



SMALL WARS

JOURNAL

Crowdsourcing: A New Perspective on Human Intelligence Collection in a Counterinsurgency

By *Nicholas Mumm*

Journal Article | Jan 3 2012 - 4:59pm

This is a game of wits and will. You've got to be learning and adapting constantly to survive.
General Peter J. Schoomaker, USA, 2004

As a result of the United States' overwhelming military superiority, its recent adversaries have chosen to apply both unconventional and asymmetric tactics aimed at undermining popular support and confidence in a nation's ruling body. In response, the United States and its allies attempt to use "all instruments of national power to sustain the established or emerging government" (FM3-24, 2006, ix) In short, warfare has become a contest of political influence centered on the population. Success in this environment relies upon the collection, aggregation, and analysis of human intelligence. Networks of human sources enhance the military's ability to understand the perceptions of the population and enrich its decision-making processes aimed at neutralizing the insurgency and shaping public opinion around the legitimacy of its operations.

Unfortunately the United States military is in danger of losing the battle of public influence. The proliferation and ubiquity of mobile (cell-phone and internet) technology has changed the rules of the game. Insurgents are capitalizing on the nearly non-existent transaction costs of establishing groups and distributing information using technology. Insurgent operations aimed at developing networks, gathering intelligence, and distributing information is outpacing the antiquated, inflexible, and unresponsive system employed by our military.

In light of this recent trend, the United States military should seek to strengthen its human intelligence gathering apparatus through crowdsourcing. Leveraging the latest technology, it could create large, interconnected networks capable of instantaneous and inexpensive communication allowing for unprecedented intelligence collection as well as widespread and immediate distribution of information critical in shaping public opinion—a cornerstone of counterinsurgency operations.

The Current System

The importance of intelligence collection in effective counterinsurgency operations is underscored in the U.S. Army's counterinsurgency manual. "Counterinsurgency (COIN) is an intelligence-driven endeavor. The function of intelligence in COIN is to facilitate understanding of the operational environment, with emphasis on the populace, host nation, and insurgents." (FM3-24, 2006, 3-1) And in counterinsurgencies

the preponderance of intelligence must be procured through human sources-human intelligence.

Human intelligence is defined as “the collection of information by a trained human intelligence collector from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities.” (FM3-24, 2006, 3-26) Anyone can receive unsolicited information from a ‘walk-up’ or anonymous source, but Army doctrine mandates that only trained collectors may gather intelligence from designated human sources. Development of a source requires a specially trained Soldier to cultivate a trusting, personal relationship that is tedious, cumbersome and often quite dangerous for both parties. Careless handling of a source by an untrained Soldier increases the source’s chances of reprisal, significantly reducing their willingness to participate. Although intelligence collectors are trained in source protection procedures, this process is not free of risk. In many cases, personal meetings are required between the source and collector to share information. Great care is taken to select a proper site for the meeting, but most must take place in enemy territory or on a coalition forward operating base. Neither offers a safe haven or refuge from the watchful eyes of an enemy insurgent or his allies. (Ohern, 2010) Fears of reprisal are palpable and their consequences are dire. In Afghanistan alone, the United Nations observed “...462 assassinations [in 2010 in reprisal for cooperating with the coalition] according to their records, double the number from the previous year. The figures may not include many killings in remote areas, like the mass beheading, because fearful villagers never reported them.” (Rivera, 2011) Direct and personal relationships with sources also can also be dangerous for the intelligence collector. In December of 2009, seven intelligence collectors were killed in Afghanistan by a source serving as a double agent who detonated a suicide vest after being granted special access to a coalition base by his handlers.

Additionally, the number and capability of trained intelligence collectors is a limiting factor to the size and scope of a human source network. On average, trained collectors represent less than five percent of the total organization conducting counterinsurgency operations and their capacity to develop sources and collect intelligence is finite. Communication between a collector and a source is often limited due to security considerations and the timeliness of a source’s response to specific intelligence requirements is unpredictable.

