Asian Security

ISSN: 1479-9855 (Print) 1555-2764 (Online) Journal homepage: http://www.tandfonline.com/loi/fasi20

Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?

Forrest B. Hare

To cite this article: Forrest B. Hare (2017): Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?, Asian Security, DOI: 10.1080/14799855.2017.1414803

To link to this article: https://doi.org/10.1080/14799855.2017.1414803

Published online: 26 Dec 2017.

ASIAN SECURITY
https://doi.org/10.1080/14799855.2017.1414803

Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?

Forrest B. Hare

ABSTRACT
Leaders in some Asian countries have argued that it is necessary to follow the lead of the Russians and Chinese, who have been promoting patriotic hackers to achieve national security goals. The arguments in support are not without historical precedence. In naval warfare, many nations advocated using private citizen fighters called privateers to support their military operations. In this analysis, I look at the role privateering has played historically in naval warfare to see what lessons can be applied to the policy option of promoting independent but government-sponsored hacking to achieve national security objectives. I also present legal considerations that have evolved since the practice of privateering was abolished. The analysis argues that countries unable to fully control and coordinate civilian hacking activity with government operations should not promote the activity.

Introduction

Several countries have begun to consider an approach to cyberspace operations that is modeled on the actions of other states that have outsourced the cyber operation components of their military and intelligence communities. Russia and China, for example, have promoted "patriotic hacking" to support their efforts to prepare for a potential conflict or to use during one. In both countries, the civilian hacker community has been leveraged to gather intelligence and create cyber effects that support conventional military operations and other coercive actions.[1] Thought leaders and officials in other Asian countries that have limited ability to generate a professional cyber force have argued that it is necessary "to fight fire with fire" and follow the lead of the Russians and Chinese. In effect, they propose that it would be more efficient to rely similarly on patriotic hacking groups to achieve their desired objectives in cyberspace.[2] Although cyberspace and its many complexities have become a national security issue only in recent decades, the arguments made here are not without historical precedence.

In naval warfare from the 1500s to the 1800s, private citizen fighters who were called privateers – in essence, legalized pirates – supported the war efforts of many countries. These countries justified their support for privateers because the privateers helped them overcome the advantage held by the naval powers of the time and enabled them to exploit all combat power at their disposal. Eventually, however, the countries that promoted privateering concluded that the practice should be banned.

In this analysis, I look at the role privateering has played historically in naval warfare to see what lessons can be applied to the policy option of promoting independent but government-sponsored patriotic hacking to achieve national security objectives. Promoting this kind of patriotic hacking, a form of modern-day privateering, may have long-term negative effects on national and international security that outweigh the potential benefits. Therefore, this analysis argues that countries unable to fully control and coordinate civilian hacking activity with government operations should not promote patriot hacking as a way to prepare for or wage war.

CONTACT Forrest B. Hare fhare@masonlive.gmu.edu 4631 27th St North, Arlington VA 22207 USA

The analysis starts with a short explanation of patriotic hacking and review of instances where it appears patriotic hackers have been tacitly encouraged or even prompted to operate in cyberspace to achieve national security objectives. I then turn to examples of thought leaders recommending that other states follow suit. With this background in mind, I address the similarities and differences between promoting privateering and patriotic hacking, and then describe the experiences that led to the decision to abolish privateering across the world at the end of the 1800s. I also present an argument based on legal considerations to further discourage governments from promoting privateering activities in cyberspace without fully integrating the actor into professional cyber organizations. The analysis ends with my conclusions and policy recommendations.

"Citizens in the Fight"

In this section, I explore the activities that common citizens conduct in cyberspace under the guise of patriotic hacking and review how the Chinese and Russians have leveraged patriotic hacking effectively. I then present cases where other Asian nations are calling for the same approach in their countries.

