

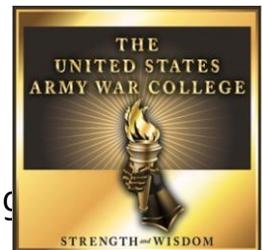
Civilian Research Project  
Army War College Fellow

Trusted Sites?  
Countering Extremist Groups in  
Cyberspace:  
Applying Old Solutions to a New  
Problem

by

LTC Robert W. Schultz  
U.S. Army

United States Army War College  
Class of 2015



DISTRIBUTION STATEMENT: A

Approved for Public Release  
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the U.S. Army War College Fellowship. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

**REPORT DOCUMENTATION PAGE**

Form Approved--OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 01-03-2015		<b>2. REPORT TYPE</b> CIVILIAN RESEARCH PROJECT		<b>3. DATES COVERED (From - To)</b>	
<b>4. TITLE AND SUBTITLE</b> Trusted Sites? Countering Extremist Groups in Cyberspace: Applying Old Solutions to a New Problem				<b>5a. CONTRACT NUMBER</b>	
				<b>5b. GRANT NUMBER</b>	
				<b>5c. PROGRAM ELEMENT NUMBER</b>	
<b>6. AUTHOR(S)</b> LTC Robert W. Schultz U.S. Army				<b>5d. PROJECT NUMBER</b>	
				<b>5e. TASK NUMBER</b>	
				<b>5f. WORK UNIT NUMBER</b>	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Dr. Hy Rothstein, Academic Associate, Joint IO Program Naval Postgraduate School, 1 University Circle, Monterey, CA 93943				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> Dr. Stephen Crocco U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>	
<b>12. DISTRIBUTION / AVAILABILITY STATEMENT</b> Distribution A: Approved for Public Release. Distribution is Unlimited.					
<b>13. SUPPLEMENTARY NOTES</b> Word Count: 5,335					
<b>14. ABSTRACT</b> Countering an adversary that is not physically observable poses a significant challenge, especially when that adversary is operating within the vast space the cyber domain offers. These virtual adversaries are made up of various extremist groups that promote hatred and violence. This paper argues that old operational concepts used in land and sea warfare over the last few centuries could be employed in tandem to counter these extremist groups operating in cyberspace. The first is the concept of false-flag operations that were once used to safely approach enemy maritime vessels in order to subsequently attack them, can now be updated to do the same against extremist websites. The second is the concept of pseudo operations, once used to infiltrate an extremist group's physical area of operation for the purposes of gathering intelligence and disrupting operations by posing as members of these groups can be updated and employed in cyberspace to infiltrate a virtual area of operation controlled by extremist groups.					
<b>15. SUBJECT TERMS</b> Cyber, Cyber Warfare, Computer Network Operations					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b> 20	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b> UU	<b>b. ABSTRACT</b> UU	<b>c. THIS PAGE</b> UU			<b>19b. TELEPHONE NUMBER (w/ area code)</b>



USAWC CIVILIAN RESEARCH PROJECT

**Trusted Sites?  
Countering Extremist Groups in Cyberspace:  
Applying Old Solutions to a New Problem**

by

LTC Robert W. Schultz  
U.S. Army

Dr. Hy Rothstein, Academic Associate, Joint IO Program  
Naval Postgraduate School,  
Project Adviser

Dr. Stephen Crocco  
U.S. Army War College Faculty Mentor

This manuscript is submitted in partial fulfillment of the requirements of the U.S. Army War College Fellowship. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the United States Government.

U.S. Army War College  
CARLISLE BARRACKS, PENNSYLVANIA 17013



## **Abstract**

Title: Trusted Sites?  
Countering Extremist Groups in Cyberspace:  
Applying Old Solutions to a New Problem

Report Date: 1 March 2015

Page Count: 20

Word Count: 5,335

Key Terms: Cyber, Cyber Warfare, Computer Network Operations

Classification: Unclassified

Countering an adversary that is not physically observable poses a significant challenge, especially when that adversary is operating within the vast space the cyber domain offers. These virtual adversaries are made up of various extremist groups that promote hatred and violence. This paper argues that old operational concepts used in land and sea warfare over the last few centuries could be employed in tandem to counter these extremist groups operating in cyberspace. The first is the concept of false-flag operations that were once used to safely approach enemy maritime vessels in order to subsequently attack them, can now be updated to do the same against extremist websites. The second is the concept of pseudo operations, once used to infiltrate an extremist group's physical area of operation for the purposes of gathering intelligence and disrupting operations by posing as members of these groups can be updated and employed in cyberspace to infiltrate a virtual area of operation controlled by extremist groups.



