BUCCANEER.COM

Privateering as a Solution to Cyberspace Threats

Michael Tanji

E-mail: michael.tanji@gmail.com

Published 2006
Journal of Cyber Conflict Studies[1]

Abstract

The Internet and related technology are being used to facilitate acts that could adversely impact national security. This use has been increasing at least as rapidly as the technology itself advances. The various government entities that are responsible for enforcing related law have been left behind in the digital arms race. Due to constraints of time, complexity, and resources, most crimes perpetrated in cyberspace go unpunished. A similar state of affairs existed long before the Internet was conceived. In that age a means was developed by which the authorities could exert power – through proxies - against malicious actors. What lessons can practitioners and policy-makers of today learn from the era of the buccaneers? Is privateering a viable way to reduce online lawlessness without turning the Internet into a digital police state?

INTRODUCTION

Cyber threats are growing at a pace that exceeds the government's ability to address them. As a major component of national economies, and the medium over which government and military communications transit, the Internet is a national security resource and securing it a national security issue. Institutions like the FBI can't provide basic information-age services to their agents[2] yet those who are seeking respite from online threats continue to seek a governmental solution.

History tells us of another age, when national and economic power was based on sea not CPU power. Far from the eyes of national authorities, pirates hijacked the precious cargoes sought by colonial powers. Nations that lacked a powerful naval force co-opted the resources and motivations of the larger and more powerful private sector. To counter the threat of piracy the counter-pirate – or privateer – was created. Armed and capable, often staffed with veterans of military service, privateers assumed responsibility for the martial and enforcement tasks that nation-states were unable to accomplish on their own.

Privateering in the INFOSEC field could be an effective way to reduce the most serious cyber threats. Private institutions conducting national security work have both the resources and the motivation to make such a scheme work: reducing threats and corresponding losses is good business. However, such an approach is not without complications. There are important political and social issues to consider, and the legal issues could very well prove to be insurmountable. Not every enterprise that suffers at the hands of digital miscreants is going to be worth a privateering effort, and the nations most adversely impacted by malicious online activities are also those most likely to suffer consequences if the approach were to get out of hand.

THE STATE OF INTERNET SECURITY

From DOD-funded experiment to engine of modern commerce and government, the Internet is often envisioned as a wonderland where free information liberates minds and solves world hunger. If anything is liberated in cyberspace it is as likely to be innocent people from their money (and amateur entertainers from their clothes) as it is minds. Concepts like Moore's Law[3] plot the speed at which related technology will advance, while ingenious concepts that address a real or imagined need end up exposing us to a new set of dangers. In this environment a great disparity exists between the ideal and the reality of cyberspace.

Consider that every year the Computer Security Institute and the Federal Bureau of Investigation conducts a cyber-crime survey. Many INFOSEC practitioners consider the survey findings questionable, though not necessarily in a

negative way. For starters, there is a significant difference between the number of surveys sent out and the number of surveys that are returned. This means that the sample being used to draw conclusions is only marginally representative of reality. It is also privately acknowledged that the numbers reported in security surveys – particularly by public firms – are intentionally tempered.

There are more focused surveys that seek to document the financial losses brought about by cyber crime. The methodology behind some of these surveys is not always clear. Even when considering a problem of global significance some low-end some estimates seem too fantastic for reality.

Since we have no widely accepted way of assessing the impact of cyber threats, we are forced to draw the broadest conclusions in a round-about way; if cyberspace were not a generally lawless environment then the INFOSEC market would not be measured in tens of billions of dollars[4] and the demand for high caliber INFOSEC practitioners would not be as high as it is.[5]

Were the government able to effectively deal with cyber threats we should see conviction figures that roughly correspond to crime impact figures, yet the number of such prosecutions is astonishingly low. Like similar activity in the physical domain: only the dumb or greedy ones get caught.[6] There are a number of reasons why convictions are so low, not the least of which is the lack of adequately trained government agents. Forensics labs tend to be in major metro areas or regional centers where the few experts in the area are pooled together for the sake of efficiency. Despite these capabilities the demand for such services is overwhelming, which forces most labs to set parameters (usually dollar-based) for case acceptance.

Issues associated with time and jurisdiction also comes into play. Without the right to conduct digital "hot pursuit" or even non-evasive police techniques, any trail left by criminals could be long gone by the time investigators arrive. Even if a trail is traced as far as can be within the boundaries of one country, a connection to a foreign computer could end any investigative action. Foreign nations willing to cooperate are also likely hampered by resource constraints, and they themselves may be just one hop in a long chain of connections. There are also nations that do not have corresponding cyber laws on the books, or ratified treaties that would enable cooperation.

