Case Western Reserve Journal of International Law

Volume 47 | Issue 1

2015

Unpunished Insults -- The Looming Cyber Barbary Wars

Matteo G. Martemucci Col.

UNPUNISHED INSULTS—THE LOOMING CYBER BARBARY WARS

Col. Matteo G. Martemucci, USAF[1]

This article argues that while current cyber literature focuses on cyber crime and cyber war, policy makers do not treat the most damaging cyber activity—large-scale economic espionage—in a manner commensurate with its importance. The threat from nation-states like China is real, and it requires a coherent strategy of response. The article analyzes the historic role of the U.S. government and the military in the protection of commerce from piracy and privateering at the turn of the last century. This provides useful context for the necessary debate over the role of the government and military in the defense of the modern cyberspace-enabled economy. This article further argues that there is a role for the US Government, and possibly the Department of Defense, in safeguarding US commerce in cyberspace just as it does in the physical domain. Policy leaders need to thoughtfully debate and define this role.

CONTENTS

1. Col. Matteo "Mooch" Martemucci commands the 318th Cyberspace Operations Group at Joint Base San Antonio-Lackland, Texas. He leads 650 professionals in the conduct of Cyber Warfare and Information Operations training, testing, tactics development, and operations. He is a career intelligence officer and cyberspace operator whose twenty one-year career has included command of the Air Force's premier Network Warfare Squadron as well as postings or deployments to Korea, the Czech Republic, France, Saudi Arabia, Iraq, Qatar and Afghanistan. His numerous decorations include the Defense Meritorious Service Medal and the Bronze Star Medal. He holds a BA in International Politics from Penn State University, an MS in International Relations from Troy University, an MS in Joint Campaign Planning & Strategy from the National Defense University, a Graduate Certificate in Organizational Management from George Washington University and a National Security Affairs Fellowship at the Hoover Institution on War, Revolution and Peace at Stanford University. The views expressed in this paper are those of the author and do not reflect the official policy or position of the U.S. Government or the Department of Defense.

> Weakness provokes insult and injury, while a condition to punish it often prevents it . . . I think it is in our interest to punish the first insult: because an insult unpunished is the parent of many others.[2]
>
> If we wish our commerce to be free and uninsulted, we must let these nations see that we have an energy which at present they disbelieve.[3]
>
> —Thomas Jefferson

I. INTRODUCTION

The current debate over threats, vulnerabilities, and responsibilities in cyberspace is incomplete. While the current cyber literature and academic debate focuses on cybercrime and cyberwar, policy makers do not treat the most damaging cyber activity—large-scale economic espionage—in a manner commensurate with its importance. The greatest single threat to the American national existence we enjoy today is the systematic, long-term economic espionage by nation-states, like China, that contribute to the shifting of the balance of economic power away from the U.S. This threat is real, it is happening now, and it is growing fast. Economic espionage requires a coherent strategy of response.

The U.S. military has historically served to maintain the security of the global commons to allow for the continuation and expansion of trade to the nation's benefit. Along with the other instruments of national power, military capability serves as a powerful deterrent for illegal action by other states. In cyberspace, however, there is currently no equivalent motivation for states to act appropriately, resulting in significant negative impact on the U.S. economy. Thus, in addition to preventing cyber attacks on critical infrastructure, there is a role for the U.S. Government, and possibly for the Department of Defense (DoD), in safeguarding U.S. commerce on the high seas of cyberspace, just as it does in physical domains of the global commons. Unfortunately, policy leaders have yet to thoughtfully debate and define this role, but their participation is vital in addressing the serious threat of economic espionage.