Dorothy Denning, a prominent cyber security researcher with the United States Naval Postgraduate School, has defined patriotic hacking as "networks of citizens and expatriates engaging in cyber attacks to defend their mother country or country of ethnic origin."[3] Considering these citizens have often acted even when their mother country was not directly threatened, the definition can be expanded to include cyber attacks launched by self-identified patriots in support of nationalist agendas of their country. The targets of these attacks are most often visible symbols of target country governments and businesses such as official websites. The classic example of patriotic hacking is the denial of service attacks on Estonian government and banking systems that were traced to many thousands of ordinary Russian citizens who were offended by the decision of Estonia to move a statue.[4] These attacks made the online government services in Estonia inaccessible for several days. Though there was no observable threat to Russian sovereignty from the move of the statue, the act appeared to offend Russian pride, and the patriots clearly felt the need to retaliate.

In China (the PRC), there is strong evidence that the government promotes state-sponsored hacking against both governments and private corporations around the world.[5] While the PRC agenda may be centrally organized and controlled, the actions are most often conducted by less tightly controlled amateurs, students, and private companies.[6] For example, researchers traced the Aurora attacks of 2010, which went after scores of businesses and the US think tank RAND Corporation, back to at least two Chinese universities identified as training grounds for patriotic hackers.[7] In 2013, *Time* magazine profiled Wan Tao of the China Eagle Union hacking group. According to Hannah Beech of *Time*, Wan Tao explained that the Chinese government closely monitored the activities of his group. While the government never punished him for his actions overseas, he was ordered on at least two occasions to censor all domestic content on the Chinese Eagle Union's website, which suggests that the Chinese government selectively controls the group's actions.[8]

Wan also identified individuals who were coerced to hack for the government.[9] These examples pertain mainly to cyber espionage that is conducted during peacetime to promote economic advantages or achieve other state goals. However, because China has not recently engaged in a conventional conflict with its regional adversaries, it may be difficult to predict how the government would interact with patriot hackers during such a conflict or what level of control they would have over the hackers' activities. Probably the best insight on this matter can be gained from Chinese hackers' response to the midair collision between a Chinese fighter jet and a US Navy EP-3 aircraft in early 2001. After this incident, Chinese patriotic hacker groups declared a "hacking war" and attacked hundreds of US government and military websites. They appeared to have done so with the encouragement of the Chinese government.[10] While it is difficult to confirm that the actions of

Chinese patriotic hackers are closely coordinated or controlled by the Chinese government, there are clear indications that the government at least encourages their actions.

Unlike the Chinese actions, one can draw a clear link between the Russian government and patriotic hackers during the conflicts Russia has been involved in recently. Cyber operations that were coordinated with Russia's invasion of Georgia provide the clearest picture of how patriotic hackers can be integrated with conventional kinetic operations. This invasion was the first conflict in which we could assess the military operations that occurred in all domains of the operation, including cyberspace.[11] A detailed analysis of the cyber component of this conflict was documented in the 2009 Project Grey Goose cyber operations report. In the report, Jeffrey Carr, the lead investigator, and his team drew a clear link between the stopgeorgia.ru forum and Russian intelligence organizations:

> In the case of possible Russian government involvement with the cyber attacks on Georgian government websites in July and August, 2008, the available evidence supports a strong likelihood of GRU/FSB planning and direction at a high level while relying on Nashi intermediaries and the phenomenon of crowdsourcing to obfuscate their involvement and implement their strategy.[12]

More recently, there have been indications that the Russian government is supporting the hacker groups that targeted the Ukrainian power grid in 2015 in an attempt to undermine Ukraine's ability to secure its territory against Russian insurgents. Attacks by the Sandworm Team, which analysts have found to have links to the Russian government, caused 800,000 Ukrainians to suffer a widespread winter power outage.[13]

