United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

FUTURE WAR PAPER

Wikiwar – Where Campaign Design Unite With The Wisdom Of Crowds

---

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

AUTHOR: LCol André Demers, Royal 22e Régiment

USMC Command and Staff College –
School of Advanced Warfighting

AY 07-08

Mentor: Dr B. Meyer

Approved: _____

Date: _____

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Wikiwar ? Where Campaign Design Unite With The Wisdom Of Crowds	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,School of Advanced Warfighting, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**24**	

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Introduction

We live in an interconnected world where information is becoming the currency of the realm. According to UC Berkeley School of Information we produce more than 550 000 Terabytes[1] of data each year and our current adversaries are leveraging this wealth of information into concrete operational advantages better then we can. By shying away from traditional operational security principles and moving to what could be described as open source warfare, they can adapt more quickly to a given situation. A striking example of open source can be found in the Iraqi insurgency. It took only 12 months to reach (and surpass) capabilities for the deployment of the full spectrum of IEDs in Iraq that took over 30 years for the IRA to achieve under more rigorous operational security (OPSEC) conditions in Ulster[2].

Based on the fact that open source concepts are currently being used by the computer programming community, by many different business sectors and by certain segments of the enemy[3] fighting in the contemporary operational environment, we must ask ourselves if the current military paradigm of operational security is still relevant. This paper will propose that a concept of open source warfare will be far more effective in supporting a campaign design methodology during complex emergencies as opposed to the traditional compartmentalized approach favoured in today's military planning process. First of all, we will look where this concept can be employed and why it would work. Having identified where open source can be useful for the military, we will turn our attention to the need of changing our understanding of OPSEC. Finally, we will propose an open source planning model which will allow us to better leverage information during campaign design and execution.

Relevance of this concept to the spectrum of conflict

The spectrum of conflict is a useful framework to define the potential area where open source warfare could be beneficial to a modern military force as a planning methodology and command and control system. Not surprisingly, open source would not be ideal as a model for operations on the higher end of the spectrum. High intensity combat operations require a high degree of OPSEC and directive command and control in order to synchronize operations across all the combat functions. However, the basic collaborative approach to planning necessary for open source warfare would be a readily transferable skill set for any planning team operating in this end of the continuum.

At the other end of the spectrum we have "phase 0" type operations. Open source warfare would be hard to implement because the lack of a crisis would reduce the willingness to cooperate of large segments of the potential community needed to conduct operations. The individual mandates of the various players will be the driving factor, not the need to coordinate and cooperate. A simple collaborative environment to share knowledge that would contribute to the overall situation awareness of the planning team would probably be sufficient.

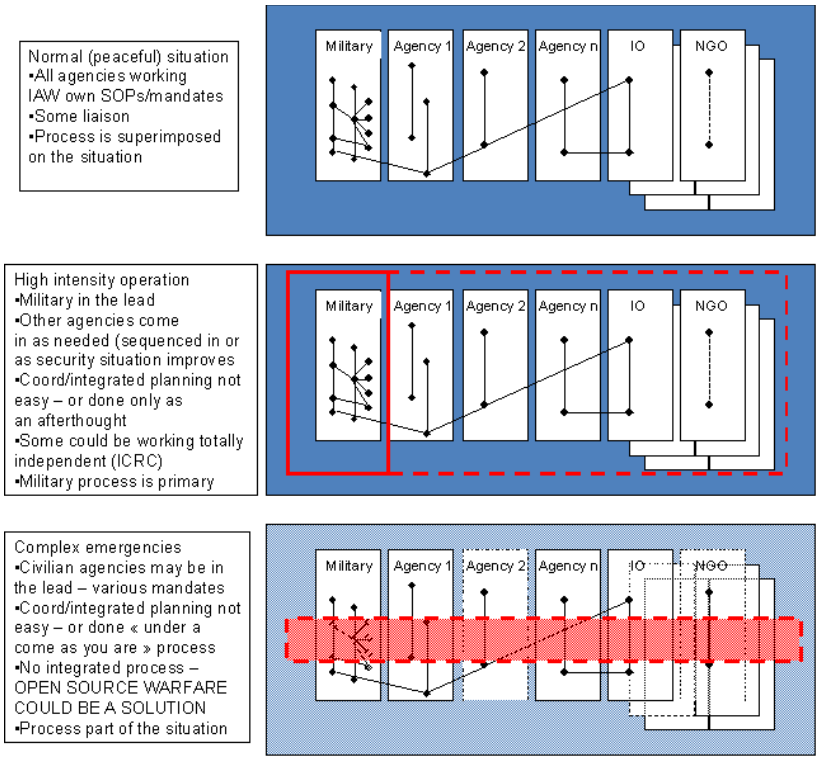

Figure 1 - Implications of the Spectrum of Conflict

Open source warfare would be most relevant for operations situated in the middle of the spectrum, or what could be called complex emergencies. These are best summarized as operations occurring in a highly complex, diverse, diffuse and lethal environment, with numerous stakeholders. Under these conditions, traditional concepts of warfare have broken down, and individual enemies have the ability to inflict strategic defeat through a wide range of means. To succeed in complex emergencies, we must operate within an integrated multi-disciplined team and adapt rapidly to the threats, and achieve instant overmatch in all areas of the theatre of operations[4].