**Trusted Sites?  
Countering Extremist Groups in Cyberspace:  
Applying Old Solutions to a New Problem**

Countering an adversary that is not physically observable poses a significant challenge, especially when that adversary is operating within the vast space the cyber domain offers. These virtual adversaries are made up of various extremist groups that promote hatred and violence. For them, cyberspace provides a virtual safe haven in which to operate using websites to promote their cause, raise funds, communicate, and grow. Based on the increasing number of extremist websites it appears that the results of United States (U.S.) efforts to counter these on-line operations have been disappointing; a lot of work undertaken too little overall effect, which points to the need for innovative strategic solutions to counter these terrorist organizations in cyberspace.<sup>1</sup> However, rather than creating new strategies that require a tremendous amount of brainpower, manpower, and money, this paper argues that old operational concepts used in land and sea warfare over the last few centuries could be employed in tandem to counter these extremist groups operating in cyberspace. Specifically this thought piece offers two age-old operational concepts. The first is the concept of false-flag operations that were once used to safely approach enemy maritime vessels in order to subsequently attack them. This tactic can now be updated to do the same against extremist websites. Second, the high risk and deceptive concept of pseudo operations, once used to infiltrate an extremist group's physical area of operation for the purposes of gathering intelligence and disrupting operations by posing as members of these groups can be updated and employed in cyberspace to infiltrate a virtual area of operation controlled by extremist groups. These operational concepts are provocative

because they have sometimes been associated with the use of “dirty tricks” since sponsorship and oversight was often haphazard.<sup>2</sup> Recognizing these concepts do not come without controversy, this paper also suggests a legal framework to feasibly and legitimately execute these operations by reinvigorating the age old practice of issuing Letters of Marque and Reprisal.

### **The Need for Novel Solutions.**

What makes extremist groups a unique threat in cyberspace is that the majority of these organizations cannot be tied to a recognizable or accountable body, namely a nation-state. During the Cold War it was much easier to tie provocative behavior to the Soviet Union, and even easier during the transparent struggle for world domination during the WWII fight with Nazi Germany and Imperial Japan. Today most extremist groups are acephalous—comprised of dispersed organizations and individuals lacking any clear command structure.<sup>3</sup> In order for these organizations to be successful, they must be able to encourage loyalty with their members through constant, clear communications. This has made these extremist groups true beneficiaries of cyberspace. Utilizing websites and social media outlets, these groups have been armed with unparalleled global reach in which to organize and conduct operations such as recruiting, fundraising, and training. This new domain has also enabled them to grow within a loose organizational structure difficult to target using conventional military power. Against these widespread and disparate groups operating in cyberspace, it is a challenge to identify and target their covert activities.

In light of the increasing illicit activities in cyberspace by a multitude of extremist groups, the U.S. must acknowledge that required tools for the application of offensive cyberspace operations against these threats are needed, and before new strategies are created, the U.S. might look to old concepts to meet these new threats.

The advent of information technology has made it possible for the U.S. to carry out unobserved operations and create new opportunities in cyberspace to counter these threats.<sup>4</sup> Additionally, few extremist groups in cyberspace, though equipped with various degrees of information technology and a cyber-security infrastructure, have the capability to detect U.S. efforts in cyberspace. This is due, in part, to the loose organizational structure of most extremist groups that does not account for the training and resources required for detecting and countering hackers, viruses, or false personas. With these favorable conditions, it is time to rethink the integration of offensive capabilities such as the employment of false-flag operations, pseudo operations, and the issuance of Letters of Marque and Reprisal into U.S. military strategy.

### **False-Flag Operations.**

Today, false-flag operations are seldom used but are defined as secret or disguised military operations designed to deceive an opponent in a manner that the operations appear as though they are being carried out by groups or nations other than those who actually planned and executed them.<sup>5</sup> When employed in cyberspace, false flag operations could be used to disguise offensive cyber operations so that they appear as though they are being carried out by other entities up until the time in which the virtual attack is executed.