While the evidence of linkages is strong, ultimately, the Chinese and Russian governments need not publicly acknowledge their relationships with their respective patriotic hacker groups. According to public statements, it appears that some influential individuals in South and East Asia are convinced that the Chinese and Russian governments have successfully leveraged patriotic hacking as a national policy. More importantly, the same individuals have argued that, instead of building a professional cyber force, their own countries should follow suit.[14] In India, Kapil Sibal, the former communications and information technology minister, first called for an army of ethical hackers to help the nation in 2011.[15] Indian cyber lawyer Pavan Duggal explained that he welcomes the effort to establish patriotic hacking groups in India, but that the IT Act would have to be amended to allow "patriotic stealth operations."[16] In Japan, a leading cyber security researcher has raised the idea of his country establishing a legion of "patriotic geeks" to counter foreign cyber threats. Professor Motohiro Tsuchiya argues that there are too few experts in the military and government because they offer lower salaries than the private sector. He calls on strident patriots to fill the gap.[17] If individuals in both India and Japan, large nations with tech-savvy populations, argue for such a policy, it would be plausible for smaller Asian nations with even more limited government resources to consider turning to patriot hackers to bolster the number of cyber operators in their nations. There are three possible reasons why encouraging patriot hackers might be more attractive to these countries than growing their own organic cyber force.

First, training a highly skilled cyber operator can take several years and be expensive. Some previous examples of patriotic hacking were committed by unskilled hackers (the online equivalent of throwing a rock at a glass window), but conducting detailed espionage and offensive operations that support national objectives against advanced targets is much more complicated. The operators must be skilled in several operating system, network protocols, and end use programs. They need to be able to infiltrate and navigate without being immediately detected. By the same token, it takes advanced training and experience to defend effectively against such attacks. Nations already reliant on cyberspace that have not implemented a policy to train for and grow such expertise are already at risk in the domain.

Second, unlike the skills developed by other military warriors who look forward to finding only a small job market outside of the government, the cyber warrior's skills are highly valued by many private-sector companies. These companies are concerned about cyber security and exploitation, and they are prepared to pay well for employees with strong cyber security skills. As such, most governments will have difficulty holding onto their cyber professionals once the professionals have fulfilled any commitment made to pay back their taxpayer-funded training and development.

Lastly, the actions of private hackers allow a government a modicum of plausible deniability.[18] States can covertly endorse patriotic hackers' actions, and if the hackers are caught or the operation otherwise backfires, the government can then claim they are not connected to the attackers and have little power to stop them.[19] In the previous examples from Russia and China, both governments denied having any links to patriotic hacking, to their advantage. This argument may therefore appeal to governments that want to employ patriotic hackers in situations where they want to avoid confrontation with a great power. Plausible deniability might also provide protection against a backlash from the international community if an action were to be uncovered and determined to be illegal. For these reasons, the call to promote patriotic hacking is understandable. However, there are several arguments against the strategy, which can be highlighted by comparing government support of patriotic hacking and the historical advocacy of privateering on the high seas.

Lessons Learned from Privateering

Although we often read about how the Internet has become a lawless space where governments can no longer control the actions of individuals, this situation is not new in the history of the world. Before the 1900s, global violence was carried out by a slew of non-state actors.[20] One of the more impactful groups of private players in the market of international conflict was the privateers. In this section, I describe the practice of privateering and compare it to governmental promotion of patriotic hacking. Then I present an example that demonstrates why privateering was ultimately abolished as a state practice, and why governments today might likewise wish to discourage patriotic or privateering hacking.

Privateering occurs when a private person or ship engages in a maritime conflict under the authority of a state involved in the conflict. Whether for reasons of patriotism or plunder, the privateer has tacitly been given license to attack enemy ships and seize the cargo.[21] Privateering could only be conducted while a conflict was ongoing between countries, and a privateer's attacks on the objects of a sovereign involved in the conflict were considered hostile acts.[22] Privateers differed from militias in that privateers acted largely independently of a national navy. They were, in fact, often employed by a sovereign to compensate for a weak national navy. Nations attempted to control the actions of their privateers by requiring them to post a bond. These governments also inspected the privateers' ships to ensure compliance with restrictions on their operations.[23] Although it originated much earlier, privateering was a popular practice in naval conflicts from the 1500s to the 1800s.[24]

