The Hyper-Personalization of War

Cyber, Big Data, and the Changing Face of Conflict

Charles J. Dunlap, Jr.

"You may not be interested in war, but war is interested in you."
Leon Trotsky

For those who participate in it, all war can seem "hyper-personalized." But advances in cyber technology have enabled personalization to literally be taken to a whole new level, and this capability may make the role of cyber in future conflicts rather different than what is conceived today.

Popular conceptions of "cyber war" conjure up apocalyptic visions of aircraft crashing into each other due to disabled air traffic control systems, entire cities darkened as result of a computer breakdowns, and even nuclear plants melting down because of misdirected computerized instructions. These are the kind of incidents former Secretary of Defense Leon Panetta warned about in 2012 speech. According to Panetta, he feared a "cyber Pearl Harbor" that "would paralyze and shock the nation and create a new, profound sense of vulnerability. Likewise, President Obama characterized the cyber threat as "one of the most serious economic and national security challenges we face as a nation."[1]

Yet, increasing numbers of scholars are questioning that premise. In 2012, Professor Thomas Rid argued in an arti-

Maj. Gen. Charles J. Dunlap, Jr., USAF (Ret.) is Professor of Law at Duke University focusing on cyberwar, airpower, civil-military relations, and other issues related to national security and international law. Previously, he was a former deputy judge advocate general in the United States Air Force, and served 34 years in the Judge Advocate Corps.

cle entitled "Cyber War Will Not Take Place" that cyberwar has never happened, is not happening, and is "highly unlikely" to occur in the future.[2] Similarly, researchers Jerry Brito and Tate Watkins contended in 2012 that the evidence of an imminent cyber catastrophe is scant. While conceding that "cyberattacks and cyberespionage are real and serious concerns," that statement "is not evidence that we face a grave risk of national catastrophe."[3]

More recently, authors Bill Blunden and Violet Cheung claim in their new book, *Behold a Pale Farce: Cyber War, Threat Inflation, and That Malware Industrial Complex*, that the cyber threat has been overhyped for the purpose, they say, of making the public "so apprehensive and uneasy [about the cyber threat] they'll accept any solution to feel safe again."[4]

Less histrionically, the New York Times reports that prior to operations in Libya in 2010, the United States considered employing cyber methodologies against Gadhafi's military, but ultimately rejected it in part due to the sheer difficulty in doing so. The Times observed that although "popular fiction and films depict cyberattacks as easy to mount…in reality it takes significant digital snooping to identify potential entry points and susceptible nodes." Even then, writing and inserting the "proper poisonous codes" is challenging.[5]

This article suggests that our understanding of the potential permutations of cyber war may be incomplete. Assuming that cyber means will inexorably impact the characteristics of war in the 21st century, it argues that the growing capabilities of cyber methodologies may find a different application in armed conflict than popularly assumed. In particular, "Big Data" technologies mainly intended for commercial uses enable not only the acquisition and archiving of vast amounts of data, but also empower a radically enhanced ability for rapid analysis. The convergence of these technologies will permit what might be called "the hyper-personalization of war."

The Technological Environment.

21st century conflicts will take place in an environment defined by enormous advances in information technologies. Though most realize that the number of people active in cyberspace has grown considerably, the actual figures can still be surprising.

For example, since the year 2000, the number of Internet users has grown 566%.[6] Significantly, this growth is not just in the developed world. The International Telecommunications Union (ITU) reports that by "the end of 2014, there will be almost 3 billion Internet users, with two-thirds of them coming from the developing world." Furthermore, ITU says "the number of mobile-broadband subscriptions will reach 2.3 billion globally," adding, "[f]ifty-five percent of these subscriptions are expected to be in the developing world."[7]

Equally important is the enormous amount of data available in cyberspace. In a 2012 estimate, "90% of the world's data was created in the last two years alone."[8] In fact, 2.5 quintillion bytes of data is created each day, which is "more data than was seen by everyone since the beginning of time."[9] Facebook users alone upload over 350 million images *per day*.[10] As those millions of images indicate, there is a huge amount of personal information accessible online.