As well, the collaborative environment of open source warfare will be useful if (or when) military organizations adopt Systemic Operational Design (SOD) as a planning methodology.

With the ability to enlist a large community of practice, the open source design team will be able to support the Strategic-Operational Commander (STROC). This will especially be true during the original discourse required to frame the problem in the SOD methodology of campaign design[5].

Why would it work ?

From Wikipedia to Linux, open source is already with us. The business community is already embracing open source (Apache Web Servers and GoldCorp Inc are but a few examples[6]) and it is getting concrete dividends for its effort. The military is already recognizing the benefit of collaborative planning and the usefulness of sharing information. Examples of such tools are the CALL website, the AKO "intranet" and sites such as companycommand.com. These sites are available to soldiers anywhere in the world as long as they have access to a computer and the web. However, these forays into open source are more akin to a form of un-vetted knowledge management rather than a true planning (or coordination) tool which can leverage the collective experiences of the entire user community.

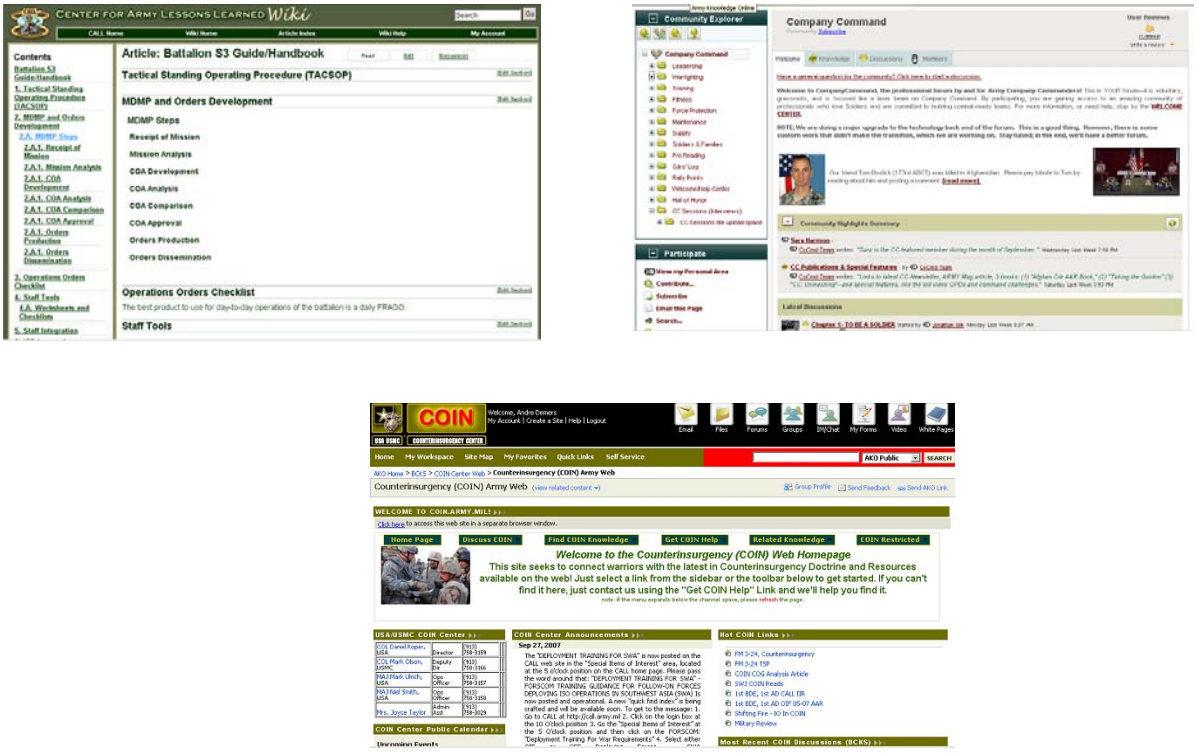

Figure 2 - Collaborative/KM sites of the U.S. Army

A recent open source warfare example is found in actions by the Commander of MNF-W[7] in Iraq. He published and distributed, down to the Iraqi street level, his commander's intent on how he will achieve Provincial Iraqi Control (PIC) in Al-Anbar province. Anyone who wants a copy is welcome to it and all the key stakeholders now have the basic conceptual map of how to achieve the desired end state (a sort of Beta v1.0). Any organisations wishing to participate can easily nest their contribution to the process because they understand the directing thread at the operational level. The tactical details are not available. In any case, these details when taken individually are irrelevant. Any actions that will be nested in the overall concept will be beneficial and will increase the operational momentum to a point where the enemy will not be able to interfere effectively.