Given this description of privateering, similarities can be found between privateering and government-sponsored patriotic hacking, and in the justifications states have used to promote these actions. First, both privateering and government-sponsored patriotic hacking may amount to combat actions taken by private individuals and groups under the authority of a national government. Second, although there is still significant debate about where the threshold is for cyber attacks, it can easily be argued that the actions of both a privateer and a patriotic hacker can amount to a hostile act that leads to or occurs during a conflict.[25] Third, both types of actors are motivated by patriotic and potential financial gain, and both often have an adventurous spirit. The privateer and hacker enjoy being legally authorized to do what would otherwise be considered illegal.[26] They both seem to enjoy the notoriety they gain from being "semi-rogue" actors in support of their nation. Even if the patriotic hackers do not gain directly from their actions during a conflict, they may use their increased notoriety to seek future financial reward as a cyber security consultant or hacker for hire. Lastly, both types of actor are free to choose their level of involvement in a conflict. Since they do not sign a contract binding them to a term of service nor are they conscripted and obligated to serve, they can withdraw from a conflict at will without the risk of being tried for desertion.

While there are several similarities, a few differences relating to relative risks of privateering and patriotic hacking also bear mentioning. First, the personal risks to the privateer are much higher. In order to seize booty, the privateer had to venture far from home and place themselves in danger of direct confrontation with foreign naval vessels. If caught by the enemy, they were often hanged as pirates. On the contrary, the patriotic hacker need never leave the relative safety of their basement. Adding in the greater potential for the patriotic hacker to act with anonymity in cyberspace, even an adversary that has the military means to retaliate will have difficulty locating them quickly enough to do so. Second, the financial risk to the patriotic hacker is also much lower. There is no need to invest in the fast and sturdy ship that was required for the privateer to chase down and threaten enemy shipping. The patriotic hacker only needs their laptop computer, Internet connection, and the short time needed to learn the skills required to contribute to a denial of service attack. In fact, the patriotic hacker need not be concerned about the financial gains of their action to compensate for any risks. They can hack at night and still work a day job. These factors surely make the idea of joining the ranks of patriotic hacking much more appealing than joining a privateer ship's crew. Lastly the physical threats to victims of the patriotic hackers' actions are much lower. Website defacement and other attacks may generate a financial loss for the victim, however there is much less risk of a loss of life from patriotic hacking than from privateering. This difference de-sensitizes the populace of both parties to a conflict to the risk from patriotic hacking and may make it more difficult to impress upon governments that they should not encourage the behavior. These differences do not lessen the practicality of drawing comparisons for policy reasons. In fact, they may serve to strengthen the argument made later that the actions of the patriotic hacker will be difficult for a government to control and align with national policy.

In addition to comparing the activities themselves, it is useful to compare the justifications forwarded by leaders who have endorsed both activities. Interestingly, sovereign rulers use the same justifications to promote patriotic hacking as they did to promote the activities of privateers. For example, England in the 1500s did not have the technology or revenues to generate a national navy strong enough to compete with sea powers like Spain, thus the English rulers authorized privateers to exercise political power and conduct warfare on their behalf.[27] In the 1600s, states essentially invented plausible deniability to promote privateering. According to Thomson, if a venture met with success, the ruler could claim a portion of the financial profit and all the political profit, but if it was a failure or was condemned in the international community, the ruler could claim it was a private operation.[28]

However, even with these arguments supporting the practice, national governments eventually decided to abolish privateering. The reasons for this change of attitude are demonstrated in the story of one of the most infamous privateers, the "Sea Dog," Sir Walter Raleigh.

Sir Walter Raleigh first set sail as an explorer in 1584 under the authority of Queen Elizabeth I to colonize the New World.[29] After many years of uneven luck, he became a privateer and led successful raids against the Spanish in the Atlantic.[30] However, in 1618, after the British and Spanish had signed a peace treaty, one of Raleigh's ships attacked a Spanish ship. The Spanish ambassador insisted that King James hold Raleigh accountable for the actions of his crew, which amounted to piracy. In this case, the king was compelled to make an example of Raleigh in order to maintain the peace with Spain. As a result, Sir Walter Raleigh was brought back to London and publicly executed.[31] This story is just one of many that show how difficult it was to control privateers, both during the conduct of war and in peacetime.