In recent years, cyber-based threats of all kinds have grabbed the consciousness of the public, pundits, and political leaders. Cyber attacks on Estonia in 2007 and on Georgia in 2008 form the outline of

2. Letter from Thomas Jefferson to John Jay (Aug. 23, 1785), http://avalon.law.yale.edu/18th_century/let32.asp.

3. Letter from Thomas Jefferson to John Page (Aug. 20, 1785), http://founders.archives.gov/documents/Jefferson/01-08-02-0325.

many discussions about cyber war.[4] The Stuxnet virus that destroyed nearly one thousand uranium-enriching centrifuges in Iran in 2010 by an as-yet unconfirmed entity has further shaded the picture.[5] Recent large-scale theft of credit card and personal information from Target, JPMorgan, and others add color to the public consciousness.[6] Yet, despite the details, the threat picture remains unclear. Many are afraid, but no one is exactly sure what to fear. The author's research suggests that, in the realm of cyberspace, we are worrying about the wrong things. Current cyber literature and academic debate focus on cybercrime, politically motivated hacking, and cyber war, but they largely ignore the most important cyber threat today: large-scale economic espionage conducted by nation-states and their proxies.

In May 2014, in the most significant case of direct attribution against a nation-state to date, the U.S. Department of Justice (DoJ) issued an indictment against five Chinese hackers, explicitly linking them to a unit of the Chinese Peoples' Liberation Army.[7] "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking," U.S. Attorney General Eric Holder said. "The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response."[8] This indictment is a good first step, but it falls short of a credible response that may actually change China's behavior because the DOJ's indictment is not a credible deterrent. With no possibility of extradition, and no further cost imposed on the Chinese economy by the U.S. Government in response, the indictment alone prevents nothing, though it sits as an interesting piece of political theater.

4. *See, e.g.*, *Marching off to Cyberwar*, ECONOMIST, Dec. 4, 2008, http://www.economist.com/node/12673385.

5. Mark Clayton, *Stuxnet Attack on Iran Nuclear Program Came About a Year Ago, Report Says*, CHR. SCI. MONITOR (January 3, 2011), http://www.csmonitor.com/USA/2011/0103/Stuxnet-attack-on-Iran-nuclear-program-came-about-a-year-ago-report-says.

6. Ryan Tracy, *In a Cyber Breach, Who Pays, Banks or Retailers?*, WALL ST. J. (January 12, 2014, 7:25 PM), http://online.wsj.com/ news/articles/SB10001424052702303819704579316861842957106.

7. Press Release, U.S. Just. Dep't, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

8. *Id.*.

II. HISTORICAL PRECEDENT: THREATS TO COMMERCE IN 1801—A NEW NATION'S ANSWER

One can never draw perfect historical parallels, nor wisely stretch an analogy beyond its logical limits. However, the history of American military involvement in matters of economics and commerce, particularly in the global commons of the sea, bears review for its potential parallels to the cyberspace domain of today. In 1801, Thomas Jefferson deployed a small fleet of newly minted American warships to the Barbary Coast to stem the tide of piracy and extortion that was crippling the new nation's trade-based economy.[9] The fifteen-year Barbary campaign, which combined diplomacy and military action, ended the centuries-old practice of paying tribute—what would be considered bribes today—to marauding states for the safe passage of commercial ships by America and Europe's trading countries. In what historian Joseph Wheelan described as "Principled American outrage," the new nation demonstrated its refusal to accept the status quo and, in turn, set itself on a path of leadership in the defense of global commerce.[10] Today, American intellectual property is a similarly lucrative prize for those seeking economic advantage. The intellectual capital, comprised of industry secrets, proprietary research, development, and business innovation,that resides in and transits through cyberspace is like the treasure of heavily laden and undefended merchant ships in pirate-infested waters.

Cyberspace, as a man-made domain, is another ocean on which individuals, corporations, and nation-states create commerce and conduct global trade. In the physical domains of land, sea, air, and space, states have long-established responsibilities to protect their sovereign interests. The U.S. military has historically served to maintain the security of the Global Commons to allow for the continuation and expansion of trade to the nation's benefit.[11] Along with the other instruments of national power, military capability serves as a powerful deterrent for illegal action by other states. In cyberspace, however, there is no equivalent disincentive for nation-states not to cheat.

In the first century of the United States' existence, its military was limited primarily to the protection of its economic interests.[12] In

9. *See* JOSEPH WHEELAN, JEFFERSON'S WAR: AMERICA'S FIRST WAR ON TERROR 1801-1805 105–107 (2003).

10. *Id.* at xxi.