The opposite example can be found on the street of a hypothetical third world country[8]. Members of an International alliance are conducting direct action missions against anti-coalition militias. As in the case of previous raids, this particular action was planned and executed in a vacuum that excluded most of the staff in the brigade HQ. The results of the raid were touted as successfully closing down a dangerous IED making facilities. However, what was called a bomb making factory by the planning team was conversely claimed to be a local businessman who was selling explosive for rock quarrying operations. The rocks would then be sold on the open market for use by the displaced persons as the primary building material for constructing new houses in the area. A collaborative approach to this operation could have helped in providing a better assessment of the target and identify second and third order effects of the operations that impacted the population in general and the politically influential friends of the local businessman/ "IED maker" in particular.

Defining OPSEC

Critical to open source warfare will be a new working definition of operational security (OPSEC). This new way of seeing information security will be the key enabler in open source warfare, which will allow for the creation of an effective community of practice available to support the commander. OPSEC is currently defined[9] as protecting information an enemy could find useful supported by the underlying principle of an exclusive "need to know". In open source warfare, the concept will shift to "all in the vetted community should know". This is a huge difference since this assumes that information will be shared by the whole team rather than

by a small select group, i.e. eliminating the OPSEC from within, as is prevalent in current military planning circles.

The OPSEC impetus is shifted onto the trusted individual who must safeguard or pass on the information based on his assessment of the situation. On the practical level, any operational details that will inevitably leak out will get lost in the background noise in the growing explosion of information available via multiple channels. In any case, a distributed enemy will be able to probe any plan by using the simple tactics of massively distributed attack[10]. Once a weakness is identified, the enemy distributes the information via open source and the cycle continues until the weakness does not exist. By this time a new weakness will have already been identified and the cycle will start afresh. This system of attack is not predicated upon the use (or non use) of OPSEC and historical centralized attempts at countering such tactics by controlling the flow of information have not been effective[11].

Because of the original investment in vetting individuals before they are invited to join the community of practice, once they are trusted enough to gain entry into the system it must be assumed that there is a need to know for everything that is relative to the problem at hand. In effect, in open source warfare, the security must be up front and once you are certified you are to be trusted until proven otherwise. There cannot be any OPSEC from within since you will need to get various actors to buy into your plan. Once you accept this fact, and only protect key operational information when it is absolutely necessary, the benefit will be a faster tempo of operation (i.e. a faster orient cycle) facilitated by the free exchange of information within the vetted community.

This paper is not advocating giving secrets away to the enemy. The idea is to be "radically transparent" only within the extended planning team. All the traditional OPSEC functions will be provided by the security architecture of the collaborative planning environment. Radical transparency is already being used in the business field. Various CEOs are now blogging about their company on the Internet, revealing strategic secrets for all to see[12]. Radical transparency is also used in certain print media where the readership base help in writing some stories that will eventually make it in the print edition of the magazine[13]. The basic guidelines for this model are easy enough to follow. First of all, the organisation line diagram (both formal and informal) with relevant biographical and contact information (within and outside the collaborative environment) is provided. This gives a clear picture of who to contact to get results (i.e who actually does the work). Secondly, the planning organisation posts all planning material in a wiki (a wiki is a kind of computer software that allows users to create, edit, and link web pages easily) for all to see. Linked to this concept, there is also a need to make all information available to the entire community of practice at the same time it is available to the planning team. Finally, once the plan is completed, it is put on its own wiki where the operators (and planners) will constantly edit and adjust the campaign in accordance with the situation[14].

Proposed model

The following model is offered for open source warfare. This model is based on the assumption that it would be used to bring together a large community of practice during a complex emergency in order to work towards an acceptable solution to all parties involved.

