigenous peoples from the era (Keenleysìde, 2003).

Amid trafficking, enslavement, and battles with Russian colonists as Alaskan Natives attempted to defend their interests, up to 80% of the Aleut population was killed. By 1800, only 2500 remained ("History: The Russian and American Periods", n.d.). By the time of the US purchase of Alaska from Russia in 1867, only about 2,000 survived ("The Aleuts" 1997, 367). Indigenous peoples would not receive full citizenship from the United States until 1924.

As the Russian fur trade–fueled by enslaved Indigenous peoples, but running out of natural resources–expanded as far as California, the United States became increasingly wary of Russian plans for further colonization. These fears were not entirely unfounded; a heavily-considered (although ultimately rejected) early 1820s Russian memo detailed potential plans to further colonize what was then Spanish-controlled California (Mazour, 1936). Amid the chaos of multiple world powers' rapid expansion into North America, US President James Monroe addressed the nation with remarks that would become a foundational foreign policy tenet driving US political thought, legislation, and even kinetic action on the ground–the use of military force–into the 21st century. In what would become known as the Monroe doctrine, the United States granted itself broad powers to defend what it considered to be its territorial interests.

In the context of this history, the Obama administration's 2009 invocation of a 19th-century foreign policy aimed in part at Tsarist Russia in discussions on cyberattacks and proportionality of force–particularly in the wake of the 2007 attacks against Estonia–is arguably an intentional allusion to not just historical, but also contemporary perceived Russian expansionism against US interests. In that same archived document expanding Davidson's remarks to the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology ("The Monroe Doctrine in Cyberspace", n.d.), the connection between contemporary attempts to establish foundational tenets in the emerging cybersecurity field and US historical territorial claims is made explicit:

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…The advantages of invoking a Monroe-like Doctrine in cyberspace would be to put the world on notice that the US has cyber "turf"...And the second is that we will defend our turf. We need to do both. Now.

These remarks elucidate a paradigm in which the US must defend its territorial interests, even in the cybersphere; contested "turf" is no longer the physical soil and waters of the Pacific Northwest or the larger Western Hemisphere, rather, it has shifted to the ties between IP addresses and the consequent real-world repercussions of their network effects.

In his 2012 speech, Koh, referencing both international law as well as Article 2(4) of the United Nations Charter, stated that cyberattacks which "*proximately result in death, injury, or significant destruction would likely be viewed as a use of force."*

This acknowledgement on the part of the US government of the destructive potential of cyberattacks in the real world contrasts with more traditional US and western European conceptualizations of cyber actions as siloed from "real world" effects. Critically, via recognizance of potentially injurious-to-crippling capabilities of actors in the cybersphere, the statement opens the door to proportionate use of force on the part of the US in the event of a cyberattack with kinetic effects: "*If an actor employs a cyber weapon to produce kinetic effects that might replicate fire power under other circumstances, then the use of that cyber weapon rises to the level of the use of force"* (U.S. Congressional Research Service, Use of Force in Cyberspace).

Within the United States Doctrine however, *any* cyberattacks during ongoing conflict are governed by the same principles of proportionality that apply to actions more classically understood as warfare–even those that may not result in kinetic effects. This indicates a subsequent principle: that the US has the right to respond to any and all cyberattacks conducted during armed conflict with proportionate *kinetic* actions:

…the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances…cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force (*ibid*).

In the same speech, Koh also cited Article 51 of the United Nations Charter–*"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."*--referencing what the US might consider a cyber action rising to a level such that it would trigger a nation's right to self

defense. These include "*computer network activities that amount to an armed attack or imminent threat thereof*" (Koh 2012).

Taken together, these remarks lay the groundwork for broad US authority to use force under a diverse, and somewhat nebulously defined, set of circumstances. They are arguably in direct line with the intellectual legacy of Davidson's 2009 remarks, and the Monroe Doctrine itself. It is further arguable that current US policy on the use of force in cyberspace–which remained largely unchanged from its 2012 status up until the early 2022 escalation of cyber hostilities in Ukraine–is itself a faithful attempt to adapt the Doctrine to modern cyber warfare. While the arena and tools might be new, the struggle between the US and Russia–as two colonial powers vying for over 200 years to define and dominate what they consider to be their territorial interests in a new frontier–remains.

References

"The Aleuts." 1997. In *Personal Justice Denied: Report of the Commission on Wartime Relocation and Internment of Civilians*, 317-359. N.p.: University of Washington Press.

Hathaway, Melissa, and President Barak Obama. n.d. "COMMITTEE: House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology SUBJECT: Federal." Obama White House Archives. Accessed February 25, 2022. https://obamawhitehouse.archives.gov/files/documents/cyber/Congress%20-%20031009%20HHS%20ETCST%20Cybersecurity%20Transcript.pdf.

"History: The Russian and American Periods." n.d. Aleutian Pribilof Islands Association. Accessed February 26, 2022. https://www.apiai.org/departments/cultural-heritage-department/culture-history/history/.

Keenleysìde, Anne. "Changing Patterns of Health and Disease among the Aleuts." *Arctic Anthropology* 40, no. 1 (2003): 48–69. http://www.jstor.org/stable/40316575.

Koh, Harold H. 2012. "International Law in Cyberspace." 2009—2017 State.gov. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

Lightfoot, Kent. (2003). Russian Colonization: The Implications of Mercantile Colonial Practices in the North Pacific. Historical Archaeology. 37. 14-28. 10.1007/BF03376620.

Mazour, Anatole G. 1936. "Dimitry Zavalishin: Dreamer of a Russian-American Empire." *Pacific Historical Review* 5, no. 1 (March): 26-37.

"The Monroe Doctrine in Cyberspace." n.d. Obama White House Archives. Accessed February 25, 2022. https://obamawhitehouse.archives.gov/files/documents/cyber/Davidson%20MaryAnn%20-%20The%20Monroe%20Doctrine%20in%20Cyberspace.pdf.

nakajima, hiroo. (2007). The Monroe Doctrine and Russia: American Views of Czar Alexander I and Their Influence upon Early Russian-American Relations. Diplomatic History. 31. 439-463. 10.1111/j.1467-7709.2007.00627.x.

U.S. Congressional Research Service. Use of Force in Cyberspace (IF11995; Dec 10, 2021), by Catherine A. Theohary. Website:https://crsreports.congress.gov/product/pdf/IF/IF11995; Accessed: February 15, 2022.

At the intersections of AI, Security, Policy, & People

https://cx7.dev/