The term "false flag" has its origins in naval warfare where the use of a flag other than the ship's legitimate flag is used to deceive an enemy maritime vessel in order to get close enough so that it could destroy or capture it. This tactic has long been legally acceptable under the *Law of Armed Conflict*, which permits the wearing of enemy uniforms prior to engaging in combat.<sup>6</sup> However, the use of false-flag operations faded away in the mid-1800s, with the exception of the German navy during both war wars, as many nation-states believed these operations were being carried out without proper oversight or governmental control, primarily by pirates to commit atrocities which were then wrongly blamed on other nation-states.<sup>7</sup> This of course would not be the case for these operations in cyberspace, and in fact, such deceptions are legitimized under articles 37-39 of the Geneva Convention which state,

Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.<sup>8</sup>

False-flag operations in cyberspace can certainly be used to create negative perceptions of targeted extremist groups by creating and amplifying the amount and veracity of self-destructive organizational behavior, such as radical changes in ideology or similar behaviors that would make would-be members, donors, or sympathizers question their support.<sup>9</sup> This makes false-flag operations ideal against these target audiences by creating falsely represented websites, blogs, and chat rooms, then creating a false image of that extremist group with web content that mirrors its ideology. Over time, as readership and membership grow, the content would change to influence

the target audience into believing the ideology is corrupt, or so devious that the target audience would feel obliged to terminate their association with the extremist group.

For example, the recent trend of using online radicalization to fill the ranks of the Islamic State could be countered through the use of false-flag operations undermining the bond of trust between those who may want to join the cause by using false-flag websites to highlight the atrocities of the terrorist organization's followers. Alienating extremist groups like al Qaeda or the Islamic State from the international Islamic community through operational concepts like false-flag operations would not only weaken these organizations' strength in the short term, but potentially eliminate their on-line activities over time.

### **Implications of False-Flag Operations Employment.**

There are three effects we can expect to see if false-flag operations are successful in influencing the trusted bonds between targeted online terrorist organizations and would be supporters. First, in theory, false-flag operations are attacking the legitimacy of a targeted extremist group. If the false-flag operations are successful, we would expect to see a decrease in membership, fundraising, blogs, and chats, as well as increases in other extremist groups attacking messages presented on the false-flag web-sites. Second, we would see targeted extremist groups policing or even attacking other like-minded websites because they are questioning the veracity of sites they do not directly manage. Finally, we would also expect to see an overall decrease in the use of cyberspace as the extremist group and its supporters no longer feel they can operate securely in the medium.

## **Pseudo Operations.**

Another effective deception based on an operational concept used previously against insurgent and terrorist organizations is the pseudo operation. Pseudo operations traditionally employed disguised military forces to infiltrate an adversary's area of operation in order to gain targetable intelligence.<sup>10</sup> In the 20th century, the U.S. has had limited experience with the employment of pseudo operations and has done little to incorporate the concept into its counterinsurgency strategy because of the difficulty and risk associated with inserting effective pseudo forces into the targeted area without compromise.<sup>11</sup> However, with the advent of cyberspace there is a new opportunity to reinvigorate pseudo operations as an operational concept to infiltrate an extremist group's virtual area of operations, with websites, blogs, and chat rooms for the purposes of gathering intelligence and disrupting its online operations. By targeting the organizations' online members, pseudo operations could be used to weaken the bonds of trust between the extremist group and its online supporters.

Historically, the British have had the most experience and success in the employment of pseudo operations. The concept of pseudo operations was essentially developed and utilized after World War II in the insurgency wars of the period such as during the Mau Mau Uprising in Kenya from 1952 to 1960.<sup>12</sup> However, the British did in fact use the concept as early as the Boer War from 1899-1902, where they first developed the concept as part of their counterinsurgency strategy.<sup>13</sup> Pseudo operations have never been fully accepted into U.S. military strategy due to the risks involved with their employment. Whether it is the potential for compromise or the implications of

associating itself with former insurgent members, the U.S. has not had a doctrinal concept on pseudo operations nor has it deployed pseudo operations as part of a military strategy, and certainly not in cyberspace.<sup>14</sup> Unlike false-flag operations that focus on audiences external to the targeted extremist group such as potential recruits and donors, pseudo operations in cyberspace would focus on gaining access to the internal workings of the targeted extremist group in order to gather information with the goal of disrupting the organization from within. Conceptually, web-based pseudo forces could be employed to “role play” as active members and supporters in order to gain access to the inner workings of a targeted extremist group’s online operation. Once inside, the web-based pseudo force would begin collecting intelligence on its members and their activities. As targets within the online organization are developed, the pseudo force would begin exploiting rifts between members and groups within the organization using misinformation, ultimately deteriorating the trust between loyal supporters and the extremist group.