There are only a few courses of action available when it comes to addressing cyber threats. The first is the maintenance of the status quo: victim hood. Note that organizations that deal with cyber threats all have "response" in their name and you will realize that INFOSEC today is almost entirely reactive.

The second course of action has the government building the capability to bring law and order to cyberspace. This is unlikely if for no other reason than the stateless nature of the 'Net precludes exercising dominion by any single nation. Consider that the Department of Justice's cyber crime budget for 2005 was projected to be roughly $300 million dollars and a similar program within Homeland Security's was much less.[7] Contrast cyber defense spending to the tens of billions of dollars malicious actors are estimated to be making and you will understand the priority cyber threat has on Capitol Hill.[8]

The final option – outsourcing – has private-sector enterprises performing the tasks necessary to defend national interests online: INFOSEC privateering.

YO, HO, HO AND A CACHE OF RAM

There was a time when the engine of commerce in the world was based on sea not CPU power. The bigger your naval force the greater a global power you tended to be. It was sea power that allowed expanding empires to seek out and plunder far-away lands.[9] In addition to being finite, the precious resources craved by these nations were hard to get out of the ground. Eventually it became clear that a more economical approach would be to claim these resources after another party did all the investing and heavy lifting. To combat piracy, nation-states leveraged private-sector resources to protect commerce and defend national interests at the same time. Thus was born the privateer.

Given authorization by a government, a privateer was a not so covert operator who served as the eyes, ears, and fist of a sovereign when war and conflicts short of war were in play. For assuming risks on behalf of a sovereign, the privateer was rewarded with a portion of the bounty taken from a defeated party, while the balance was delivered to the government as settlement for whatever grievance was being avenged.

The primary difference between a pirate and a privateer was sponsorship. A privateer had government sanction – a Letter or Marque or Letter of Reprisal – that was in effect a license to kill and steal.[10] Pirates were outlaws and they received treatment as such if captured; privateers were proxy soldiers of a foreign government and if captured considered prisoners of war. This is not to say that all privateers were models of sea-faring propriety, since many were former (and once again future) pirates.

As with nearly every official solution to a given problem there was abuse. Over time, Letters evolved into the Elizabethan equivalent of a "get rich quick" scheme for colonial governors, businessmen, and privateers. Crackdowns ensued and as the age of the Galleon waned so did the need for a privatized seaborne security force. Letters of Marque officially ceased to be valid instruments of national power with the signing of the Declaration of Paris in 1856.[11]

THE MORE THINGS CHANGE…

You have a freely navigable environment in which both nations and private concerns can operate. Throughout this environment there are finite resources being fought over by rivals whose capabilities vary widely. Despite the existence of

a patchwork of laws, customs and practices, as a whole it is an anarchic environment that cannot be effectively and uniformly governed. Am I describing the ocean-centric world of the 17th century or the Internet-centric world of the 21st? Aside from the nature of the technology involved, is there a meaningful difference? Given the parallels is it unreasonable to assume that the solution developed to solve these problems centuries ago would not also work to resolve its modern counterpart?

There is no exact equivalent of the privateer in modern life. No government sanctions private actors to wage war on another state (at least not publicly). There are a number of examples that come close though the parallels are inexact.

The modern-day bounty hunter is one such example. A private citizen operating under the auspices of a bond agent, the bounty hunter has more liberty to act in certain ways than law enforcement officers. Their mission however, is to deliver alleged criminals to court, not avenge crimes or fight wars.

The Private Military Corporation (PMC) is another close example, but such firms do not engage in combat on behalf of one government against another.[12] PMCs make a point of distancing themselves from the term "mercenary" in part because the employment of mercenary forces is illegal under international law.[13] Their limited focus precludes the labeling of PMCs as modern-day privateers in the strictest sense.

Another close parallel includes organizations like the Business Software Alliance (BSA). The BSA is a private entity funded by software firms. It gathers information about enterprises that use and traffic in pirated software. While entities like the BSA may assist in the enforcement of the law, their primary goal is to help private enterprise, not national security in any direct sense.

From a sheer numbers perspective, tapping private capabilities makes perfect sense. The number of INFOSEC practitioners in just one large commercial firm likely equals if it doesn't exceed the federal security workforce in any given government agency. The situation was not much different in US colonial times as privateers outnumbered colonial navy ships by 26-to-1.[14] It isn't that our security and law enforcement agencies are neglecting cyber threats because they don't consider them important, but in an age of terrorism and scarce resources, some decisions make themselves.