Currently organizations conducting counterinsurgency operations are limited in their abilities to gather intelligence from or directly communicate with the entire general populace of the host nation. The Army’s Counterinsurgency manual acknowledges that all Soldiers are potential collectors and organizations should incorporate systems to capture intelligence informally collected during routine patrolling. Similarly, it highlights the importance of establishing a security environment that encourages the population to provide unsolicited information (walk-up sources). And, it implores commanders to consider other sources of community-collected, intelligence-written surveys or information gathered by the media, non-government organizations, or contractors as amplifying data for use in analysis and trend identification. However, all of these methods of intelligence collection are contingent upon the security of the population, offer little anonymity, and place anyone who cooperates with the counterinsurgent force in danger of reprisal. Moreover, none of these techniques afford the counterinsurgent force the opportunity to disseminate widely information or receive immediate feedback from the population. Conversely, many insurgent networks are interconnected with technology (social media) and have the ability to immediately and inexpensively broadcast information to the population in their own language. Their message reaches the population first, often, and is effective in shaping public opinion.

Finally, current military organizations conducting counterinsurgency operations lack the technological infrastructure to respond quickly to the “demonstrated ability of extremists to respond quickly with information and misinformation” (Himelfarb, 2010, p. 2). Successful counterinsurgency operations

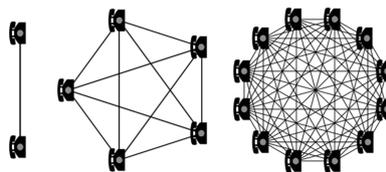
demand the immediate broadcasting of event-driven news. Distributing good news or mitigating the effects of a crisis is critical to a strategy aimed influencing public opinion. The Army's current system lacks the complexity to counteract the insurgent's media dominance. Personal contact with a finite number of human sources, limited engagement of the population at large, distribution of leaflets, radio broadcasts from military outposts, and reluctant use of social media do little to target an increasingly technologically savvy populace inter-connected with a social network.

The Power of the Network

Groups of people are complex, in ways that makes those groups hard to form and hard to sustain; much of the shape of traditional institutions is a response to those difficulties. New social tools relieve some of those burdens, allowing for new kinds of group-forming... – Clay Shirky

Historically humans have gained strength from reliance upon each other. Hunting in groups increased efficiency, consolidated workforces and the creation of the assembly line increased production, and nations bound together by some form of representative government tended to flourish. The contributions of many surpassed those of the individual. The advent of social media based technology has lowered the transaction costs of organization even further. Now, an organization enabled with today's technology can form quickly, establish an informal hierarchy, and communicate cheaply and instantaneously.

The size and capability of these organizations can be explained using Metcalf's law which states that the value of a network is proportional to the square of the number of connected users of the system (n^2). One can simply illustrate this law with the introduction of a cell phone into a community. One cell phone is useless, but the value of every cell phone increases with the addition of more cell phones into the network because of the number of people with whom each user can send and receive phone calls. (See figure 1.1)



(Figure 1.1)

Technology that creates small world networks (social networks) further increases its power. This phenomenon can be explained using Reed's law which states utility of large networks, especially social networks, can scale exponentially with the size of the network. According to Reed, "[E]ven Metcalfe's law understates the value created by a group-forming network [GFN] as it grows. Let's say you have a GFN with n members. If you add up all the potential two-person groups, three-person groups, and so on that those members could form, the number of possible groups equals 2^n . So the value of a GFN increases exponentially, in proportion to 2^n . I call that Reed's Law. And its implications are profound" (Reed, 2001, p. 23-4). Simply stated, technology that creates small world networks establishes structure within a large organization by creating multiple, densely connected small groups making large groups seem smaller and more personal. In essence, this technology has eliminated the transaction cost for humans to fulfill their

basic instinct of participating in a group that shares, participates or acts in concert (Shirky, 2008).

The world-wide proliferation of cell phone technology creates tremendous opportunity for a counterinsurgent force to create a large social network within the population for human intelligence collection. Similar to wireless internet, mobile phone coverage is prolific, inclusive, and growing. Currently there are 5.3 billion mobile subscribers in the world (77% of the world's population) with over 3.8 billion subscriptions (68% of the population) in the developing world alone. Also, almost a third in the US--as well as the 28% of consumers globally report ownership of multiple cell phones (SSI, 2011). Mobile phones are multi-faceted devices with clocks, cameras, and calculators and possess extraordinary latent potential for intelligence collection. Globally, 86% of owners have clocks on their phones, 84% have still cameras, calendars and calculators, 81% have text messaging and 75% have Internet capabilities (SSI, 2011).