Identifying the right selection criteria of personnel for the conduct web-based pseudo operations are critically important. In order to mitigate the chances of compromise to the pseudo operation, it is essential that the recruits for these operations hail from various organizations to further create a common yet vague association of pseudo team members with each other and also further mask the team from the internal security apparatus of targeted extremist group. History has also proven that the best executors of pseudo operations are those who enjoy seeking a greater degree of adventure in their lives rather than those who are or once were fanatics or could be swayed by peer pressure. In these types of operations the adventure seekers and risk

takers were considered much more reliable and easier to retain for future operations.<sup>15</sup> With the explosion of online gaming over the past 20 years, finding motivated individuals who enjoy the excitement of role playing and the relative secure and low-cost environment of cyberspace will likely be easy to locate, recruit, and train for operations.

The effectiveness of pseudo operations is also proportional to the level of approval and support provided by senior civilian and military leadership. However, despite the possible utility of pseudo operations, there is currently very little support for its implementation in the U.S. military. This is mainly because of the associated risks to pseudo forces and the unintended consequences of compromised operations. Cyberspace, in effect, helps alleviate these concerns with the increased anonymity of the environment and the ability to operate with minimal risk to physical compromise. Including pseudo operations for the future will help address and fully leverage powerful effects that can be brought to bear against extremist groups in cyberspace.<sup>16</sup> Perhaps the freedom that cyberspace offers will give pseudo operations new prospects in the 21<sup>st</sup> century networked world.

### **Implications of Pseudo Operations Employment.**

If pseudo operations are effective, we would expect to see three observable effects. First, since pseudo operations directly attack the internal workings of an extremist group operating online, we would expect to see a decrease in their overall cyber operations and an increase in security measures at targeted sites which would also increase the costs for the extremist group to operate in cyberspace. Examples of increased security measures could be notifications for members to change their

passwords more often, or the use of image credentialing to verify user identification. Second, since pseudo operations are intended to exploit rifts between members and groups within the extremist group, we would expect to see online splintering of the group or its disappearance altogether. Third, as pseudo operations by design induce distrust internal to the organization, the anonymity of cyberspace will exacerbate these types of fissures seen in the physical world as members grow distrustful of each, even other in regular online activities such as chatting and blogging.

### **Letters of Marque and Reprisal.**

To employ false-flag and pseudo operations in cyberspace, there must be a domestically and internationally acceptable policy for their use, a legal framework that justifies their employment, and a necessity for their continued practice. In the U.S., the answer can be found in its overarching legal document, *The United States Constitution*, which states that the U.S. Congress has the power “To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water.”<sup>17</sup>

In the days before nation states possessed a strong naval force, Letters of Marque and Reprisal offered an alternative method of defending interests on the high seas. The strategy of choice at a time where governments found themselves short on revenue and naval vessels became the issuance of these letters.<sup>18</sup> The British government has used this concept since the 13<sup>th</sup> century; known as Privateering Commissions, private individuals would be issued these letters to infiltrate into an adversary’s territory for the purposes of retaliation or retribution against specific people believed to have committed offenses against the British government.<sup>19</sup> In 1765, the

concept of Letters of Marque and Reprisal were written into the Commentaries of English Law which states,

These letters are grantable by the law of nations, whenever the subjects of one state are oppressed and injured by those of another; and justice is denied by that state to which the oppressor belongs. In this case letters of marque and reprisal (words in themselves synonymous and signifying a taking in return) may be obtained, in order to seize the bodies or goods of the subjects of the offending state, until satisfaction be made, wherever they happen to be found. Indeed this custom of reprisals seems dictated by nature herself; and accordingly we find in the most ancient times very notable instances of it.<sup>20</sup>

Simply put, a “Marque” means to make a pledge to someone or something. A “reprisal” means to retaliate for violations or actions taken against one’s own party. A reprisal could be the seizing or destruction of property or persons. A reprisal could involve a small-scale attack or major operations against one’s adversary.<sup>21</sup> Therefore a Letter of Marque and Reprisal would authorize a private entity or person to conduct reprisal operations anywhere in the world or outside of it as is the case within cyberspace.