It appears that in the not-too-distant future, the U.S. military will be able to launch swarms of drones of drones equipped with facial recognition software…

The loosely defined term for today's massive data sets is "Big Data."[11] Because of its potential to revolutionize how goods are sold, it is almost impossible to overstate the impact of the rise of "Big Data" on global commerce. Recognizing "Big Data's" potential to personalize marketing efforts to a truly unprecedented degree, businesses of all types are clamoring for a way to utilize it, and companies are responding. In the January 2014 issue of the *New York Review of Books*, Alice Marwick reports an entire "database marketing" industry has arisen that is devoted to "collecting, aggregating, and brokering personal data."[12] Marwick describes a firm that:

> [C]reates profiles, or digital dossiers, about millions of people, based on the 1,500 points of data about them it claims to have. These data might include your education level; how many children you have; the type of car you drive; your stock portfolio; your recent purchases; and your race, age, and education level.

Such digital dossiers are sold to retailers who use the information to "hyper-personalize" their marketing efforts to specific consumers.[13] Some companies have used the "phenomenon of hyper-personalization" to categorize "users into neatly defined clusters based on their search history, buying behavior and social trending."[14] In other words, commercial entities can identify individuals or groups of individuals based on their behavior patterns gleaned from data in cyberspace.

The Weaponization of "Big Data". Historically, developments in commerce and industry tend to make their way into the conduct of war. The availability of "Big Data" and the tools to analyze it present a real opportunity for governments to use "off-the-shelf technologies" to enhance their war fighting ability.

One obvious opportunity is to build databases of potential opponents' militaries that could be so detailed as to include electronic dossiers of individual members. The capability may already exist: according to press reports, the NSA collects millions of facial images each day for use in a sophisticated facial recognition program.[15] Consider the recent allegation that Chinese hackers stole thousands of personnel files on U.S. government workers.[16] Such information together with other data and technologies could be exploited during conflicts to personalize the means and methods of warfare to a wholly new degree.

It is critical to understand that cyber-derived data does not sit in isolation from other developing technologies. One technology that achieved significant prominence in recent years is the use of remotely-piloted aircraft commonly known as "drones" to engage in long-term surveillance of battlefields in Iraq, Afghanistan, and elsewhere, and to attack enemy fighters wherever found. Militaries around the world see the potential of these aircraft, and over the next decade spending on drones could top $89 billion worldwide.[17]

While issues exist regarding the current generation of drones' survivability against sophisticated opponents, there will no doubt be further improvements that could permit them to operate in contested air environments. Furthermore, published reports reveal that the U.S. military is developing a generation of small drones capable of operating in networked groups, or "swarms."[18] Other reports suggest efforts to develop lethal micro-drones that "resemble winged, multi-legged bugs" which "swarm through alleys, crawl across windowsills, and perch on power lines" as they seek their target.[19]

Parallel to the rapid development of drone technology is the swift advance of facial recognition software.[20] The linkage of the two in the context of "Big Data" was virtually inevitable. In 2013 the Associated Press, in a story provocatively entitled, "Drones With Facial Recognition Technology Will End Anonymity, Everywhere," explained that given the growing ubiquity of drones linked to massive databases:

> [C]yber experts believe it's only a matter of years — and research dollars — until computers can identify almost anyone instantly. Computers then could use electronic data to immediately construct an intimate dossier about the person, much of it from available information online that many people put out there themselves.

The military sees the potential of these capabilities. *Popular Science* reports the U.S. Army is developing drones that can recognize people at a distance and in crowds.[21] The Army is also seeking to develop a "system [that] would integrate data from informants' tips, drone footage, and captured phone calls" so "a human behavior modeling and simulation engine" could spit out "intent-based threat assessments of individuals and groups."[22]

Warfighting Implications. What does this "cocktail" of cyber technologies mean for warfighting? Quite simply, it appears that in the not-too-distant future, the U.S. military - and likely other militaries - will be able to launch swarms of drones equipped with facial recognition software to roam battlefields looking for very specific members of an enemy's force. These could be officers, but also selected technicians and battle-hardened leaders who possess vital and difficult-to-replace skills.

Of course, militaries have long sought to 'decapitate' their enemies' forces. During the Revolutionary War, General Daniel Morgan, the commander of Morgan's Rifles (an elite group of sharpshooters) employed a "hyper-personalization" methodology that some considered "dishonorable."[23] Morgan and his unit "would hide and target British officers and Indian guides that the British sent out to scout out the land."[24] Although controversial, "it was effective" as it "would often send the British Army into chaos."[25] Sending an army into chaos though hyper-personalized attack is a valued capability in any era.