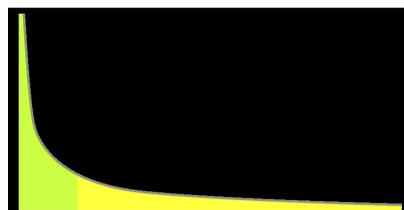
Phone users find value in text messaging and it is regarded as the king of mobile messaging, with 37% saying they use this feature almost all the time and 41% reporting they use it very or quite often (SSI, 2011). In 2011 mobile subscribers are estimated to send eight trillion text messages, and application to person (A2P) messaging, e.g. bank alerts and mobile advertising, is set to overtake person to person messaging in 2016 (mobiThinking, 2011). Internet capability is the third most popular feature (after clocks and text messaging) used almost all the time by 27% of respondents and very or quite often by 31% (SSI, 2011). In 2009 over one-half of a billion people accessed the web via the cell phone and usage is expected to double in the next five years, overtaking web access by PCs. And, by 2011 nearly 85% of handsets sold will allow access to the internet (mobiThinking, 2011).

The growth of the mobile phone market is not isolated to the largest, most-developed countries in the world. For example, nearly 12 million of Afghanistan's 22 million people (54% of the population) are reported to have cell phones (Ackerman, 2010) with coverage spreading across 300 towns in all 34 provinces in the country (Nystedt, 2010). Additionally, nearly 41% of all Africans and almost 68% of Asian countries own some type of cellular device (mobiThinking, 2011).

The global population's participation in social media is prolific across multiple demographics and access through their mobile device seems to be quite commonplace. It appears that it would require little effort by a counterinsurgent force to create a large network using some type of social media. Twitter has grown over 500% in the last few years and Facebook reaches over 56% of active American internet users and is the third most visited site for users 65 and older (Nielsen, 2010). Worldwide, "there are more than 350 million active users [44 percent] currently accessing Facebook through their mobile devices. People that use Facebook on their mobile devices are twice as active on Facebook as non-mobile users" (mobiThinking, 2011). And the amount of time spent by the average American on social media increased over 277% this year (Nielsen, 2010).

Finally, data indicates that cell phone users are quite responsive to calls-to-action sent to their handset via SMS. In June 2009, Shedd Aquarium used advertising on four network television stations to create awareness and drive visitors to a new aquatic show. Each commercial was the same except one of the four stations asked viewers to text instead of navigating to a website. After a viewer texted in, they received a message asking them to respond with their e-mail address and zip code. The study found that the ad with the SMS call-to-action generated 325% more contest entries and comprised nearly 52% of total contest entries despite only running 25% of the ads (Mobile Commons, 2009). Practically speaking, members of an ad-hoc human intelligence community would be quite responsive to direction from the counterinsurgent force. Commanders could instantly broadcast messages to the community directing them to be on the lookout for a certain individual or vehicle or solicit input from the community on the effects of recent operations, and they should expect widespread community compliance

Participation within these large group-formed networks can be modeled using the Power Law or Long-Tailed distribution (Shirky, 2008). What is unusual about a long-tailed distribution is that the “most frequently-occurring 20% of items represent less than 50% of occurrences; or in other words, the least-frequently-occurring 80% of items are more important as a proportion of the total population” (Figure 1.2) (Long Tail-Wikipedia, 2011).



The right side of the graph represents the long tail of the power law of distribution.

(Figure 1.2)

Simply stated, a large number of single human intelligence reports collected from a large population size exceed the value of a large number of reports collected from a few sources. In the past, it was neither possible nor efficient to collect human intelligence reports from everyone in the community; time and resources had to be aligned with a few, reliable sources. Now, it is possible to quickly and inexpensively create a large, inclusive network to take advantage of data collected from sources that were once inaccessible, including those who will only have one significant contribution, ever.

Crowdsourcing

Crowdsourcing is defined as “the act of a company or institution taking a function once performed by employees and outsourcing it to an undefined (and generally large) network of people in the form of an open call” (Howe, 2006). The advantage of crowdsourcing rather than performing operations internally is an organization can gain access to a very large community of potential workers who have a diverse set of skills and expertise who are willing to participate on a limited basis and at a much lower cost (Whitla, 2008). A recent example of crowdsourcing comes from the London bombings of July 7, 2005. Before any of the mainstream media could respond to the scene, eyewitness began to photograph and report the tragedy via their blogs providing the public with thorough and instantaneous media coverage. Having an amateur photographer at the scene with cell-phone cameras was better than a professional photo-journalist who had to travel. Not only did these photos document the destruction of the bombing, but they served as means of immediate communication between survivors and their families, messages of defiance, and means of official notice to the community (a photography of a sign that said all services are suspended) (Shirky, 2008).