So effective were these letters during periods of war in expeditiously authorizing a much-needed military capability to wage war at sea that they became solidified in *The United States Constitution*, providing the legal authority by which naval warfare could be conducted by private individuals, commonly known as privateers to promote commerce raiding and the seizing of adversarial ships.<sup>22</sup> The situation is not dissimilar today, a time when extremist groups operate virtually unopposed in cyberspace as the U.S. finds itself falling short on either ability to confront them. Hence the need exists for Letters of Marque and Reprisal to be used to help execute a strategy

that employs a private army of hackers, or cyber privateers, who could legally and legitimately execute cyber activities like false flags and pseudo operations.

The U.S. military, still in the midst of conflicts in Afghanistan and Iraq, finds itself in a conundrum of diminishing funds, resources, and people. Recent sequestration measures have dictated cuts in defense spending that limits the military's ability to create new capabilities and formations. At the same time the use of cyberspace by extremist groups is continuing to grow to the point where cyber warfare is a daily and continuous fight that must be won. The use of these letters to build a force of cyber privateers without the use of taxes could protect U.S. interests in cyberspace while legally justifying the employment of offensive cyber capabilities.

In building these capabilities, Letters of Marque and Reprisal could be issued to any number of the private organizations or individuals that have expressed a willingness to counter extremist groups in cyberspace.<sup>23</sup> Two examples of this in U.S. history were the all-volunteer Rough Riders of the Spanish-America War and the Abraham Lincoln Brigade of the Spanish Civil War. Both were privately-raised American forces that fought for idealistic principles. Today, like-minded private organizations could recruit socially concerned and tech savvy individuals to conduct false-flag and pseudo operations from their personal computers.<sup>24</sup> However, for this concept to work there will need to be economic incentives for the cyber privateers. Each Letter of Marque and Reprisal would need to articulate in detail the parameters of the privateers' activities. For example, the Letter of Marque and Reprisal could prohibit conducting cyber-attacks solely on the grounds of retaliation for attacks against individual privateers. Additionally, the letters would need to define the fiscal incentives

for cyber raids against an opponent's exploitable data such as personal and fiscal information. An appropriate incentive for a privateer would be the use of bank account data or a portion of funds that may have been donated to a targeted online extremist group and confiscated by the cyber privateer. With the proper legal oversight, these prizes would be theirs to keep and profit from. Potential cyber privateers have already showed interest in conducting operations in cyberspace for these purposes. For example, following the deadly attacks on the French newspaper *Charlie Hebdo* Headquarters, outraged tech savvy individuals and groups launched private cyber-attacks on jihadist websites in an attempt to shut down their online propaganda.<sup>25</sup> Imagine the outcome if these attacks were grounded in law and oversight and incentivized with profit?

In addition to false-flag and pseudo operations, cyber-privateers could be issued Letters of Marque and Reprisal to fill specific military requirements the U.S. military cannot or will not meet immediately. Fueled through the incentive of profit, the privateers could expeditiously begin cyber operations as stipulated under the letter.<sup>26</sup> However, in the past privateers have achieved mixed results while supporting state militaries.<sup>27</sup> Whether it was operating beyond the scope of their contracts, or the perception that they exist solely for profit, privateers have yet to establish a positive reputation in national defense. To help correct this perception, the U.S. can draw on a 200-year-old mechanism for providing legal oversight of privateers: prize courts. Historically, representatives of a sponsoring government's prize courts ensured privateers were not rewarded beyond the scope or the authority outlined in the specified Letter of Marque and Reprisal.<sup>28</sup> A prize court could be used to make rulings on the

sale or destruction of seized items, and the distribution of any proceeds. A prize court may also order the return of seized property or funds if the seizure was deemed unlawful. The same judicial concept could be applied today without the need to expand the size or scope of a state's legal system.<sup>29</sup> Under current law in the U.S., federal district courts located throughout the country under Congressional control and oversight have exclusive jurisdiction in prize cases. However, no prize cases have been heard in the U.S. since the statutes were adopted in 1956 as no Letters of Marque and Reprisal have been issued.<sup>30</sup> In any case, should the U.S. decide to reinvigorate Letters of Marque and Reprisal the system to provide judicial oversight exists.