Ironically, the state's efforts to incentivize the privateer to take personal risks made it that much more difficult for the authorities to control their actions and the risks they posed to international relations. Once the privateers had tasted the excitement of acting with impunity during a conflict, the crews became harder to control during lulls in the action. During such lulls, the privateers reverted to piracy.[32] The cycle would start again during the next war when, suddenly, pirates were legitimized as privateers. The privateers then began to attack both friendly and neutral ships during war and peacetime, a pattern of privateering behavior that several researchers found throughout history. Statham noted, for example, that even if a privateer captain wanted to follow the rules, his crew had little regard for the laws of war, and trying to control them risked sparking a mutiny.[33] The famous naval theorist Julian Corbett complained that, by the 1800s, the privateers' actions had become militarily counterproductive.[34] He argued that sporadic and disorganized attacks by privateers "could never be so efficient as an organized system of operations to secure a real strategical control of the enemy's maritime communications."[35] The pressure mounted, and by the 1800s the allies of countries that still promoted privateering, neutral countries, and insurance companies all began to complain about the effects of privateer attacks.[36] Finally, when Great Britain determined that privateering was becoming more advantageous to its weaker adversaries than to itself, the government agreed to ban naval attacks on neutral ships in exchange for a ban on privateering. The resulting Declaration of Paris was signed in 1856 by parties to the Crimean War.[37] By World War I, all major powers had committed to adhere to the tenets of the Declaration of Paris, and privateering was no more.[38]

So how do these lessons apply to cyberspace? Experts have in fact identified similar challenges in synchronizing the private actor's actions in cyberspace with government objectives. For example, the hacker could ignore orders to stay off critical networks and direct their attacks against domestic and friendly targets.[39] Lin takes the challenges of controlling patriotic hackers a step further, arguing that they could even hinder control over escalation of a conflict. He suggests that a rush of patriotic hacking activity may contribute to "catalytic escalation," which occurs when "some third party succeeds in provoking two parties to engage in conflict."[40] The anonymity of cyberspace exacerbates the potential for malicious third parties to blend in with patriotic hackers and instigate instability or contribute to escalation.

The issues raised to this point have been developed independently of legal considerations, given that privateering was widely abolished before the laws of armed conflict had been codified. However, as the application of international humanitarian law in cyberspace becomes clearer, two additional disadvantages to promoting patriotic hacking have become apparent: the potential for patriotic hackers to become legally targetable during a conflict, and the potential for their actions to make a government responsible for violating the laws of armed conflict.

Additional Concerns with Promoting Patriotic Hacking

Governments that adhere to international law, specifically the law of armed conflict (LOAC), should consider the legal implications of their position toward patriotic hackers. The *Tallinn Manual*, drafted by a panel of international legal scholars under the sponsorship of the NATO Cooperative Cyber Defense Center of Excellence, provides an analysis of international law as applied to cyber warfare.[41] While the manual is not considered a definitive interpretation of LOAC as it pertains to the domain, policymakers may use the arguments contained therein as a starting point when considering the actions of patriotic hackers and national responsibilities under LOAC. As argued by the authors of the *Tallinn Manual*, LOAC does not prohibit private actors from participating in a conventional conflict nor does it prohibit anyone from participating in a cyber operation as part of an international conflict. However, the legal consequences of being an active participant may differ according to the category to which an individual belongs.[42] For example, members of the armed forces of a party to a conflict are designated as combatants, and they have the legal right to participate in international conflicts. Importantly, this affords them combatant immunity and, if captured, prisoner of war status. However, lawful combatants are also assigned "targetability," meaning they can be lawfully targeted by the adversary. In the extreme, such targeting means being killed without any repercussions for the adversary, who also has combatant immunity. Thus a civilian who participates directly in hostilities will lose the protections given civilians during the time they are participating.[43] Therefore, it is important to understand what status a patriotic hacker will maintain during a conflict and the implications for their personal safety if they should become the target of a conventional attack. This status, which is directly influenced by the state's position toward the patriotic hacker, may also affects state authorities' liability for the hacker's actions.