Drones are widely used today, but what is contemplated here is *swarms* of drones – hundreds, if not *thousands*. This would be a substantially more robust operation than the relatively modest, ongoing but limited effort to use drones to attack "senior operational terrorist leaders."[26] Nevertheless, it is instructive that the publicly available documents obtained from Osama bin Laden's compound during the raid that killed him express much concern about the damage done by drones. As one official put it, correspondence from an Al Qaeda field commander complained "that their guys were getting killed [by drones] faster than they could be replaced."[27]

What makes hyper-personalized war potentially so effective is not simply its ability to cripple military force by eliminating key personnel, but the *psychological* effect it could have on the force as a whole. One of the things that sustains soldiers in the crucible of combat is their relationship with others in their unit. This bonding process – the proverbial "band of brothers" – provides a shield against the psychological isolation of the battlefield. Otherwise, the extreme stress of combat can morph into fear, then panic, and even flight.

Hyper-personalized war alters this calculation by overtly targeting particular individuals; it makes it very clear that certain unit members – primarily the leadership cadre but also critical technicians and experts – are much more at risk than others. To some extent this is always been the case in war; however, the convergence of technologies in the 21st century accentuates and facilitates it in an unprecedented way.

Furthermore, history shows that certain weapons have tapped into primal human instincts in a way that conjures up a dislocating fear that is out of proportion to their actual effect. For example, the taboo regarding gas weapons seems to have originated in the "innate human aversion to poisonous substances."[28] Similarly, it might be said the hyper-personalization of war taps into the primal fear of being hunted.[29] This adds to the psychological disorientation that hyper-personalized war can inflict on modern armies.

Hyper-personalization of war also removes one of the chief "palliative techniques" that soldiers use to deal with combat stress: denial.[30] Essentially, the individual appreciates the danger of the situation but still believes that although others around him may become casualties, "the worst will never happen to [them]" personally.[31] Obviously, when an adversary has the ability to personalize the threat – and perhaps even communicate it directly – that fragile coping mechanism becomes inadequate.

The notion of wide scale - yet personal - contact with individuals of an opposing force is not without precedent. In fact, an early version of the hyper-personalization of war occurred before the start of the war against Iraq in 2003. U.S. forces dispatched thousands of personal e-mails to "Iraqi military officers warning them to abandon their positions and vehicles so not to suffer harm."[32]

Another opportunity to create psychological damage on an opponent's force was suggested in a 2001 article by Christopher C. Joyner and Catherine Lotrionte. They pointed out how terrorists and criminals could:

> "[D]ivert finds from bank computers and corrupt data in databases, causing disruption or panic" and "steal and disclose confidential personal, medical or financial information, as a tool of blackmail and extortion, and cause widespread social disruption or embarrassment."[33]

Today's "Big Data" capabilities would allow these examples to be converted into a means and method of warfare to be used not just by groups of terrorists and criminals, but also by armies in an effort to distract enemy troops from their war fighting focus. Such an operation could include, for example, widespread hacking of various cyberspace accounts of individual deployed soldiers and their families.

Knowing that an adversary could focus their efforts in such a personalized way could itself inflict psychological trauma.[34] Daniel Ventre records a 2007 incident in Denmark where "opponents of Western armed forces in their interventions" identified this vulnerability. He explained that Muslim extremists had "tried to intimidate families of Danish soldiers in Afghanistan" by contacting them directly. According to Ventre, this event "triggered a strong worry amongst the Danish."[35]

What makes hyper-personalized war potentially so effective is not simply its ability to cripple military force by eliminating key personnel, but the psychological effect it could have on the force as a whole.

Ventre relates that the Muslims achieved this effect by hacking email accounts, and by "intercepting cell phone calls between soldiers in Afghanistan and their families." It certainly seems possible that today a belligerent, and particularly one with state resources, could replicate this type of cyber-enabled – yet hyper-personalized - exploitation on a much wider scale.

Legal and Policy Implications.