11. Barry R. Posen, *Command of the Commons: The Military Foundation of U.S. Hegemony*, 28 INT'L SEC. 5, 8-9 (2003).

12. *See generally*, Michael A. Palmer, *The Navy: The Continental Period, 1775-1890*, NAVAL HIST. & HERIT. COMMAND, http:// www. history. navy.mil/history/history2.htm (last visited Oct. 5, 2014) (explaining

fact, the new nation overcame its aversion to a powerful standing military only when the need arose to protect the commerce that supported a growing economy. Even then, it took years of economic losses to spur the government to military action.[13]

The *de facto* dissolution of the American Continental Navy occurred when Congress sold off the last of its warships in 1785. Ironically, this occurred less than two years after Algiers seized six American merchant ships, and one year after the New York merchant ship *Empress of China* arrived in Canton to open trade with China.[14] It is significant that the establishment of the U.S. Navy was largely in response to foreign affronts to the fledgling nation's commerce abroad. Protecting U.S. commerce from piracy and state-sponsored privateering along the Barbary Coast was a key factor in the commissioning of the U.S. Navy's first warships in 1794.[15] Over the ensuing two centuries, the predominant purpose of U.S. military engagements abroad, particularly those of the U.S. Navy and Marine Corps, were to protect American lives and property, usually by protecting commerce on the high seas.

While the Caribbean proved fertile ground for piracy and privateering, the rampant extortion of commerce by pirates in the Mediterranean, operated by the independent Barbary States of Morocco, Tripoli, Algiers, and Tunis, was what first spurred the new United States to action. This brazen exploitation of European powers infuriated President Thomas Jefferson. He was incensed not only at the brutality of the Barbary tactics, but also at the European states' unwillingness to respond.[16] At the time of Jefferson's election in 1801, America had also been complicit. It had paid an amount equivalent to one-fifth its entire annual income in tribute to the Pasha of Tripoli and the other states on the North African coast.[17] After witnessing

---

that "[t]he major post-War of 1812 mission of the U.S. Navy remained commerce protection.").

13. Robert F. Turner, *President Thomas Jefferson and the Barbary Pirates*, *in* 35 PIRACY AND MARITIME CRIME: HISTORICAL AND MODERN CASE STUDIES 157, 158–163 (Bruce A. Elleman, Andrew Forbes & David Rosenberg, eds., 2010).

14. James Bradford, *Defending U.S. Maritime Commerce in Peacetime from 1794 to Today*, *in* AMERICAN MILITARY HISTORY: A RESOURCE FOR TEACHERS AND STUDENTS 211, 211 (Paul Herber & Michael G. Noonan eds., 2013), http://www.fpri.org/docs/ American_Military_History _A_Resource.pdf.

15. *Id.*

16. *See* Turner, *supra* note 12, at 157, 159.

17. For a review of U.S. Treasury estimates of the cost of the Peace with Algiers as a portion of the federal budget, *see* JOSHUA E. LONDON, VICTORY IN TRIPOLI 43 (2005)

this awkward game of extortion and complicity for years, first as minister to France and then as Washington's Secretary of State, Jefferson had had enough. Both economic necessity and national honor caused Jefferson to eschew his aversion to a national military, and in 1801, he sent the majority of the U.S. Navy's combat power—comprised of four ships led by the USS *Constitution*—to the Mediterranean. By ordering the small fleet to Tripoli, Jefferson began what was to be a fifteen-year undeclared war against piracy, privateering, and the payment of tributes to the leaders of the Barbary States.[18]

In his century-old writings on "The Attack and Defence [sic] of Trade," the British naval historian Julian Corbett defined fertile and infertile areas for trade, arguing that "[t]he most fertile areas always attracted the strongest attack, and therefore required the strongest defence [sic]."[19] In our time, cyberspace-enabled commerce has created an entirely new map of fertile areas for trade to occur. Foreign cyber pirates and privateers, backed by their state governments, are taking over the modern cyber equivalents of those merchant ships, their ports, and their transit routes. They conduct computer network exploitation with the support of their governments, routinely looting from American *ships of commerce* in cyberspace, while our military's *cyber warships* are still under construction or, at best, protect only the military ports in which they remain moored.