Understanding the circumstances and conditions in which a Letter of Marque and Reprisal could be issued is very important with regard to cyberspace. Unlike land and naval warfare, targets in cyberspace are not physical and therefore not easily identified due to false identifications and Internet Protocol (IP) addresses. However, the burden of proof to determine whether to issue a letter to disrupt, corrupt, influence, or destroy a targeted website or computer network remains the same. These actions should in all likelihood be characterized by three thresholds of legal action, beginning with showing probable cause to conduct offensive cyber operations. Second, the government would be required to demonstrate the preponderance of evidence to the Letter of Marque issuing body. Finally this process would require evidence for action beyond a reasonable doubt.<sup>31</sup>

### **Implications of Letters of Marque and Reprisal.**

Perhaps the best part about the strategic use of Letters of Marque and Reprisal is that they are completely legitimized and therefore legal under current International law and Constitutional law. In *The United States Constitution*, Congress not only had the authority to declare war, but to issue these letters so that the U.S. would have alternatives to engaging in costly wars. This alternative also empowered private citizens to work on behalf of the U.S. government in a military capacity.

Letters of Marque and Reprisal have not been used by the U.S. since 1815 following the conclusion of the war of 1812. However, during the Civil War (1861-1865) the Confederate States used these letters quite extensively.<sup>32</sup> Opponents to letters of Marque and Reprisal often point to the Paris Declaration Respecting Maritime Law, which was ratified by 55 countries in 1856 banning nations from commissioning privateers.<sup>33</sup> However, the U.S. was not a signatory to this declaration which was only pertaining to their use in naval warfare and to date there is no other international laws pertaining to privateering that would preclude the U.S. from using these letters once again for cyberspace operations.

Militarily, issuing Letters of Marque and Reprisal would assist the U.S. in bridging any existing and un-forecasted gaps in cyber-related offensive capabilities due to shirking defense budgets and manpower. In addition to false flag and pseudo operations, these letters could refresh other operational concepts such as spoofing attacks which would provide the U.S. with an even greater strategic advantage in cyberspace.<sup>34</sup> However, attempts to introduce new legislation in Congress over the last two decades authorizing the issuance of Letters of Marque and Reprisal to counter Al Qaeda in 2001 and again in 2007 fell on deaf ears and were quickly dismissed.<sup>35</sup> If

taken seriously, these letters could have saved a tremendous amount of funds, resources, and potentially lives by privatizing the U.S. led coalition's presence in Afghanistan to find Osama Bin Laden.

With cyberspace being such a vast space to operate in, the potential for new or revisited concepts and opportunities are endless. Issuing Letters of Marque and Reprisal empowers the U.S. to implement unique strategies using existing human capital from outside its military apparatus. These letters, given to carefully selected privateers with the skills to traverse cyberspace, may achieve significant effects against adversaries without fearing legal retribution. By recruiting and regulating talented cyber-privateers to carry out false flag and pseudo operations, the U.S. could implement a cost effective approach against extremist groups operating in cyberspace.<sup>36</sup>

### **Considerations for the Employment of New Solutions in Cyberspace.**

With the legal backing of Letters of Marque and Reprisal, false-flag and pseudo operations could be successfully integrated into a U.S. strategy for operating against terrorist organizations in cyberspace. However the following must be considered. **1. Feasibility.** Maintaining clarity between these operational concepts in cyberspace and the civilian authorities and laws that govern their employment is much easier. **2. Suitability.** Normally, these operational concepts come with a limited shelf life because of their deceptive nature. Meaning, adversaries in the physical domain would eventually catch on to the presence of these methods used against them.<sup>37</sup> However, in cyberspace time is on the side of the implementer. Though these operational concepts may take longer to achieve effectiveness, the vastness and anonymity of cyberspace,