Does the hyper-personalization of war offend legal or ethical regimes? The short answer seems to be, generally, "no". Developing a means to focus an attack on individual members of an enemy force is not unlawful; it is not, for example, an illegal form of assassination as many seem to believe.[36] In his 1989 U.S. Department of Defense memorandum about Executive Order 12333 (a Presidential directive about policies concerning intelligence activities, including assassination) Hays Parks, one of the nation's foremost experts on the law of armed conflict, detailed why killing individual enemy combatants in war is not "assassination" as understood in common parlance.[37]

Parks draws a sharp distinction between peacetime and wartime killings. "Peacetime assassination," he says, “would seem to encompass the murder of a private individual or public figure for political purposes” something international law prohibits irrespective of an Executive Order.[38] However, the killing of combatants in war is a very different matter. Parks points out that as a matter of international law “the role of the military [in wartime] includes legalized killing” and that combatants “are liable to attack at any time or place.”[39]

Hacking a civilian's e-mail system during armed conflict to direct a propaganda e-mail personally to him or her does not violate the law of war…

An individual combatant's “vulnerability to lawful targeting,” Parks observes, “is not dependent upon his or her ‘military duties, or proximity to combat as such’.”[40] Furthermore, any lawful weapon or technique can be used. Parks cites a number of historical examples, including the 1943 downing of a Japanese aircraft carrying Admiral Yamamoto Isoroku. Accordingly, a cyber-empowered technique that permits hyper-personalization of war could be lawfully employed against individual belligerents.

Furthermore, the consensus among international lawyers is that non-state actors in a bona fide armed conflict who organize themselves into armed groups engaged in continuous combat operations against other similar armed groups or nation-states are subject to individualized attack on the same basis as members of traditional, uniformed militaries, as long as they perform a “continuous combat function.”[41]

Of course, international law prohibits making targets of civilians not directly involved in hostilities. Protocol I to the Geneva Conventions calls upon the parties to distinguish “between the civilian population and combatants in between civilian objects and military objectives.”[42] Protocol I further directs the parties to a conflict “shall direct operations only against military objectives.”[43]

Consequently, civilians “enjoy general protection against dangers arising from military operations.”[44] Additionally, international law provides that “acts or threats of violence the primary purpose of which is to spread terror among civilian population are prohibited.” However, this prohibition does not exempt civilians from *all* consequences of war.

For example, international law only considers “attacks” as cyber operations that are “violent“ - that is, designed to cause death, injury or significant damage.[45] A cyber-operation that is purely *psychological* in nature – such as propaganda - may ‘target’ civilians so long as it does not aim to “incite the population to commit crimes.”[46]

Along these lines, hacking a civilian's e-mail system during armed conflict to direct a propaganda e-mail personally to him or her does not violate the law of war (although it may violate domestic law).[47] Even if a personalized email threatens to target a son or daughter who is serving in the armed forces unless the family fails to take steps to actively oppose the war, it is unlikely that such action would violate international law. It is permissible to attack or threaten to attack a bona fide combatant as, presumably, the actively deployed military family member would be.

In contrast, an email that threatened an action violating the law of war would indeed violate international law. For example, it would be unlawful to threaten to kill or kidnap a civilian family member not directly participating in hostilities. Furthermore, international law prohibits targeting a civilian object not being used for military purposes.[48]

This would mean that a cyber "operation" (as the term is used in Protocol I) designed to hack into a civilian's personal bank account or medical records (as Joyner's and Lotrionte' article hypothesizes criminals or terrorists might do) would be illegal under international law. Indeed, targeting the personal property of a *combatant* is likewise typically a breach of the law because it is not necessarily part of a proper military objective.

Conclusion. The emergence of cyber-enabled "hyper-personalized" war raises a variety of issues for 21st century democracies. For instance, what effect will it have on military recruitment and retention, particularly in the growing number of countries like the US that rely on all-volunteer militaries? Adversaries' abilities to literally "reach out and touch" particular individuals could adversely affect the mindsets of individuals who otherwise would be disposed to serve in the military, as well as "influencers" of military service, such as parents, spouses, and friends.[49]

Moreover, there are a nearly endless number of scenarios where adversaries could hyper-personalize conflict via cyber means. Enemy agents could track the online habits, school schedules, and other activities of servicemembers' children and employ data-mining and other cyber-techniques to pinpoint them. This information could then be used to plot all kinds of actual malevolence against their children, or to simply craft very precise threats toward their families. In either case, enormous anxiety would be generated among the troops about the safety of their loved ones. It would make it almost impossible for soldiers to focus on warfighting duties.