III. The Necessary Debate: Can and Should the Military Defend Commercial Cyberspace?

Currently, the U.S. military is responsible for defending the *.mil* domain, which is its small portion of the global internet infrastructure.[20] The Department of Homeland Security (DHS) is responsible with defending the *.gov* domain, which is the U.S. Government enclave within the larger internet sphere.[21] Yet, no one is

18. For a more detailed look at the conflict between the U.S. Navy and the Barbary pirates during the Jefferson Administration, *see* GREGORY FREMONT-BARNES, THE WARS OF THE BARBARY PIRATES: TO THE SHORES OF TRIPOLI: THE BIRTH OF THE U.S. NAVY AND MARINES 39-64 (2006).

19. Julian Corbett, *Some Principles of Maritime Strategy*, *in* 4 ROOTS OF STRATEGY 149, 250 (David Jablonski ed., 1999).

20. William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF., Sept.–Oct. 2010, at 97, 103; Joseph S. Nye Jr., *Nuclear Lessons for Cyber Security?*, STRAT. STUD. Q., Winter 2011, at 18, 22.

21. U.S. DEF. DEP'T, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 8 (2011), http://www.defense.gov/ news/ d20110714cyber.pdf.

responsible for defending American interests, economic or otherwise, in the *.com*, *.edu*, *.net*, or any of the other public Internet Protocol domains. Both the government and the military, however, rely greatly on the larger public internet space outside the *.gov* and *.mil* domains. In its own reporting, the DoD admits to its dependence on cyberspace, which by definition includes the vast non-DoD-controlled portions of the Internet and commercial systems.[22]

Furthermore, the private sector has a rather schizophrenic outlook on the topic. The private sector may well expect the DoD to defend its digital interests in cyberspace, just as the private sector expects the DoD to defend American physical and personal interests on the land, in the air, and on the sea. However, individuals and corporations are fearful of any over-regulation and invasion of privacy that they associate with an equivalent defensive effort in cyberspace.[23] The U.S. military, on the other hand, is beginning to realize that it may be called upon one day to defend a virtual territory for which it currently has no defensive capability.

Setting aside capability for a moment, this current condition of responsibility (or lack thereof) is akin to building a military whose sole purpose is to defend the frontier fort in which it is garrisoned, or the ports in which its ships are berthed, but not beyond. In this analogy, the U.S. Army has never left the safety of its protected perimeters despite the fact that the enemy is ravaging the pioneer towns just outside its walls, nor has the U.S. Navy left its protected ports despite the extortion of commercial shipping by foreign pirates in American territorial waters and beyond. There will come a day when the U.S. Government, including the DoD, may be asked to defend infrastructure (e.g. dams, power grids, banking networks), industries, or even corporations themselves. In order to provide for that defense, the military would need to operate in public IP space, on networks upon which they currently do not. Neither the general public nor private industry is prepared to make the perceived concessions to civil liberties necessary to enable that type of defense. This is a difference of expectations worth studying.

There are myriad questions we must debate when considering the role of the government and the private sector in securing cyberspace to enable the American economic engine. There are legal issues of

22. *Id.* at 8 ("Along with the rest of the U.S. Government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe.").

23. Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 316-318 (2008) (describing the concerns with military regulation and oversight in cyberspace).

privacy and liability, practical issues of capability and capacity, and philosophical issues of roles and responsibilities. Protection from cyber economic espionage merits serious consideration beyond the simplistic division of the internet into separate "spaces" for the military, government, industry, and academia to develop and defend (or not defend) in their own ways. Sadly, these difficult issues have all received less attention than those of cybercrime and a potential "Armageddon-like cyber shutdown." As a result, the National Academy of Sciences reports that there are currently "no legal mechanisms or institutional structures available to provide immediate relief" in the case of a computer network exploitation against an entity in the private sector.[24]

IV. RECOMMENDATIONS

In fairness, no element of the U.S. Government, including the military, has adequate organization or resources to meet the challenge of defending American economic interests in cyberspace. The prospect of severe cuts to the defense budget, and deep concern by the public over perceptions of intelligence overreach by the National Security Agency (NSA) in the wake of the Edward Snowden leaks, will not make the challenge easier.[25] That does not, however, diminish the need for informed debate on the responsibilities of both the military and the intelligence community in this new domain. At some point, the cavalry must ride and the frigates must take to the high seas. The questions are when and how, and the time to debate them is now, not years from now when the advantage will lie even more squarely with cyber pirates and privateers backed by even more emboldened governments.