A FRAMEWORK FOR INFOSEC SWASHBUCKLING

In a notional world where cyber threats were dealt with by INFOSEC privateers, the issuance of a Letter would have to be predicated on some minimum, specific, and verifiable criteria. For starters there has to be a reasonable belief that the perpetrators of a malicious act have placed the nation at risk.[15] This could include the theft of data from a federal interest computer system, or interfering with the networks of the critical infrastructure. Details may vary but the only reasonable conclusion that can be drawn by the action in question is that someone is seeking to undermine our national security.[16]

Additional principles to be applied should include:

- Principle of Self-Help: Reasonable and timely defensive steps have to have been taken prior to the event (e.g. properly configured firewalls, up to date on patches, etc.).
- Principle of Proportionality: Actions must be equal to or less than the actions taken by the perpetrator.
- Principle of Sovereign Control: Nations participating in a privateering regime have to have adequate controls on when and how privateering can be used.
- Principle of Qualification: Privateers must demonstrate a minimum level of competence and a means by which competence can be verified (read: certification).

COMPLICATING FACTORS

Most complicating factors associated with privateering are legal in nature. I am neither a lawyer nor do I attest that what follows is a comprehensive treatment of pertinent law. I hit a few high points to illustrate just how complicated this can be from even a 50,000-foot view.

Past attempts to impose an international legal regime for cyber threats made a number of flawed assumptions.[17] The first is that national laws would be readily altered to bring a nation into compliance with an international regime. Unfortunately, what constitutes a crime in one nation may be viewed quite differently in another. There is no disputing the fact that the "I Love You" worm had a serious impact on information systems in the US, yet the Filipino author of the worm has yet to answer for his actions. In the US we revile spam and pop-ups, but in some corners of the world such techniques may be considered protected speech or simple commerce.

The second flaw is that ratification somehow fixes the law enforcement capability problem. Recall our earlier discussion on the dearth of government-employed cyber crime professionals in the technically advanced US and then extrapolate downward. Better yet try to envision the effectiveness of a joint US, UK, German, Estonian, Peruvian and Bhutanese investigation.[18]

Third, some nations may be unwilling to assist in all investigations. Indeed one nation's clandestine digital espionage program may very well look like the work of hackers: if it is not actually carried out by hackers. Any adversary or erstwhile ally can claim with great indignity that evidence of a break-in that points to their nation is the work of digital malcontents and not a government sponsored activity; *"Mon Dieu! Have you not heard of the fallacy of the 'last hop'?"*

Let us also not forget that progression along the international legal front can be glacial, which would be fine if the impact of threats was not growing by orders of magnitude. At this point we could argue that international cyber security is something of an illusion, in which case we have the opportunity to invoke a right that we never abrogated:

> *"Congress shall have power to . . . Declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water."*[19]

CONCLUSIONS

INFOSEC privateering is certainly a provocative idea. It is easy to get carried away with romantic imagery – and milk nautical metaphors to excess - and belay the fact that this is a course of action that could have serious repercussions if not carefully monitored. Privateering is arguably the most economical, technically feasible and historically relevant approach to the problem. Despite potentially insurmountable legal hurdles, privateering is precedence, and where is precedence valued more than in the law?

Taking no dramatic action to bring order to cyberspace is always an option. The current state of affairs has been going on for so long that unless people start dying because of cyber attacks some may consider it the safest course of action to pursue.

The only real constructive alternative to privateering - a large and powerful government enforcement capability - is unlikely. The excessive cost and lack of political will two key mitigating factors. As this paper was being drafted much was being made of online government surveillance programs. While a minority of people polled took issue with these programs, the attitude of the electorate might change considerably if a massive digital police force patrolling cyberspace were being proposed. People don't mind the innocuous glance; they take great umbrage with the prolonged and unwarranted stare.

Privateering really only makes sense for institutions supporting critical infrastructure and national defense; they have the most to lose, the most qualified resources, and can most easily meet proposed compliance requirements. Malicious actors will think twice about attacking all but the most inconsequential targets because the price for attacking anyone substantial is too high. Patently unfair? Perhaps, but since we will never be fully rid of cyber threats, reducing them to mere irritation is a far cry better than the status quo.

Privateering would require a strong, independent and transparent mechanism for validating activity the potential for abuse would be strong. There is no shortage of events that could potentially qualify for privateer action, so much so that there will probably be a temptation over time to make the language in Letters more ambiguous or to issue a "blanket" Letter that takes responsibility for deciding when to act out of the hands of the government.

Ocean-going piracy today is a trifling problem that has achieved some notoriety of late following events off the coasts of Somalia and in Southeast Asia. No one calls for a force of privateers to combat these belligerents because they are no match for even commercial cruse ships.[20] The point to take away is that piracy in the physical world is essentially a nuisance; privateering in cyberspace is one way to exercise national power and to reduce cyber threats so as to achieve the same goal.