This scenario also shows that the hyper-personalization of war, particularly through the exploitation of open-source information, may disadvantage democracies and other open societies simply because it would be easier to build the database of targets. While it is probable that even the relatively few remaining truly closed societies (like North Korea) will eventually be obliged to provide their peoples with access to the Internet, it is readily conceivable that freer societies where individuals are almost fully unconstrained about the sharing of personal information would obviously be more vulnerable.

Another dark side of the hyper-personalization of war is that the cyber technologies that enable it are not especially unique to the United States or other advanced democracies. In most instances, they are available on the commercial market. In the hands of the totalitarian or repressive regimes - something that is virtually inevitable – these capabilities would facilitate the identification and elimination of dissidents.

At the same time, combatants waging hyper-personalized war who also observe the law could aid in shielding innocents from the consequences of conflict. Not only might the application of force be limited to bona fide belligerents, even within that group only a select few might need to be targeted. Narrowing the number of combatants at risk, and limiting (or even eliminating) many of the dangers to civilians might ameliorate some of the horror of war. Recently, the Israelis illustrated another risk-limiting hyper-personalization technique when they called the personal cell phones of Gaza civilians to warn them that the building they were occupying was about to be bombed.[50]

Finally, it cannot be over-emphasized that hyper-personalized war is not necessarily the only, or even most likely, form of "cyberwar" that we could see in the 21st century. Still, acknowledging and preparing for the inventive application of cyber capabilities occasioned by the rise of "Big Data" and all that comes with it is vital. Absent doing so, we may find ourselves suffering not the "cyber Pearl Harbor" that Mr. Panetta fears, but another one with consequences equally as serious consequences.

NOTES

1 President Barak Obama, "Remarks by the President on Securing Our Nation's Cyber the Structure" (Washington, DC, 29 May 2009).

2 Thomas Rid, "Cyber Will Not Take Place," *Journal of Strategic Studies* 35 (February 2012): 6.

3 Jerry Brito and Tate Watkins, "Cyberwar Is the New Yellowcake," Wired, February 14, 2012 http://www.wired.com/2012/02/yellowcake-and-cyberwar/ (accessed 29 June 2014).

4 Bill Blunden and Violet Cheung, *Behold a Pale Farce: Cyber War, Threat Inflation, and That Malware Industrial Complex* (Walterville, OR: Trine Day, 2014) 9.

5 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya." *New York Times*, 17 October 2011.

6 "World Internet Usage and Population Statistics," Internet World Stats, http://www.internetworldstats.com/stats.htm (accessed 29 June 2014).

7 Brahima Sanou, "The World in 2014: ICT Facts and Figures," http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf (accessed 29 June 2014).

8 "How Much Data is on the Internet and Generated Online Every Minute?," Internet, http://removeandreplace.com/2013/03/13/how-much-data-is-on-the-internet-and-generated-online-every-minute/ (accessed 29 June 2014).

9 Ibid.

10 Cooper Smith, "Facebook Users Are Uploading 350 Million New Photos Each Day," *Business Insider*, September. 18, 2013, http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9#ixzz350CnZqkK (accessed 18 June 2014).

11 Uri Friedman, "Big Data: A Short History," *Foreign Policy*, http://www.foreignpolicy.com/articles/2012/10/08/big_data (accessed 29 June 2014).

12 Alice E. Marwick, "How Your Data Are Being Deeply Mined," *New York Review of Books* 61, no. 1 (9 January 2014).

13 Rachel Strugatz, "Digital's Next Wave: Hyper-Personalization," *WWD* (15 April 2013) http://www.wwd.com/retail-news/marketing-consumer-behavior/digitals-next-wave-hyper-personalization-6892657 (accessed 29 June 2014).

14 Ibid.

15 Dana Ford, *Report: NSA collects millions of facial images per day*, CNN, 2 June 2014, http://www.cnn.com/2014/06/01/politics/nsa-facial-recognition/ (accessed 29 June 2014).

16 Michael S. Schmidt, David E. Sanger, and Nicole Perloth, "Chinese Hackers Pursue Key Data on U.S. Workers," New York Times, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (accessed 10 July 2014).

17 *Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2013 UAV Market Profile and Forecast*, Teal Group, June 17, 2013, http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/94-2013-uav-press-release (accessed 30 June 2014).