Referring to the *Tallinn Manual*, the authors argue that organized patriotic hackers that have any *de facto* relationship to a party to an armed conflict may be considered combatants.[44] As such, the patriotic hacker would be afforded combatant status rights but also the responsibility to adhere to LOAC. The two important requirements here would be that the hackers be organized, meaning there is some form of leadership and internal discipline system to enforce adherence to LOAC, and that some form of relationship exists between the state and the organization that need not be officially declared. According to Rule 26 of the *Manual*, the authors suggest that the relationship may be a "tacit agreement or conclusive behavior that makes clear for which party the group is fighting."[45] Therefore, when a state openly promotes the behavior of organized patriotic hackers, or others can show that the state has even covertly promoted the actions, it may achieve the threshold of a *de facto* relationship between the state and the hacker group. Therefore, "promoting" and "integrating" could be seen as the same relationship from the perspective of international law.[46]

If a state chooses to ignore or even discourage the actions of the patriotic hackers, the *Tallinn Manual* authors assert it no longer matters whether the hackers are organized as a group. In this case, there is no *de facto* relationship, so the patriotic hackers would not meet the minimum requirements to be lawful combatants. They then become at best "unprivileged belligerents." According to Rule 29 of the *Tallinn Manual*, they would remain civilians and no longer enjoy the benefits of combatant status, such as combatant immunity and prisoner of war status, should they be captured. However, should the hackers still choose to engage in the conflict, they would lose their protection from attack, by cyber or other means, and become lawful targets of the adversary. Should the state actively discourage the patriotic hacker, it will recognize its responsibility to protect citizens from being targeted by an adversary's military operations. The state could also assert it is acknowledging its responsibility under international law to reduce the possibility that any of its citizens will commit a war crime.

To summarize, from the perspective of the authors of the *Tallinn Manual*, if patriotic hackers are organized and at least promoted by the state, they will be recognized as a party to the conflict and have combatant status. In most other cases, patriotic hackers who take it upon themselves to enter the fray will be considered citizens who have lost their protection from attack, including a kinetic attack, when engaging in the conflict with cyber operations. The hackers also will be directly responsible for any war crimes they may commit. Therefore, from a legal perspective, any nation considering encouraging patriotic hacking should take pause: if the patriotic hacker cannot be fully integrated into the operations of government forces, they are best discouraged from launching attacks. Any option in between may leave the hacker in a grey area and create unnecessary risk to both the government and the individual.

Conclusions and Policy Recommendations

In 1856, the world's major powers came together and decided it was time to stop the practice of privateering on the high seas. Is it time to do the same in cyberspace?

Non-state actors continue to play a significant role in international conflicts, as they have for hundreds of years. Most types of private party involvement, such as privateering and mercenaries, were largely removed from the international system by the early 1900s. State control of violence in the international system has been looked upon as a much more favorable way to manage conflicts and reduce the potential for escalation and heinous acts. While there have been appealing arguments for promoting patriotic hacking to achieve national ends, history has shown that promoting private violence for public ends has had a detrimental impact on the nations that encouraged it, as well as on global security. A comparison with the historical practice of privateering has been useful to highlight the drawbacks of such a course of action. Patriotic hacking is similar to privateering in many ways such as the combatant status and goals of the private actors to engage in conflict to support national objectives. They are also similar in the justifications that governments used to encourage their behavior such as the desire to leverage expertise outside the military and provide plausibility deniability for hostile actions. Admittedly, there are significant differences between the high-risk but high-reward pursuit of privateering and the low risks and low barriers to entry associated with patriotic hacking. However, the differences do not significantly detract from the potential lessons that modern nations can gain from a comparison. In fact, the lower risks to the patriotic hacker will most likely exacerbate the challenges a government would have controlling their actions. Some countries less interested in their standing within the international community may continue to encourage patriotic hacking to achieve state objectives, if the benefits continue to outweigh any challenges the government has in controlling the hackers' actions. But for countries that want to adhere to international law and ensure their citizens do the same, promoting patriotic hacking in lieu of developing a professional force should not be considered an option.