ABOUT THE AUTHOR

Michael Tanji has spent nearly 30 years successfully fulfilling front-line, managerial, and CxO roles in both the military, government, and commercial concerns. Trained in both signals and human intelligence disciplines, he has worked on a wide range of intelligence and secuirty issues for the Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, the U.S. Army's Intelligence and Security Command, National Intelligence Council, National Security Council and NATO. Co-founder of cybersecurity companies Kyrus Tech and Carbon Black, Michael is also the editor of *Threats in the Age of Obama*,[21] author of the oral history *Working in Cybersecurity*,[22] contributor to *The Handbook of Research on Counterfeiting and Illicit Trade*[23] and featured in *Tribe of Hackers: Blue Team.*[24]

---

[1] This paper was originally published in the inaugural issue of the peer-reviewed Journal of the Cyber Conflict Studies Association. No longer in publication, it has been reformatted for the sake of posterity and author information updated.

[2] New York Daily News, "Internet Untouchable for FBI Agents in City," *Nydailynews.com* home page on-line; available at http://www.nydailynews.com/front/story/401323p-339883c.html; accessed 5 May 2006.

[3] The 1965 projection of Intel Corporation co-founder Dr. Gordon Moore that microprocessors will double in complexity - commonly interpreted as doubling in power - every two years.

[4] Information Security Magazine, "Infosec News," infosecuritymag.techtarget.com; available at https://infosecuritymag.techtarget.com/2003/feb/digest10.shtml#brief4; accessed 6 May 2006.

[5] JobStats, "Trend in Demand for the Skill," jobstats.co.uk; available at http://www.jobstats.co.uk/jobstats.d/Details.d/Trends.d/SKILL/CISSP.d/index.html; accessed 6 May 2006.

[6] Had they not fallen for the FBI's false pretence of a job offer, Russian hackers behind the CARDKEEPER case - Alexy Ivanov and Vasiliy Gorshkov - would likely have never been convicted.

[7] CNET, "News" news.com; available from http://news.com.com/Bush+budget+sweeps+in+tech,+cybercrime/2100-1028_3-5152145.html; accessed 7 May 2006.

[8] Business Week, "Viewpoint" businessweek.com; available at http://www.businessweek.com/technology/content/feb2006/tc20060202_832554.htm; accessed 7 May 2006.

[9] The author thanks M.J. Tempest, CAPT, USNR (Ret) and 1LT Brian C. McClain, US Army, for freely sharing their knowledge and insights on the age of piracy.

[10] Issued by a sovereign and later colonial governors a Letter of Marque gave a privateer license to attack the ships of nations hostile to the issuing authority until the Letter was revoked or hostilities were over; Merchantmen who lost a ship to a foreign navy or privateer could be issued Letters of Reprisal; essentially a license to reclaim stolen property, though the prize (ship) taken might not have been the actual ship lost.

[11] A treaty not ratified by the US.

[12] The UK-based PMC Sandline was hired by the government of Sierra Leone to put down an insurgency, which is indeed combat, but not war against another state.

[13] International Committee of the Red Cross, "International Humanitarian Law," icrc.org; available from http://www.icrc.org/ihl.nsf/FULL/530?OpenDocument; accessed 8 May 2005.

[14] American Merchant Marine at War "Privateers and Mariners at War," usmm.org; available from http://www.usmm.org/revolution.html; accessed 8 May 2005.

[15] In order to portray a world with a privatized INFOSEC regime it is necessary to suspend a certain amount of disbelief. A variety of broad assumptions about changes to existing laws and policies have to be made in this notional example, though in interest of brevity they are not all explicitly stated.

[16] Attribution of such action is something of a holy grail in the INFOSEC field, and a topic that is beyond the scope of this work. Suffice it to say that the utility of certain types of information are limited to those who can make best use of it.

[17] Center for Democracy and Technology, "International Issues" cdt.org; available from http://www.cdt.org/international/cybercrime/; accessed 7 May 2005.

[18] With all due respect to the Bhutanese cyber crime squad.

[19] Cornell Law School, "US Constitution, Article I, Section 8" law.cornell.edu; available from http://www.law.cornell.edu/constitution/constitution.articlei.html; accessed 6 May 2005.

[20] USA Today, "Tech Innovations" USAToday.com; available from http://www.usatoday.com/tech/news/techinnovations/2005-11-07-cruise-blast_x.htm; accessed 9 May 2005.

[21] https://www.amazon.com/dp/B003KRP320

[22] https://www.amazon.com/dp/B07JR5W2V9

[23] https://www.amazon.com/dp/1785366440/

[24] https://www.amazon.com/dp/1119643414