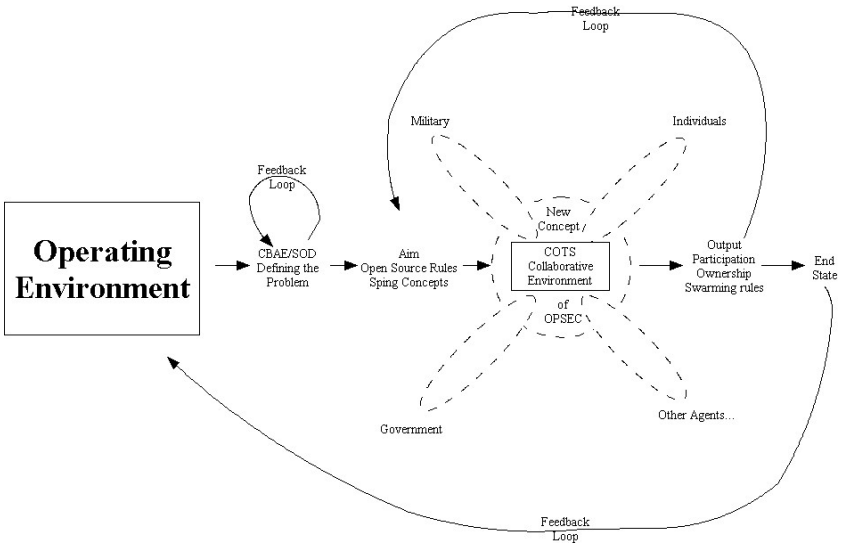

Figure 3 - Open Source Warfare Planning Model

The first step in the model is for the design team to sit down with the commander and define the boundaries of the problem. Once completed, the Commander's Battlespace Area Evaluation (CBAE) is posted via web based collaborative software for the planning community to see and improve upon. As soon as possible, a simple set of operational rules with the desired end state is also posted in the collaborative environment in order to kick start actions on the ground. At this point, the entire community of practice is invited to participate. Using open source rules and a series of simple supporting concepts, everybody starts contributing to the process. Key to the model are the numerous and continuous feedback loops that ensure constant corrections throughout. Every time a correction is included, the process can start afresh or branch off in the new directions caused by the amendment. Super imposed on the model is the new concept of OPSEC allowing for a large pre-vetted community of practice to receive all the information available to the planning team at virtually the same time. Finally, the community of practice collaborates via a very simple web based collaborative architecture operating at the PGP[15] level of cryptographic security. This commercial-off-the-shelf (COTS) architecture will

ensure that all can participate as long as they have a computer, a web browser and access to the World Wide Web.

Open source Rules

The basic rules for open source warfare are derived from the work of Eric Raymond, a computer programmer, outlined in his book *The Cathedral and the Bazaar*[16]. The basic idea comes from the fact that computer programming is a form of complex problem solving. There are two distinct schools of thought on how to create a programme. The 'Cathedral' is a very structured way of approaching the problem. In this method, programmers follow very strict rules and design parameters. This ensures that the final product is shrouded in mystery and can only be truly understood by the design team. The second method, the 'bazaar', is a very loose method of design that allows anybody and everybody to see the basic design philosophy and the basic source code to the programme. Armed with a series of simple, yet elegant, rules any programmer can tap in to the collective wisdom of his co-developers to achieve a viable solution. The end product will improve overtime because all can contribute to the project by building on the basic design as long as they allow, in turn, access to their work. Transferred to a military situation, the cathedral style of planning could be called MCPP, MDMP, JOPES, OPP[17], or any other formal way of conducting planning in accordance with a set of rules prescribed in official doctrinal publications.

This paper recognizes the fact that the military is exploring collaborative planning and C2 systems in order to improve its way of conducting business in the information age. Initiatives like the command post of the future or the current practice of posting planning material, orders, reports and returns and various briefings on unit intranets are all steps in the right direction.

However, these initiatives fall short of open source warfare since they are akin to complex knowledge management procedures in a structured hierarchical system. As the military explore new ways to collaborate and eventually flatten its decision-making process, they will exclude inter-agency and NGO partners that will not be able to plug into this new command and control architecture. The risk inherent in this approach will be an ever-increasing delta between the structured collaborative planning ability of the military and the actual planning capabilities of the inter-agency team. If we agree with the current paradigm that inter-agency operations are the key to winning the peace in future complex emergencies then we need to adopt new rules to help integrate the campaign design efforts early in the process.

This is where open source design rules will come to our help. These rules, coupled with the new concept for OPSEC, are the foundation of the proposed model for open source campaign:

Rule number 1. Know what concept to use (and reuse). Because a basic solution worked in the past and his known and recognized by the community of practice, there is nothing wrong with applying it to the problem under consideration. The experiences of the various agents participating in the collaborative effort should be able to readily adapt the historical model to the situation at hand, nested within their own area of expertise. The military planners would then benefit from seeing the campaign from many different angles all at once and could reconcile major differences of opinion by conducting live Delphi[18] exercises. Recognizing, and implementing, a good idea from the community of practice is a good way to get early buy in into the process of achieving the desired end state. This notion will be linked to the supporting concept of reputation later on in the paper[19].

Rule number 2. Use the power of the entire community of practice. The strength of open source warfare is the ability to leverage the knowledge of all the participants in designing and executing a campaign. Because of this openness, the campaign design and execution team will get rapid validation and improvement of concepts. As well, with enough people looking into the campaign design, part of the problem will probably be obvious to someone in the team and a solution will be crafted. Finally, the people who work for the various members of your community of practice are key in the process as they will immediately field test your solution and provide instant feedback[20].