Crowdsourcing creates tremendous opportunity to enhance our Army’s human intelligence gathering apparatus. No longer will the population be passive observers of counterinsurgency operations, they will become active participants and stakeholders in the struggle to defeat an insurgency. Additionally, human intelligence gathering will become less dependent upon the security situation of the region. Sources can find security in anonymity, decreasing the likelihood of reprisal for their actions. Also, treating each member of the population as a stakeholder could increase their willingness to participate. As the population begins to see the success and positive outcomes of their reporting, it is safe to assume that the probability of further contributions will increase: success begets success.

A New Model for Human Intelligence Collection

The following could serve as a model for enhanced human intelligence collection. Upon arrival to an area of conflict, the commander on the ground broadcasts a call-to-action via conventional means: media advertisement, leaflet distribution, cell-phone distribution, or word-of-mouth to solicit text message responses from the populace within the area of operations. As members of the community respond via SMS, the counterinsurgent force will capture their information (phone number and e-mail), establish a social network, and initiate an ongoing, two-way conversation with the public through their mobile device. Not only can the commander pass on requests for information to the community, he can use the medium to engage them consistently in an attempt to outpace or delegitimize the message broadcast by the insurgents. As the human intelligence reports begin to arrive from the community, a commander can use a relatively inexpensive software package to aggregate, map, and analyze the reporting, similar to the software analysts currently use to evaluate traditional all-source intelligence. Using the large amounts of data collected, the commander should be able to analyze trends and develop further priority information requirements to push back to the community. A commander can expect the distribution of the population's participation in this social-network to follow the power law distribution. Using this information, the 20% who provide the most frequent reporting could be further evaluated as potential formal, human intelligence sources. Developing a more intimate relationship with these sources will allow a commander to answer additional requirements that may be too sensitive, dangerous or complex to present to the community at large.

As the network becomes more robust, the complexity of both the intelligence requirements and human source reporting could evolve to the point where both could lead to real-time responses to crises. For example, a human source could report the location of an insurgent safe haven via SMS. Upon receipt of this report, the commander could query the particular source or the community for additional information including pictures of the building(s) or the person(s) inside providing a ground force with enough information for an immediate response. Finally, after the ground force responded to the reporting, the commander could broadcast the results of the operation to the entire community providing them with immediate, positive feedback for their contributions.

Haiti Disaster Relief-A model of success

Recently, the concept of crowd-sourced intelligence in support of military assisted disaster relief has proven to be quite successful. In fact, Craig Clarke, an open-source intelligence analyst in the U.S. Marine Corps, noted, "In this postmodern age, open-source intelligence outperforms traditional intel. . . . The notion of crisis mapping demonstrates the intense power of open-source intelligence. . . . [W]hen compared side by side, Ushahidi reporting and other open sources vastly outperformed 'traditional intel' [after the Haiti earthquake]" (Heinzelman & Waters, 2010, p. 2).

On January 12, 2010 a 7.0 magnitude earthquake struck Haiti destroying most of the infrastructure (including 70 percent of its cell phone towers) of its most populous areas and killing over 230,000 people. Multiple organizations from the international community, including the United States military, responded immediately to provide assistance. Despite the widespread devastation, workers were able to restore quickly mobile service providing a lifeline to nearly 85 percent of Haitian households (Heinzelman & Waters, 2010). Although traditional disaster-relief mechanisms allowed for communication and information sharing between the many international organizations, relief efforts lacked the ability to "aggregate and prioritize data that came from outside sources, making it difficult to benefit from valuable

information coming from the Haitian community” (Heinzelman & Waters, 2010, p. 1). With Ushahidi, open-source crisis-mapping software, relief agencies were able to collect, aggregate, and share information they received directly from Haitians quicker and more efficiently than they could through traditional intelligence gathering means.