Therefore, these private actors should be either discouraged from participating in a conflict on behalf of the government or the patriotic hackers should be fully integrated with government cyber defenders. In order to discourage the actions of patriotic hackers, a publicly stated policy denouncing their actions could be developed and promulgated by national law enforcement agencies. The hackers must be made aware of potential criminal penalties to which they would be subjected should they engage in a conflict as a private citizen. On the other hand, integration could take the form of an auxiliary cyber militia to be mobilized during a crisis, such as the one established in Estonia. In Estonia, the voluntary Estonia Defence League Cyber Unit (CU) was established in response to the events of 2007. The main tasks of the CU are to aid in the protection of Estonia's e-lifestyle and strengthen the cooperation between public and private stakeholders in the domain of cyberspace.[47] The Estonia Defence League even provides refresher training for its volunteers so the civilian employers of the members can benefit during peacetime as well.[48] This model appears to be working well for this small Baltic nation as it provides for a close control of the volunteers' actions in the domain but allows the government to maintain a smaller, full time defense organization.

Privateers have historically been proven to be difficult to control both during and after a conflict. We can expect that modern day privateers in cyberspace will be equally difficult to control. Their improper integration can lead to either violations of international law or poor protection from retaliation in a conflict. We should use lessons learned from the past to encourage the professionalization of cyber operators and keep cyber conflict within the domain of state actors in order to reduce global insecurity.

Acknowledgements

I am grateful for the research assistance of Tengku Nur Qistina of the Institute of Strategic & International Studies Malaysia. I am also thankful for comments received on earlier versions of the manuscript from Jordan Thomas, David Fahrenkrug, and two anonymous article reviewers.

Disclaimer

The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or U.S. Government.

Notes

1. Jeffrey Carr, *Project Grey Goose Phase II Report* (Seattle Washington, USA: Grey Logic, March 20, 2009), fserror.com/pdf/GreyGoose2.pdf.
2. James Simpson, "Motohiro Tsuchiya: Patriotic Geeks Wanted to Counter a Cyber Militia," *Japan Security Watch*, February 20, 2012, http://jsw.newpacificinstitute.org/?p=9952; "Desi Hackers Join Indian Cyber Army!"

Gadget Now, August 5, 2010, http://www.gadgetsnow.com/jobs/Desi-hackers-join-Indian-cyber-army/articleshow/6260494.cms