Rule number 3. Often a solution will come from realizing that the original concept was wrong. Multiple and immediate feedback loops within the model will allow for constant review of the basic rules guiding the design and execution teams. Any fault in the original understanding of the problem or in the basic execution rules will be corrected on the spot rather than waiting for the traditional planning cycle to go through its normal evolution. By removing certain options, other avenues will appear (even counter intuitive ones) resulting in positive momentum with regard to achieving the end state[21].

Rule number 4. Solutions should lend themselves to use across the community of practice. Once a solution has proven to be workable within one area of the community of practice, efforts should be dedicated to adapt it to other areas and gain momentum from the implementation of a proven concept. This rule will become self evident when operating in a region that is composed of distinct sub-areas that will often require solutions to be adapted individually across the lines of operations and in accordance with specific conditions on the ground[22].

Rule number 5. Provided the core planning team has a communication medium at least as good as the internet, and knows how to lead without coercion, many heads are better than one. This rule is more oriented toward the technical aspect of the model. By using COTS software and regular access to the Internet anybody that is invited (and vetted) to join the planning and execution community of practice will be allowed to join. The military will need to accept the difference in training, ability and mandate of the various partners within the community of practice. Because most members of the planning community never heard of MCPP, MDMP, JOPES, etc… the planning software will be the only common piece of the puzzle allowing for easy integration. In the end what should be prized is not the command and control structure but the inputs and solutions offered[23].

Supporting Concepts: Swarming, Wisdom of Crowds, Reputation and COTS Architecture

Open source warfare will rely on large mass of individuals contributing to the campaign design process. A basic understanding of how large groups interact will also be needed in order to support the proposed model:

Swarming

Swarming is defined as "a scheme of manoeuvre where there is a convergent attack of several semi-autonomous (or autonomous) units on a target."[24] Swarming as a form of manoeuvre depends on robust, rapid communications system based on very simple set of command and control instructions. Swarming rules will be one of the first outputs of the planning team. The simple rules will allow agents in the field to self synchronize their actions with each other. Actions in the field will cycle through the swarming cycle of locate, converge,

attack, and disperse[25] using the basic rules issued by the commander to guide their actions. Because of the pulsating nature of operations conducted under swarming rules, it will be very difficult for the enemy to mount an effective counter action, even if the rules themselves become known. As an added benefit, the result of these actions when integrated in the collaborative environment will quickly provide feedback to the community of practice on what works and what does not work.

Wisdom of crowds

According to James Surowiecki, large groups of loosely interconnected individuals are well adapted for solving certain types of problems that are relevant to complex emergencies. Optimum problem sets for these large groups are defined as cognition, coordination and cooperation problems. Cognition problems are problems, which have or will have a definitive solution[26] (where to locate a forward operating base, out to set up a food distribution system for internally displaced persons). Coordination problems are problems that require groups to coordinate behaviour with each other, knowing that everyone else is trying to do the same[27] (using MSR in a theatre of operation while facing an IED threat, distribution of humanitarian aid to a given sector with a heterogeneous population). Finally, we have cooperation problems where the challenge is getting self-interested, distrustful people to work together, even when narrow self interest would seem to dictate that no individual should take part[28] (achieving mission success while respecting individual mandate or ethos, creating a local government).

Within this community of practice, the open source team must guard against homogeneity. The very nature of the collaborative environment should ensure enough variance and access to private information to offset any homogeneity with the main subgroups. The open

source team must also guard against too much centralization. In accordance with the rules of open source warfare, the command and control must be loose and based on collaboration rather than directive control. Once again, the nature of a web based collaborative environment will help in flattening the command structure and its accompanying reporting channels. The design team must also ensure that the collaborative environment does not generate stove piped reporting channel (private chat rooms or private wikis). Finally, because some decisions will need to be made to keep the process moving, the design team must be careful not to take each decision in a way that will force future choices to be made without considering new, emerging facts.

Reputation

Another component of this concept will be how to create team cohesion and trust among the various players involved in an open source planning project. Currently, operational planning teams are usually homogeneous and outsiders are only invited in to address a specific deficiency at a given point during the planning process. Their expertise does not evolve with the plan and their credibility must be rebuilt every single time they contribute to a different planning effort. In open source warfare, the metrics for evaluating the worth of participation will be the prestige resulting from a contribution that moves the process forward towards the defined end state. One's work will become one's statement, where the quality of the input to the process will speak for itself, requiring a free exchange of ideas. Any extra level of OPSEC will be the equivalent of white noise corrupting the vital signal of collaboration.