Using social media (blogs, Twitter, Facebook) and text messages sent from mobile phones, relief workers were able to capture real-time reports, identify immediate needs for medical assistance, food or water, and plot them on an interactive web-based map available to anyone with an internet connection. This data significantly aided relief agencies in the prioritization of their resources. In one example two women and a young girl were rescued from the rubble of a supermarket a few hours after sending a text for help.

Crowdsourcing harnessed innovation from the community, further enhancing the quality of the data and the effectiveness of the relief efforts. With the help of hundreds of volunteers and the Haitian diaspora, relief workers assisted in the collection and translation of thousands of text messages that decreased on-call response times and responses to Haitian community requests for additional resources. Additionally, the thousands of data points received from the community enabled responders to create accurate maps—nonexistent before the earthquake depicting the change in the landscape as a result of the natural disaster and the progress of the disaster relief. Jacob Quintanilla, the coordinator for Communicating with Disaster Affected Communities in Haiti noted in 2009 that the crowdsourcing intelligence model “opens the gates of information to anyone interested, allows citizens in crisis to seek help and helps to foster dialogue between affected communities and services providers” (Heinzelman & Waters, 2010, p. 3).

Additionally, this technology-enabled dialogue created between the populace and the relief workers allowed for the early detection and prevention of violence. On two occasions, the U.S. Marine Corps responded to Ushahidi reports of the formation of angry mobs near food distribution sites. In both cases, security forces dispersed crowds before the situations became violent.. “Ushahidi security reports provided not only information on individual incidents but also insight on the contextual factors that were triggering violence,” a critical aspect in any type of intelligence driven operation. (Heinzelman & Waters, 2010, p. 10)

Despite many successes of disaster relief in Haiti, the use of crowdsourcing did highlight areas that need to be considered to improve future implementation. First, using crowdsourcing to identify and respond to violence requires the establishment of trust through assured confidentiality and confidence in the system. Between February and August of 2010 only 100 of the 12,286 reports received by the disaster relief workers were security-related information (Heinzelman & Waters, 2010). Surveys of the population indicated that initially respondents were reluctant to report in fear of reprisal, but a public education program that introduces the “SMS reporting system in which they [the population] see the computer where the reports come in and are introduced to the staff that receive, respond to, and follow up on messages” (Heinzelman & Waters, 2010, p. 13) will alleviate the public’s fear and instill trust in the system. In short, developing an effective crowd-sourced, human intelligence network will require effective communication, community education and conditioning of the populace.

Second, verification of crowd-sourced information is difficult. “In order for crowd sourced reports to be permanently integrated as legitimate and actionable sources of information, a system must be created to rapidly identify inaccurate information, whether intentional, exaggerated, or accidental” (Heinzelman & Waters, 2010, p.11). Commanders of counterinsurgent forces must be wary of attempts by the insurgents to use the system to their advantage. Limiting reporting to only verified participants or using multiple similar incident reports as a form of corroboration are two techniques that could be used to usurp the efforts of those attempting to game the system. And, continued engagement and on-going public education will be necessary to improve the quality of community reporting.

Conclusions

Harnessing the latent potential of the populace with the use of technology will increase the effectiveness of both human intelligence collection and counterinsurgency operations. Moreover, using the power of a group formed network increases our military's ability to widely and effectively distribute its message. In the words of Rear Admiral Greg Smith "We found that Afghans in the most troubled, insurgent-held areas lived in information wastelands dominated by militant propaganda [and]... we are fighting back with a revamped strategy that puts the people and their ability to communicate at the forefront of our effort" (Lakshmanan, 2010). An ever expanding mobile network is enabling societies throughout the world to become increasingly connected and the United States military should seek to capitalize on this unique opportunity that will permanently change the face of public influence and human intelligence collection.

References

Ackerman, Spencer. "Can Cell Phones Bring Justice to Afghanistan" Wired. October, 6 2010.

