General Dempsey joins Secretary Carter for testimony before U.S. Senate Committee on Armed Services hearing discussing Counter-ISIL strategy, July 2015 (U.S. Army/Sean K. Harp)

Countering Extremist Groups in Cyberspace

By Robert William Schultz

How can the United States develop effective strategic options to counter extremist groups operating in cyberspace? For groups that promote hatred and violence, cyberspace provides a virtual safe haven from which to operate, using Web sites to promote their causes, raise funds, communicate, and grow. The ability to remain elusive has made these groups the true beneficiaries of cyberspace. Using social media outlets, these groups have a global reach for organizing, planning, and conducting operations. They instill loyalty among their followers through near-constant, clear communication. Cyberspace has also enabled extremist groups to adopt decentralized organizational structures with indiscernible command hierarchies, making them difficult to identify and target using conventional military power.[1]

Countering these adversaries poses a significant challenge. With an ever-increasing number of extremist Web sites, U.S. efforts to degrade these online operations have been inadequate, pointing to the need for innovative strategic solutions to counter these threats.[2] However, the same protection cyberspace offers them also makes these extremists susceptible to deception. This article argues that false-flag operations could provide the strategic means to mask a deception that could degrade the bonds of trust among extremists operating in cyberspace and their loyal supporters by undermining the legitimacy of their governing ideology.

Deception Works

Deception is often employed strategically to manipulate an adversary's perceptions to gain a competitive advantage while disguising the basic objectives, intentions, strategies, and capabilities of the deceiver.[3] In cyberspace,

Lieutenant Colonel Robert William Schultz, USA, wrote this essay while a student at the U.S. Army War College. It won the Strategy Article category of the 2015 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

suitable deception targets could include an organization's ideological infrastructure, legitimacy, and bonds of trust that connect the group with its followers. By targeting these three facets, a deception strategy could directly challenge an extremist group's online existence.

During the 20th century, deception was an essential element of significant military operations. Between 1914 and 1968, over 90 percent of the deceptions conducted in support of military operations were successful.[4] Based on the technology available at the time, these deceptions were executed in the physical domain where actions and messages had to be seen or heard by their intended audience for the deception to achieve its effect. In the virtual reality of cyberspace, however, anyone has the ability to post a message or influence perceptions. In loosely associated groups that are built on rigid ideology, there is space to sow the seeds of dissent by making members look as if they are not conforming to the agreed-upon ideology. Of note, "it is much easier to lead a deception target astray by reinforcing their existing beliefs, thus causing the target to ignore the contrary evidence of one's true intent, than it is to persuade a target to change his or her mind."[5] For this reason, the decision to employ deception must be based on the ability to deceive adversaries into believing something they want to believe as opposed to embracing an entirely new idea.[6] In light of this, the United States should acknowledge that rapidly improving information technologies enhance the ability to initiate unobserved operations and create believable deceptions in cyberspace over a protracted period of time.[7] With these favorable conditions, a means of employing deception could be realized through the use of an age-old operational concept called false-flag operations (FFO).

False-Flag Operations

The term *false flag* originated in naval warfare and describes a ship's attempt to deceive an enemy maritime vessel by hiding or replacing its flag to maneuver closely enough to destroy or capture the enemy's vessel. Though FFOs faded away in the mid-1800s because many states believed they were being carried out without proper oversight or governmental control, FFOs today are more than just a maritime deception tactic. They are holistically defined as secret or disguised operations intended to deceive an adversary into believing that groups or states other than those who planned and implemented the operations are responsible.[8] When employed in cyberspace, FFOs could disguise deceptions in a similar manner. Additionally, where traditional FFOs used a disguise to approach the enemy, in cyberspace the interaction between the deceiver and the deceived is reversed. The deception target must choose to visit the FFO's Web site in the first place for the deception to work.

Furthermore, this concept has long been legally acceptable under the Law of Armed Conflict, which permits the use of disguises prior to engaging in combat, and is also legitimized under Articles 37–39 of the Geneva Conventions: "Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly."[9] Since posting Web-based content is far from engaging in combat, the need to eventually reveal attribution of the sponsor remains a question for legal study. Thus, without actual combat, the Web-based FFO concept is more akin to black or covert deceptions in which the sponsor's attribution remains hidden.[10]

How This Would Work

This concept of FFOs in cyberspace is designed around creatively developing Web sites, blogs, and chat rooms that mirror a targeted extremist group's ideology. First, cyber-deceivers would develop FFO Web-based content consistent with the targeted group's narrative in order to attract and co-opt potential extremist followers as readership and membership grew, the content on FFO sites would gradually change. Over time, the narratives would shift subtly to influence the target audience into believing the target group's ideology is either corrupt or so devious that the target audience would see the bond of trust had been broken, thus compelling supporters to terminate association with the extremist group in cyberspace.[11]