Feedback[29] on all members will be based on an evaluation coming from all the participants of the open source team based on two easily identified and traceable inputs. This profile will stay with any participant for as long as they are part of any open source efforts giving an added incentive to effective participation. The first input will be a rating of the contribution

based on its quality with regards to the overall process. A simple positive, negative or neutral feedback will be tracked. The second input will be a short comment. The collaborative software will then issue an overall rating to each member which will be useful in establishing trust between members of the virtual community based on proven past performance rather than face to face relationships. To ensure that the process is fair, the participant can evaluate how the core planning team used his contribution. The core team will gain (or loose) in reputation as a team based on effective use of proposed inputs. This feedback loop will ensure that only the best products get to be included in a planning effort and that the plan actually reflects the best work of the community.

To ensure that this system is manageable and does not stifle creative input for fear of losing credibility on the reputation profile, the most effective contribution to the process must be seen as an improvement to an already accepted solution. Discrediting a contribution is not acceptable in open source warfare; all input must be seen as a potential foundation to future improvement. Planning time used to attack rather then improve past concepts will be seen as wasted time. In reputation terms, the added value to the process will be shared by both individuals; the one that came up with the original idea as well as the one who improved it. In effect, the original creator will be credited for the original idea, but any improvement can also be credited to the new designers, linking back to the previously stated idea that one's work is one's statement.

Finally in order to keep the designing process going, once a better way of doing something has been identified by the community of practice, past error or design flaws will not be held against the original author and the entire planning community now continues to plan based on the latest improvement[30].

COTS Model

The last supporting concept covered by this paper will be the information exchange architecture that will support the model. As already mentioned, all support to this model should be available COTS and be usable via the Internet in order to ensure complete plug and play for every member of the community of practice regardless of their resources.

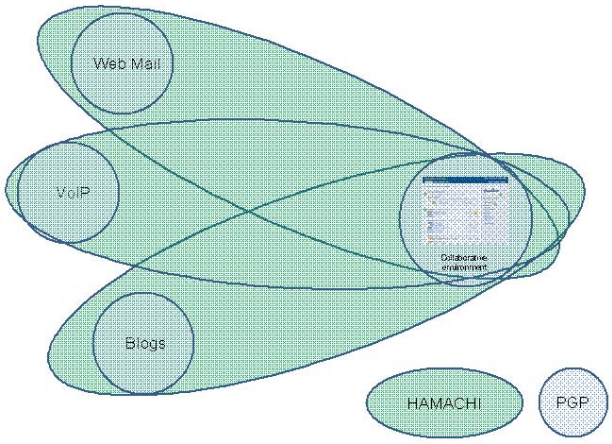

Figure 4 - Proposed Collaborative Architecture

The collaborative environment software would be similar to what is provided by the web 2.0 basecamp[31] application with an added wiki for tracking best practices and other knowledge management needs. Individual communication could either be web mail (Yahoo, MSN, Gmail, etc…) or blog (Google Blogger[32]) based. All security would be provided by PGP[33] for posted documents or Hamachi VPN[34] for communications between one or more individuals within the design team.

Conclusion

The information revolution is here to stay, we must learn to work with it or be condemned to a slower orientation cycle in future complex emergencies. Open source

techniques are already being used to tackle complex problems in business and computing. By accepting a new concept of OPSEC that is all encompassing rather than restrictive at the operational level, the military will be able to institute better collaboration practices across the interagency process. Instead of looking for technological solutions focused on complex communication architecture, we should look at providing simple rules that will guide the planning and coordinating efforts of the various agencies required to solve the problems arising out of future complex emergencies.

Open source warfare planning method will be the great leveller. Anybody who wants to contribute will be able to, as long as they use the basic directing idea in their contributions. In return, an accepted contribution to the process will enhance the value of the planning team and the value of the contributing individual. By keeping the rules simple, actions in the field will be easier to synchronize. In the end, by preserving transparency, we will achieve one of the key elements in the interagency fight – an early acquiescence into the project that will guide everyone's action toward the desired end state rather than simply reacting after the fact in an endeavour similar to herding cats...

---

[1] 1,000,000,000,000 bytes OR 10^{12} bytes; 1 Terabyte: 50000 trees made into paper and printed; 2 Terabytes: An academic research library; 10 Terabytes: The print collections of the U.S. Library of Congress; 400 Terabytes: National Climactic Data Center (NOAA) database – See Peter Lyman and Hal R. Varian, "How Much Information", 2000. <http://www2.sims.berkeley.edu/research/projects/how-much-info/summary.html> (27 April 2008).

[2] Andy Green, Countering Common Adversary Weapons. Presentation at the Unrestricted Warfare Symposium, 15 March 2006, slide number 8 of 12. Interestingly, the terminal effects of an IED developed and controlled using open source warfare are sensibly the same as what can be achieved by a 500 lbs bomb delivered by an F-18 (Cost = $24 million (without cost of maintenance, pilot training, deployment costs, etc…)), but at a much lower cost (cost of an IED from $0 (if recuperated UXO) to a few thousand dollars).