18 Debra Warner, *Drone Swarm: Networks of Small UAVs Offer Big Capabilities*, Defense News, June 12, 2013, http://www.defensenews.com/article/20130612/C4ISR/306120029/Drone-Swarm-Networks-Small-UAVs-Offer-Big-Capabilities (accessed 30 June 2014).

19 http://www.theatlantic.com/technology/archive/2013/02/like-a-swarm-of-lethal-bugs-the-most-terrifying-drone-video-yet/273270/ (accessed 30 June 2014).

20 Facial recognition software is:

> [A]n application that can be used to automatically identify or verify individuals from video frame or digital images. Some facial recognition software uses algorithms that analyze specific facial features, such as the relative position, size and shape of a person's nose, eyes, jaw and cheekbones.

"Facial Recognition Software," Tecopedia, http://www.techopedia.com/definition/26948/facial-recognition-software (accessed 30 June 2014).

21 Noah Shachtman, "Army Tracking Plan: Drones That Never Forget a Face," Wired, September 28, 2011, http://www.wired.com/2011/09/drones-never-forget-a-face/ (accessed 30 June 2014).

22 Ibid.

23 "Daniel Morgan," The History Junkie, http://thehistoryjunkie.com/daniel-morgan/ (accessed 29 June 2014).

24 Ibid.

25 Ibid.

26 White House, "Fact Sheet: US Policy Standards and Procedures for Use of Force in Counterterrorism Operations outside the United States and Areas of Active Hostilities," May 23, 2013, http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism (accessed 30 June 2014).

27 Greg Miller, *Bin Laden document trove shows strain on Al Qaeda*, Washington Post, http://www.washingtonpost.com/national/national-security/bin-laden-document-trove-reveals-strain-on-al-qaeda/2011/07/01/AGdj0GuH_story_1.html (accessed 30 June 2014).

28 Harold Maas, *A Brief History of Chemical Warfare*, The Week, September 7, 2013, http://shawnelliott.blogspot.com/2009/03/primal-fear-haunted-by-ghosts-of.html (accessed 30 June 2014).

29 Shawn Elliot, *Primal Fear: Haunted by Ghosts of Predators Past*, March 22, 2009, http://shawnelliott.blogspot.com/2009/03/primal-fear-haunted-by-ghosts-of.html (accessed 30 June 2014).

30 Richard Holmes, *Acts of War: the Behavior of Men in Battle* (New York: The Free Press, 1985) 233.

31 Ibid.

32 Roscini, 240.

33 Christopher C. Joyner and Catherine Lotri-

NOTES

onte, "Information Warfare as International Corecion: A Legal Framework," 12 European Journal of International Law 838 (2001).

34 Daniel Ventre, *Cyber War and Information Warfare* (London: Wiley, 2011) 75.

35 Ibid.

36 See e.g., Bill Quigley, http://www.informationclearinghouse.info/article31330.htm

37 W. Hays Parks,"Executive Order 12333 and Assassination," (US Department of Defense, 2 November 1989), https://www.law.upenn.edu/institutes/cerl/conferences/targetedkilling/papers/ParksMemorandum.pdf (accessed 29 June 2014).

38 Ibid.

39 Ibid.

40 Ibid.

41 *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge Univ: Press, 2013) 116.

42 International Committee of the Red Cross (ICRC), *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, 1125 UNTS 3, art. 48, available at: http://www.refworld.org/docid/3ae6b36b4.html (accessed 29 June 2014). Although The United States Is not a party to Protocol 1, most scholars consider this portion to be part of customary international law applicable to all nations.

43 Protocol 1, art. 52 defines military objectives as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."

44 Protocol I, art 51.

45William H. Boothby, *The Law of Targeting* (Oxford: Oxford Univ. Press, 2012) 387.

46 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford Univ. Press, 2014), 241.

47 Boothby, 398.

48 *Tallinn Manual*, Rule 38, 125-135.

49 Donna Miles, "Army Recruiting Campaign Focuses on Prospects, Influencers," 30 August 2005, http://www.defense.gov/news/newsarticle.aspx?id=16767 (accessed 30 June 2014).

50 Steven Erlanger and Fares Akram, "Israel Warns Gaza Targets by Phone and Leaflet," New York Times, July 9, 2014, http://www.nytimes.com/2014/07/09/world/middleeast/by-phone-and-leaflet-israeli-attackers-warn-gazans.html?_r=0 (accessed 10 July 2014).