First, U.S. Cyberspace Command (USCYBERCOM) must define specific roles for its National Cyber Protection Teams, which it is currently building. Second, USCYBERCOM must create trust relationships with key intellectual property companies, just as they currently have with cleared defense contracting companies. Third, DoD must increase its cooperation and information sharing with the DHS on all matters of cyber defense. Much of the private sector

24. NAT'L RES. COUNCIL NAT'L ACADS., TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 203 (William A. Owens, Kenneth W. Lam & Herbert S. Lin eds., 2009), http://www.nap.edu/catalog.php?record_id=12651.

25. *See* Runa A. Sandvik, *Illuminating The Billion Dollar U.S. Intelligence Budget: Project SpyLighter Documents NSA Surveillance Technology*, FORBES (Nov. 26, 2013, 9:56 AM), http://www.forbes.com/sites/runasandvik/2013/11/26/illuminating-the-united-states-billion-dollar-intelligence-budget-project-spylighter-documents-surveillance-technology-used-by-the-nsa/.

naturally fears working with the NSA or the military, but the private sector may be more willing to work with DHS. Leveraging that relationship as a bridge between the military and the private sector may lead to innovative solutions in cooperative cyber defense from economic espionage. Fourth, both DoD and DHS need to explore the notion of deterrence in cyberspace, and they must make recommendations for coordinated government policy approaches. This is an area ripe for exploration, and it is a matter of policy more than technology. The technical challenges of attribution are difficult but not impossible. The possibilities of active defenses, retaliation, and penalties for continued cyberspace-enabled economic espionage must inform the strategic idea of a national will to create effective deterrence against such attacks. Finally, to enable the above recommendations, there must be an informed academic, and very public, debate about the role of the U.S. military in the defense of public cyberspace. Only then can we resolve the differences in expectations that exist today.

V. CONCLUSION

We must elevate the level of analysis and debate over the greatest long-term threat to American national security, which is the significant and ever-increasing state-sponsored economic espionage enabled by our global connectedness in cyberspace. This debate must include a discussion of responsibilities of the public and private sectors in securing the pillars of the American economy. From the earliest days of its inception, the U.S. military has played an important role in the defense of global trade and, as a result, the growth of the American economy. As a man-made domain, cyberspace has taken on many of the characteristics of the domains of the sea and land as they relate to trade and commerce. It is necessary to define the role of the government in response to state-sponsored, cyber-enabled economic espionage, as well as the role of the modern military in the protection of American interests in the cyberspace domain.

Writing in the early 1900s about the opportunistic Barbary leaders who jumped on the new, ripe target of American commerce in the late 1790s and early 1800s, Lord Stanley Poole noted that "[a]s early as 1785 the Dey of Algiers found in American commerce a fresh field for his ploughing [sic]; and of all traders, none proved so welcome as that which boasted of its shipping, yet carried not an ounce of shot to defend it."[26] Today, America's intellectual capital floats exposed in the undefended sea of cyberspace, and none of its ships of industry

26. STANLEY LANE-POOLE, JAMES DOUGLASS, & JERROLD KELLY, THE STORY OF THE BARBARY CORSAIRS 274 (1890) *available at* Project Gutenberg.

carries an ounce of shot to defend it from what are increasingly identifiable foreign, state-sponsored threats. The defense of American intellectual property in cyberspace carries enormous legal, philosophical, and practical implications regarding the role of the government and military in that effort. We must debate these issues and arrive at a coherent strategy, however, before the wholesale theft of American intellectual property in cyberspace begins to look like the centuries-long insult of extortion payments paid to the Barbary states.