[3] See John Robb, Brave New War (Hoboken: John Wiley & Sins, 2007). The book expands on this concept from the point of view of potential opposing forces.

[4] Adapted from Australian Army, Future Land Operational Concept Complex Warfighting (DRAFT Version 1.3 Correct as at 1 Aug 03), 6.

[5] See USMC School of Advanced Warfighting, Course Card 7195 – Operational Design (Quantico : MCU, AY 2006-07), 12-27.

[6] Thomas L Freedman, The World is Flat (New York: Farrar, Straus and Giroux, 2008), 96-97 and 113-116.

[7] As discussed during the AY 07-08 USMC School of Advanced Warfighting EX PACIFIC CHALLENGE.

[8] Based on actual operations. Ironically because of current OPSEC rules, the actual details must remain sketchy.

[9] Joint Chief of Staff. Joint Publication 3-13.3 – Operations Security (29 June 2006), GL-4: "A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation".

[10] For examples of distributed attack see: Distributed password recovery (Elcomsoft. Distributed Password Recovery Page. <http://www.elcomsoft.com/edpr.html> (27 April 2008)); Search for extra terrestrial life SETI project (SETI. Home Page. <http://setiathome.ssl.berkeley.edu/> (27 April 2008)), or any IED campaigns against U.S./Coalition lines of communication in Iraq or Afghanistan.

[11] John Whisenhunt, "Exploring Second Life. Interview with Cory Ondrejka," IO Sphere Fall (2007), 28.

[12] See Mark Cuban, Weblog. <http://www.blogmaverick.com/> (27 April 2008).

[13] See Clive Thompson, "The See-Through CEO." Wired Magazine. March 2007, <http://www.wired.com/wired/archive/15.04/wired40_ceo.html> (27 April 2008).

[14] The original version would always be available and any changes could be tracked by looking at the version history.

[15] Pretty Good Privacy is a computer program that provides fairly high levels of cryptographic privacy and authentication. It was originally created by Philip Zimmermann in 1991. See PGP Corporation. Home Page. <http://www.pgp.com/> (27 April 2008) for more details.

[16] See Eric S. Raymond, The Cathedral & The Bazaar (Cambridge: O'Reilly, 2001), 19 to 63. The complete list of applicable rules is: Every good work of software starts by scratching a developer's personal itch; Good programmers know what to write. Great ones know what to rewrite (and reuse); Plan to throw away; you will, anyhow; If you have the right attitude, interesting problem will find you; When you lose interest in a program, your last duty to it is to hand it off to a competent successor; Treating your user as co-developers is your least-hassle route to rapid code improvement and effective debugging; Release early and often. And listen to your customers. Try new forms of attacks against different types of targets early and often. Don't wait for a perfect plan; Given a large enough pool of co-developers, any difficult problem will be seen as obvious by someone, and solved. Eventually some participant of the bazaar will find a way to disrupt a particularly difficult target. All you need to do is copy the process they used; Smart date structures and dumb code works a lot better than the other way around; Your co-developers (beta-testers) are your most valuable resource; The next best thing to having good ideas is recognizing good idea from your users. Sometimes the latter is better. Recognize good ideas from your co-developers. Simple attacks that have immediate and far-reaching impact should be adopted; Often, the most striking and innovative solutions come from realizing that your concept of the problem was wrong; Perfection is achieved when there is nothing left to take away (simplicity). The easier the attack is, the more easily it will be adopted. Complexity prevents swarming that both amplifies and protects; Any tool should be useful in the expected way, but a truly great tool lends itself to uses you never expected; To solve an interesting problem, start by finding a problem that is interesting to you; Provided the development coordinator has a communications medium at least as good as the internet, and knows how to lead without coercion, many heads are inevitably better than one.

[17] Marine Corps Planning Process, Military Decision Making Process, Joint Planning and Execution System, Operational Planning Process.

[18] "The Delphi method is a systematic interactive forecasting method for obtaining forecasts from a panel of independent experts. The carefully selected experts answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgments. Thus, participants are encouraged to revise their earlier answers in light of the replies of other members of the group. It is believed that during this process the range of the answers will decrease and the group will converge towards the "correct" answer. Finally, the process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results." See Norman Crolee Dalkey, The Delphi Method: An Experimental Study of Group Opinion (Santa Monica: RAND, 1969) for more details and explanations.

[19] Raymond, 24.

[20] Raymond, 27 and 29-30.

[21] Raymond, 40.

[22] Raymond, 44.