3. Dorothy E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas Holt and Bernadette Schell (Idea Group Inc, 2010), 170–86, https://www.igi-global.com/chapter/cyber-conflict-emergent-social-phenomenon/46425.
4. "A Cyber-Riot," *Economist*, May 10, 2007.
5. James Mulvenon, "Workshop Keynote Speaker James Mulvenon Discusses Dangers of Chinese Cyber Attacks Against America," Text, *Hoover Institution*, http://www.hoover.org/news/workshop-keynote-speaker-james-mulvenon-discusses-dangers-chinese-cyber-attacks-against-america.
6. James Andrew Lewis, "Five Myths about Chinese Hackers," *The Washington Post*, March 22, 2013, https://www.washingtonpost.com/opinions/five-myths-about-chinese-hackers/2013/03/22/4aa07a7e-7f95-11e2-8074-b26a871b165a_story.html?utm_term=.2abf4380709d.
7. Mara Hvistendahl, "China's Hacker Army," *Foreign Policy*, March 3, 2010, http://foreignpolicy.com/2010/03/03/chinas-hacker-army/.
8. Hannah Beech, "China's Red Hackers: The Tale of One Patriotic Cyberwarrior," *Time*, February 21, 2013, http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/.
9. Beech, "China's Red Hackers."
10. Richard Stiennon, *Surviving Cyberwar* (Lanham, MD: Government Institutes, 2010); P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 1st ed. (Oxford and New York: Oxford University Press, 2014).
11. Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* 10, no. 7, http://eujournal.org/index.php/esj/article/view/2941.
12. Carr, "Project Grey Goose Phase II Report."
13. Matthew Dean and Catherine Herridge, "'Patriotic Hackers' Attacking on Behalf of Mother Russia," Text. Article, *FoxNews.Com*, January 16, 2016, http://www.foxnews.com/politics/2016/01/16/patriotic-hackers-attacking-on-behalf-mother-russia.html.
14. Segal, "The Danger of Patriotic Geeks."
15. ET Bureau, "We Need a Community of Ethical Hackers, Says IT Minister Kapil Sibal," *The Economic Times*, November 16, 2011, http://economictimes.indiatimes.com/news/politics-and-nation/we-need-a-community-of-ethical-hackers-says-it-minister-kapil-sibal/articleshow/10748691.cms.
16. "Desi Hackers Join Indian Cyber Army!"
17. Motohiro Tsuchiya, "No. 143: 'Patriotic Geeks Wanted to Counter a Cyber Militia,'" Institute for International Policy Studies, Tokyo, Japan. February 17, 2012, http://www.iips.org/en/publications/2012/02/17153229.html.
18. Heather Harrison Dinniss, *Participants in Conflict: Cyber Warriors, Patriotic Hackers and the Laws of War* (Leiden, Netherlands: Martinus Nijhoff Publishers, 2013), 251–78, http://www.diva-portal.org/smash/record.jsf?pid=diva2:699087.
19. Segal, "The Danger of Patriotic Geeks."
20. Janice E. Thomson, *Mercenaries, Pirates, and Sovereigns* (Princeton, NJ: Princeton University Press, 1996).
21. Edward Phillips Statham, *Privateers and Privateering* (London, England: Cambridge University Press, 2011).
22. Statham, *Privateers and Privateering.*
23. Thomson, *Mercenaries, Pirates, and Sovereigns.*
24. Thomson, *Mercenaries, Pirates, and Sovereigns.*
25. Actions executed through cyberspace that could be classified as hostile acts would be attacks to degrade a national command and control system or attacks that disable critical infrastructure.
26. Ian Rice and Douglas A Borer, "Bring Back the Privateers," *National Interest*, April 22, 2015, http://nationalinterest.org/feature/bring-back-the-privateers-12695?page=3.
27. Thomson, *Mercenaries, Pirates, and Sovereigns.*
28. Thomson, *Mercenaries, Pirates, and Sovereigns.*
29. "Charter to Sir Walter Raleigh: 1584," Avalon Project Lillian Goldman Law Library (New Haven, CT: Yale University, 2008), http://avalon.law.yale.edu/16th_century/raleigh.asp.
30. Angus Konstam, *Elizabethan Sea Dogs 1560–1605* (Oxford, UK: Osprey, 2000).
31. Thomson, *Mercenaries, Pirates, and Sovereigns.*
32. John Jameson, *Privateering and Piracy in the Colonial Period: Illustrative Documents* (New York: Macmillan Company, 1923).
33. Statham, *Privateers and Privateering.*
34. Julian S. Corbett, *Principles of Maritime Strategy* (Mineola, NY: Dover Publications, 2004).
35. Corbett, *Principles of Maritime Strategy*, p. 93.
36. Thomson, *Mercenaries, Pirates, and Sovereigns.*
37. Charles H. Stockton, "The Declaration of Paris," *The American Journal of International Law* 14, no. 3 (July, 1920): 356–68. doi:10.2307/2187654.

38. Stockton, “The Declaration of Paris.”
39. Segal, “The Danger of Patriotic Geeks.”
40. Herbert Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” *Strategic Studies Quarterly* 6, no. 3 (Fall, 2012): 53.
41. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: Cambridge University Press, 2013).
42. *Tallinn Manual*, Rule 25.
43. *Tallinn Manual*, Rule 35.
44. There was disagreement among the writers of the *Tallinn Manual* as to whether or not the members of the patriotic hacker organization needed to wear a patch in order to meet combatant status. An additional requirement for combatant status under international law is for the combatants to carry arms openly. The complexity of this point would be the topic of another article. Therefore, this article assumes that computers are weapons and those placed on a desk are considered to be in the open.
45. Schmitt, *Tallinn Manual*, p. 98.
46. Dinniss, “Participants in Conflict.”
47. Estonian Defence League, “The Main Tasks of the EDL CU,” Government Document, *KAITSELIIT* (August 17, 2017), http://www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu.
48. Estonian Defence League, “The Main Tasks of the EDL CU.”

ORCID

Forrest B. Hare http://orcid.org/0000-0001-5655-9119