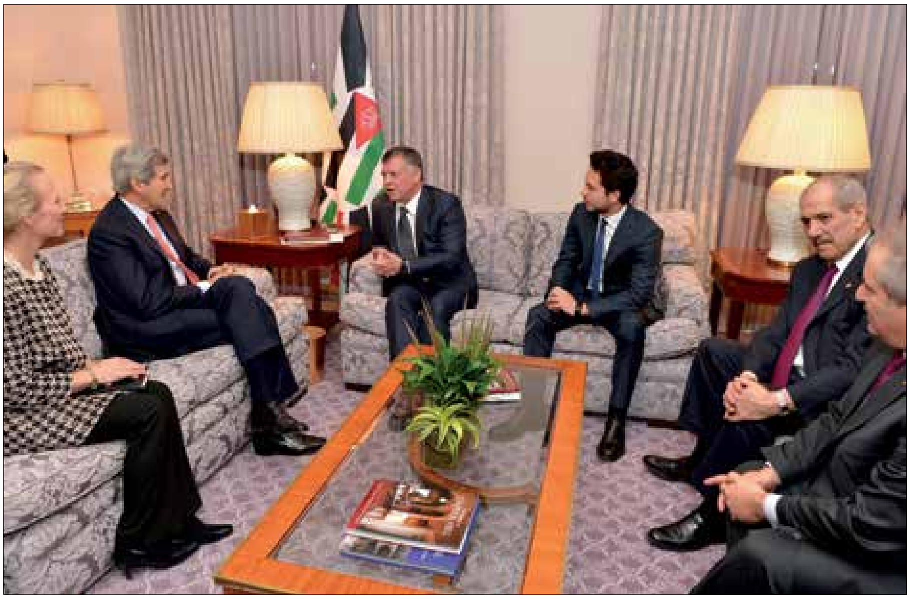
As an example, the recent trend of using online radicalization to fill the ranks of the Islamic State of Iraq and the Levant (ISIL) could be countered through the use of FFOs that undermine the bond of trust between ISIL and potential recruits by using false-flag Web sites to highlight the atrocities of the group's ongoing operations, thus delegitimizing the movement. Alienating extremist groups such as ISIL from the international Islamic community through FFOs would not only degrade such organizations in the short term, but could also potentially discredit its online activities over longer periods.

Implications

There are three effects we could expect to see if FFOs were successful in undermining the bonds of trust between targeted online extremist groups and would-be supporters. First, because cyberspace FFOs would target the legitimacy of extremist groups, we would see measurable changes in online activity, including decreases in membership, fundraising, blogs, and chats, and increases in offensive messages posted on FFO Web sites. Second, we would see targeted extremist groups policing or even attacking other like-minded Web sites because they are questioning the veracity of ideology on sites they do not directly manage. Finally, we would expect to see an overall change in the use of cyberspace, as targeted extremist groups and their supporters—even if they detect the FFO—would no longer feel secure operating in the virtual realm.

Mitigating Risk

FFOs normally have a limited shelf life, as targets will eventually become attuned to the presence of active deception.[12] However, in cyberspace, time is on the deceiver's side. Though cyber-based deceptions may take longer to be effective, the vastness and anonymity of cyberspace allow the deceiver to continually adjust messages and techniques with new strings of code. In terms of



Secretary Kerry and U.S. Ambassador to Jordan Alice Wells meet with King Abdullah II of Jordan, Crown Prince Hussein bin Abdullah, and other top advisors in Washington, DC, February 2015 (Department of State)

targeting ideology, cyber-based FFOs seek to achieve an aggregated effect over a series of unceasing efforts. Just as everyday Internet users have grown aware of the variety of hacking tactics, so will extremist groups grow to distrust their own Web sites as their ideological messages appear to deviate from approved narratives. Therefore, FFO compromises should be expected and welcomed in cyberspace; it would be just as advantageous to the deceiver if targeted groups discovered FFO sites and began to doubt their own information assurance measures.[13] Furthermore, cyberspace's ever-growing domain provides the deceiver with an increased area of operation. If compromised, it is a matter of taking the FFO offline, adjusting content, and then placing it elsewhere in the cyber realm. Regardless, common sense dictates that the United States should not ignore a low-cost and relatively safe tool to help achieve its goals.

Extremist groups such as ISIL are making highly effective use of the rapidly emerging cyber technologies that connect the world. Concepts such as false-flag operations could be instrumental in developing solutions to achieve the desired strategic effect of countering these groups in cyberspace. While some defensive cybersecurity tools are effective, more offensive capabilities are needed to counter emerging threats in the 21st century. Cyber-based deceptions such as FFOs offer a cost-effective complement to traditional military force in the fight against extremist groups. When it comes to undermining and marginalizing the legitimacy of a governing ideology in cyberspace, deception through the use of false-flag operations could provide a variety of strategic options from which to choose. In the end, targeted extremist groups would be hard-pressed to determine which of their own Web sites to trust. JFQ

Notes

[1] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 241.

[2] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 15.

[3] Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981), 294.

[4] Barton Whaley, *Stratagem: Deception and Surprise in War* (Norwood, MA: Artech House Press, 2007), 82–118.

[5] Richards J. Heuer, Jr., "Cognitive Factors in Deception and Counterdeception," in *Multidisciplinary Perspectives in Military Deception*, ed. Donald C. Daniel et al. (Monterey, CA: Naval Postgraduate School, 1980), 60.

[6] Carolyn Pumphrey and Antulio Echevarria II, eds., *Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges* (Carlisle Barracks, PA: U.S. Army War College, November 2003), 4.

[7] Charles A. Fowler and Robert F. Nesbit, "Tactical Deception in Air-Land Warfare," *Journal of Electronic Defense* (June 1, 1995), available at <www.highbeam.com/doc/1G1-17620824.html>.

[8] Geraint Hughes, *The Military's Role in Counterterrorism: Examples and Implications for Liberal Democracies*, Letort Paper (Carlisle Barracks, PA: U.S. Army War College, May 2011), 105. Mid–19th century states feared pirates were primarily conducting false-flag operations (FFOs), and as a result the practice was discontinued. However, during both world wars, the German navy continued to conduct FFOs globally.

[9] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 37. See also Field Manual 27-10, *Law of Land Warfare* (Washington, DC: Headquarters Department of the Army, July 18, 1956), 23.

[10] Thomas W. Smith, Jr., *Encyclopedia of the Central Intelligence Agency* (New York: Facts on File, 2003), 31.

[11] 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.

[12] James Adams, *The Next World War: Computers Are the Weapons and the Frontline Is Everywhere* (New York: Simon and Schuster, 2001), 286.

[13] Heuer, "Strategic Deception and Counterdeception," 294.