[23] Raymond, 54

[24] Sean Edwards, Military History of Swarming (National Ground Intelligence Center, January 2003), presentation slide #3.

[25] Edwards, Military History of Swarming , presentation slide #4

[26] Gerry Smedinghoff, "The Art, Philosophy and Science of Data," Contingencies May/June (2007): 40. For full treatment on this subject see: James Surowiecki, The Wisdom of Crowds, (New York: Anchor Books, 2005).

[27] Ibid.

[28] Ibid.

[29] Based on the concept of feedback as used by internet business sites such as e-bay (see eBay. Feedback Forum. <http://pages.ebay.com/services/forum/feedback.html> (27 April 2008) for an example of feedback system)

[30] As a matter of fact it cannot be held against the original author because of the evolutionary design process

[31] See Basecamp. Home Page. <http://www.basecamphq.com/index> (27 April 2008).

[32] See Google Blogger development team. Home Page. <https://www.blogger.com/start?hl=en> (27 April 2008).

[33] See PGP Corporation. Home Page. <http://www.pgp.com/> (27 April 2008).

[34] See LogMeIn Inc. Home Page. <https://secure.logmein.com/products/hamachi/vpn.asp?lang=en> (27 April 2008).

Bibliography

Books and Articles

Anderson, Chris. Long Tail, The: Why The Future Of Business Is Selling Less Of More. New York: Hyperion, 2006.

Arquilla, John, David Ronfeldt. Swarming and the Future of Conflict. Santa Monica: RAND, 2000.

Barabasi, Albert-Laszlo. Linked. New York: Plume, 2003.

Dalkey, Norman Crolee. The Delphi Method: An Experimental Study of Group Opinion. Santa Monica: RAND, 1969.

Edwards Sean. Military History of Swarming. National Ground Intelligence Center, January 2003.

Edwards, Sean. Swarming and the Future of Warfare. Santa Monica: RAND, 2005.

Edwards Sean. Swarming on the Battlefield: Past, Present, and Future. Santa Monica: RAND, 2000.

Freedman, Thomas L. The World is Flat. New York: Farrar, Straus and Giroux, 2008.

Green, Andy. Countering Common Adversary Weapons. Presentation at the Unrestricted Warfare Symposium, 15 March 2006.

Raymond, Eric S. The Cathedral & The Bazaar. Cambridge: O'Reilly, 2001.

Rheingold, Howard. Smart Mobs: The Next Social Revolution. Cambridge: Basic Books, 2002.

Robb, John. Brave New War. Hoboken: John Wiley & Sins, 2007.

Smedinghoff, Gerry. "The Art, Philosophy and Science of Data," Contingencies May/June (2007): 36-42.

Surowiecki, James. The Wisdom of Crowds. New York: Anchor Books, 2005.

Whisenhunt, John. "Exploring Second Life. Interview with Cory Ondrejka," IO Sphere Fall (2007): 25-30.

Official Publications

Australian Army. Future Land Operational Concept Complex Warfighting. DRAFT Version 1.3 Correct as at 1 Aug 03.

Joint Chief of Staff. Joint Publication 3-13.3 – Operations Security. 29 June 2006.

USMC School of Advanced Warfighting. Course Card 7195 – Operational Design. Quantico : MCU, AY 2006-07.

USMC School of Advanced Warfighting. MSTP exercise (EX PACIFIC CHALLENGE). Quantico : MCU, AY 07-08

Websites

Anderson, Chris. Weblog. <http://www.longtail.com/the_long_tail/> (27 April 2008).

Basecamp. Home Page. <http://www.basecamphq.com/index> (27 April 2008).

Cuban, Mark. Weblog. <http://www.blogmaverick.com/> (27 April 2008).

eBay. Feedback Forum. <http://pages.ebay.com/services/forum/feedback.html> (27 April 2008).

Elcomsoft. Distributed Password Recovery Page. <http://www.elcomsoft.com/edpr.html> (27 April 2008).

Google Blogger development team. Home Page. <https://www.blogger.com/start?hl=en> (27 April 2008).

LogMeIn Inc. Home Page. <https://secure.logmein.com/products/hamachi/vpn.asp?lang=en> (27 April 2008).

Lyman, Peter and Hal R. Varian, "How Much Information", 2000. <http://www2.sims.berkeley.edu/research/projects/how-much-info/summary.html> (27 April 2008).

PGP Corporation. Home Page. <http://www.pgp.com/> (27 April 2008).

Robb, John. Weblog. <http://globalguerrillas.typepad.com/globalguerrillas/> (27 April 2008).

SETI. Home Page. <http://setiathome.ssl.berkeley.edu/> (27 April 2008).

Thompson, Clive. "The See-Through CEO." Wired Magazine. March 2007, <http://www.wired.com/wired/archive/15.04/wired40_ceo.html> (27 April 2008).