allows the false-flag and pseudo operations, supported by the issuance of Letter of Marque and Reprisal, to continue to adjust their methods, techniques, and timing. In terms of targeting extremist groups in cyberspace, operational concepts and overarching strategies of this nature are best when aggregated effects are achieved over time. **3. Risk.** Operations in cyberspace can be difficult to control. However, the risk of compromise should be an acceptable part of doing business. Implementers of these new solutions should assume these efforts will be compromised, as it might be just as advantageous to the operations in cyberspace if the targeted extremist group detected these offensive cyber operations. This would force these organizations to adjust online methods and in the end constantly question their “trusted sites”. Additionally, in the advent of compromise, false-flag and pseudo operations merely need to take the operation off-line and reconfigure and then reappear under another persona, avatar, or website. Finally and perhaps most obvious, operations in cyberspace of this nature assume less physical risk compared to their historical forerunners. For these types of operations, cyberspace should prove to be a forgiving environment that continually allows for renewed innovation without the associated operational risk of loss of life and collateral damage. Regardless, common sense dictates that the U.S. should not ignore any of these low cost and relatively safe tools that can help it achieve its goals in cyberspace with greater efficiency.

## **Conclusion.**

The rapid emergence of cyber-technologies that has connected every corner of the world is being used quite efficiently by extremist groups. Concepts such as false-

flag and pseudo operations can be instrumental in developing strategic solutions that are legally reinforced by Letters of Marque and Reprisal to achieve desired effects. In essence, these concepts in cyberspace represent a departure from conventional U.S. doctrine. Numerous effective defensive cyber-security tools have been developed and implemented already. However, more offensive capabilities are needed in cyberspace to counter emerging threats in the 21<sup>st</sup> century. Creatively cultivating new solutions such as the options discussed here are just such tools. These operational concepts offer a cost effective alternative to building new cyber force structure within the U.S. military or other governmental organizations. But when it comes to countering extremist groups in cyberspace, false flag operations, pseudo operations, and Letters of Marque and Reprisal can provide a myriad of creative options to choose from. However, for the extremist groups, desiring to operate in cyberspace, these operational concepts will cast layers of doubt onto their own cyber operations. In the end, targeted extremist groups will be challenged in determining which of their own websites to trust.

#### Endnotes

<sup>1</sup> Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006) 15.

<sup>2</sup> Dirty Tricks are unethical or illegal tactics employed to destroy or diminish the effectiveness of opponents. See Lawrence E. Cline, *Pseudo Operations and Counterinsurgency: Lessons From Other Countries* (Carlisle, Pennsylvania: Strategic Studies Institute, 2005) 20.

<sup>3</sup> John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (California: Rand Corporation Press, 2001), 241.

<sup>4</sup> Charles A. Fowler and Robert Nesbit, "Tactical Deception in Air-Land Warfare," *Journal of Electronic Defense* (Horizon House Publications Inc., June 1, 1995), 50.

<sup>5</sup> Geraint Hughes, *The Military's Role in Counterterrorism: Examples and Implications for Liberal Democracies*, Letort Paper (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, May 2011), 105.

<sup>6</sup> U.S. Department of the Army, *Law of Land Warfare*, Army Field Manual 27-10 (Washington, DC: Department of the Army, July 18, 1956), note 15, para 54.

<sup>7</sup> Geraint Hughes, *The Military's Role in Counterterrorism: Examples and Implications for Liberal Democracies*, Letort Paper (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, May 2011), 105.

<sup>8</sup> See 1977 *Protocol Addition to the Geneva Conventions of 12 August 1949*, art. 37-39.

<sup>9</sup> Mark E. Stout, John R. Schindler, and Jessica M. Huckabey, *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements* (Annapolis, MD: Naval Institute Press, 2008), 122.

<sup>10</sup> Lawrence E. Cline, *Pseudo Operations and Counterinsurgency: Lessons From Other Countries* (Carlisle, Pennsylvania: Strategic Studies Institute, 2005) 1.

<sup>11</sup> *Ibid.*, 23.

<sup>12</sup> For more information on pseudo gangs during the Mau Mau Uprising see Wunyabari O. Maloba, *Mau Mau and Kenya: An Analysis of a Peasant Revolt* (Indiana: Indiana University Press, June 1993).

<sup>13</sup> *Ibid.*, 2.

<sup>14</sup> Paul Melshen, *Pseudo Operations*, (Newport, RI: U.S. Naval War College, February 1986) 2.

<sup>15</sup> Franks Kitson, *Ganga and Counter-Gangs*, (London: Barrie and Rockliff, 1960), 126.