<http://www.wired.com/dangerroom/2010/10/can-cellphones-bring-justice-in-afghanistan/>

Department of the Army (2006). *Field Manual (FM) 3-24 Counterinsurgency*

Heinzelman, Jessica & Waters, Carol. "Crowdsourcing Crisis Information in Disaster-Affected Haiti"

United States Institute of Peace Special Report #252. October 2010. www.usip.org

Himelfarb, Sheldon. "Media and Peace building in Afghanistan." United States Institute of Peace-Peace

Brief 15. March 20, 2010. www.usip.org

Howe, Jeff "The Rise of Crowdsourcing." Wired Magazine. June 2006

http://www.wired.com/wired/archive/14.06/crowds.html?pg=1&topic=crowds&topic_set=

Lakshmanan, Indira A.R. "US effort in Afghanistan focuses on cellphone use." Boston Globe. April, 3 '10

http://www.boston.com/news/world/asia/articles/2010/04/03/us_effort_in_afghanistan_focuses_on_cellphone_use/

Li C. & Bernoff J. (2011). *Groundswell-Winning in a World Transformed by Social Technologies*. Boston: Harvard Business Review Press

MobiThinking. "Global mobile statistics 2011: all quality mobile marketing research, mobile Web stats, subscribers, ad revenue, usage, trends..." November 2011. <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats>

Mobile Commons. "Shedd Aquarium Drives Oceans of Awareness with Mobile Commons."

http://www.mobilecommons.com/media/pdf/casestudies/mobile_commons_shedd_aquarium_case_study_20090901.pdf

The Nielsen Company. "2010 Media Industry Fact Sheet." November 2009.

<http://blog.nielsen.com/nielsenwire/press/nielsen-fact-sheet-2010.pdf>

Nystedt, Dan. "Mobile Phone Use Grows in Afghanistan." PC World. July 23, 2008.

http://www.pcworld.com/article/147413/mobile_phone_use_grows_in_afghanistan.html

Ohern, Steven. "Details on Suicide Bomb Attack at CIA Base – FOB Chapman." Intelligence Wars.

January 11, 2010. <http://intelligencewars.com/?cat=14>

Reed, David P. "The Law of the Pack." Harvard Business Review, February 2001.

Rivera, Ray. "Militants Turn to Death Squads in Afghanistan" The New York Times. November 28, 2011
http://www.nytimes.com/2011/11/29/world/asia/haqqani-militants-use-death-squads-in-afghanistan.html?pagewanted=1&_r=1

Shirky, C. (2008). *Here Comes Everybody*. New York: Penguin Books

Survey, Sampling International. "Cell Phones Approach Total Penetration Globally, With Smartphones Moving Toward Market Dominance." Market Watch. November 15, 2011.
<http://www.marketwatch.com/story/cell-phones-approach-total-penetration-globally-with-smartphones-moving-toward-market-dominance-2011-11-15>

Whitla, Paula. "Crowdsourcing and its Applications in Market Activities"
http://www.clickadvisor.com/downloads/Whitla_Crowdsourcing_Application_in_marketing.pdf

About the Author



Nicholas Mumm

MAJ Nicholas Mumm is currently a graduate student at Harvard University's Kennedy School of Government. He is a USMA graduate and has spent the last eleven years serving in the Infantry including a company command and three combat deployments with Second Ranger Battalion

Available online at : <http://smallwarsjournal.com/node/12036>

Links:

- {1} <http://smallwarsjournal.com/author/nicholas-mumm>
- {2} <http://www.wired.com/dangerroom/2010/10/can-cellphones-bring-justice-in-afghanistan/>
- {3} <http://www.usip.org/>
- {4} http://www.wired.com/wired/archive/14.06/crowds.html?pg=1&topic=crowds&topic_set=
- {5} http://www.boston.com/news/world/asia/articles/2010/04/03/us_effort_in_afghanistan_focuses_on_cellphone_use/
- {6} <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats>
- {7} http://www.mobilecommons.com/media/pdf/casestudies/mobile_commons_shedd_aquarium_case_study_20090901.pdf
- {8} <http://blog.nielsen.com/nielsenwire/press/nielsen-fact-sheet-2010.pdf>
- {9} http://www.pcworld.com/article/147413/mobile_phone_use_grows_in_afghanistan.html
- {10} <http://intelligencewars.com/?cat=14>
- {11} http://www.nytimes.com/2011/11/29/world/asia/haqqani-militants-use-death-squads-in-afghanistan.html?pagewanted=1&_r=1
- {12} <http://www.marketwatch.com/story/cell-phones-approach-total-penetration-globally-with-smartphones-moving-toward-market-dominance-2011-11-15>
- {13} http://www.clickadvisor.com/downloads/Whitla_Crowdsourcing_Application_in_marketing.pdf



Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our [Terms of Use](#).
Please help us support the [Small Wars Community](#).