<sup>16</sup> Mathew Maybourer and Jeffer Johnson, *Pseudo Operations and the GWOT: Prospects for Success* (Monterey, CA, Naval Postgraduate School, 2007), 7.

<sup>17</sup> U.S. Constitution, art. 1, sec. 8.

<sup>18</sup> Ian Rice and Douglas Borer, "A Private Sphere Approach to Combatting Terrorism," *forthcoming in The National Interest* (May-June 2015).

<sup>19</sup> Kelly Gneiting, "A Constitutional Alternate to War, Marque and Reprisal," October 18, 2013, <http://www.independentamericanparty.org/2013/10/an-constitutional-alternate-to-war-marque-and-reprisal/> (accessed February 9, 2015).

<sup>20</sup> William Blackstone, Commentaries on the Laws of England, Section I, Page 249.

<sup>21</sup> Fred E. Foldvary, "Letters of Marque and Reprisal," October 8, 2002, <http://www.progress.org/tpr/letters-of-marque-and-reprisal/> (accessed February 10, 2015).

<sup>22</sup> Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars* (The University of Chicago Law Review Vol. 64, No 3 Summer, 1997) 960-961. See also Theodore M. Cooperstein "Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering," *Journal of Maritime Law & Commerce* Vol. 40, No. 2 (April 2009) 224-229.

<sup>23</sup> Ian Rice and Douglas Borer, "A Private Sphere Approach to Combatting Terrorism," *forthcoming in The National Interest* (May-June 2015).

<sup>24</sup> Abraham Lincoln Brigade Archives, "Spanish Civil War: The Abraham Lincoln Brigade and the Spanish Civil War," <http://www.alba-valb.org/history/spanish-civil-war> (accessed 14 January 2015).

<sup>25</sup> David Goldman and Mark Thompson, "Anonymous blocks jihadist website in retaliation for Charlie Hebdo attack," <http://money.cnn.com/2015/01/11/technology/security/anonymous-charlie-hebdo/> (accessed 10 February 2015).

<sup>26</sup> Ian Rice and Douglas Borer, "A Private Sphere Approach to Combatting Terrorism," *forthcoming in The National Interest* (May-June 2015).

<sup>27</sup> William Young, "A Check On Faint-Hearted Presidents: Letters of Marque and Reprisal," (Washington & Lee University School of Law, VA, May 2009) 10.

<sup>28</sup> Ian Rice and Douglas Borer, "A Private Sphere Approach to Combatting Terrorism," *forthcoming in The National Interest* (May-June 2015).

<sup>29</sup> Kevin Marshall. "Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars" *The University of Chicago Law Review* Vol. 64, No 3 (Summer, 1997) 961-963.

<sup>30</sup> 10 U.S. Code § 7681 - Reciprocal privileges to cobelligerent.

<sup>31</sup> Michael Todd Hopkins, "The Exceptionalist's Approach to Private Cybersecurity: A Marque and Reprisal Model," *ProQuest Dissertations and Theses* (George Washington University: August 15, 2011), <http://search.proquest.com/docview/921187461> (accessed February 2, 2015).

<sup>32</sup> Confederate States Navy Research Center, "Index to Letters of Marque and Reprisal 1861-64 ORN," <http://www.csnavy.org/marque,reprisal.htm> (accessed February 9, 2015).

<sup>33</sup> Donald Petrie, *The Prize Game: Lawful Looting on the High Seas in the Days of Fighting Sail* (Annapolis, Md.: Naval Institute Press, 1999), 143.

<sup>34</sup> Spoofing effects falsify online data and images in order to influence and/or deceive online users to surrender their own data. See Dorothy E. Denning, *Information Warfare and Security* (New York, NY, ACM Press, 1999).

<sup>35</sup> Kelly Gneiting, "A Constitutional Alternate to War, Marque and Reprisal," October 18, 2013, <http://www.independentamericanparty.org/2013/10/an-constitutional-alternate-to-war-marque-and-reprisal/> (accessed February 9, 2015).

<sup>36</sup> Jeremy A. Rabkin and Ariel Rabkin. "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," <http://www.hoover.org/research-teams/national-security-law-task-force/essay-series/emerging-threats> (accessed 10 February 2015).

<sup>37</sup> James Adams, *The Next World War: Computers are the Weapons & the Frontline is Everywhere*, (New York, Simon & Schuster, March 23, 2001), 286.