A User Driven Strategy to Recover the Web
Presentation at the OSCE Experts Meeting, 16 November 2007
Johnny Ryan, Senior Researcher, Institute of International and European Affairs (www.iiea.com)

I should like at the outset to recognise and acknowledge the very valuable work done by the OSCE in this area. The OSCE was the first organisation to recognise the importance of radicalisation and recruitment on the Internet. It did this at Ministerial Council level in December 2004, and the EU followed its example some considerable time afterward. Also, at their experts meeting in Spring 2006 in Barcelona, the OSCE continued its labours and produced illuminating insights into the role of public-private partnerships in dealing with the problem of violent radicalisation. The question of public-private partnerships is what this panel will speak about today.

The problem we face is at the nexus of two key trends: the democratisation of communications driven by user generated content on the Internet; and the democratisation of strategic violence driven by mass-casualty non-state terrorism. The question is how can we capitalise on the first trend to counter the second?

In this presentation I will propose "a user driven strategy to recover the web", which places the internet user rather than government at the forefront. This strategy has three participants: i) Governments, ii) what I term "enabling stakeholders" across society, and iii) internet end users.

I shall divide my remarks into two parts. First I will discuss why a user driven strategy is required. Then I will turn to how it could be implemented.

WHY: Why OSCE members should pursue a user driven strategy

In the last two to three years, a profound change has occurred on the Internet. There are two aspects to this change. The first might be described as part of the evolution of "Web 2.0", but what I refer to here as the "user driven revolution". In February 2007, PiperJaffray, a well respected investment consultancy specialising in communications, issued an important report that noted that a shift had occurred in online communications. Internet users in the general public were no longer behaving as passive consumers of content, but were increasingly contributing to and creating their own content.

In the United States last year, the number of internet subscribers grew by 2 per cent. However, the number of people in the United States using websites dependent on user generated content (such as Bebo, MySpace, YouTube, Wikipedia, Flickr, and Facebook) grew 100%. What this indicated is that in an Internet saturated country, all growth arises from users wishing to view content generated by their peers, rather than by specialists in advertising agencies or delivered vertically, top-down, from an authority or government. Internet users are increasingly communicating horizontally, among each other at peer level. This change has empowered militants, and reduced government's ability to directly control communications on the Internet.

This is nothing less than a communications revolution, and might be no less significant than the deregulation of the printing presses in the aftermath of the French Revolution. As Audrey Kurth Cronin noted, this enabled the mass indoctrination of the whole French nation, and resulted in the "levée en masse" of Napoleonic armies that dwarfed their predecessors.

The second aspect is what Joe Nye referred to some years ago as the "paradox of plenty". What that means is that Internet users, with an unprecedented amount of information available to them, find it increasingly difficult to choose what information to view. For the information provider, this increases the need to compete for credibility.

These two aspects have turned the norms of communication, marketing, business, and innovation upon their heads. The result is that individual internet users are now the designers, editors, and contributors of content on the internet, and that they trust their peers' opinions about what content merits attention. Clearly governments cannot take the lead role in countering the militant call to violence in such an environment. Governments lack the credibility, the technical wherewithal, and in many cases the legal credibility to do so.

Regulation?

Despite the emerging realisation that online communications are increasingly horizontal, among peers, the vertical, top-down-from-government mentality persists. Over the course of this meeting, this has been illustrated by the debate among OSCE members about the need to regulate and control Internet access on the one hand, and the need to preserve open access and free expression on the other. This question goes to the heart of how we as countries deal with this new type of commons in the future.

The global nature of the Internet makes common action to take down websites among OSCE partners technically impossible and legally irrelevant in the absence of a binding international treaty and an attendant consensus on what material should be subject to censorship. Another approach could be to require ISPs to act on governments' behalf and attempt to censor user's access to particular content. This approach would be counterproductive. Of the technical methods currently available, "hybrid URL" filtering, which is currently used in the UK and elsewhere, would be the best of a very poor selection. This method, along with the other types of filtering, is an impractical option for a number of reasons:

1. ISP filtering is very easy to circumvent – and for this reason alone should not be considered;

2. Whether through human or technological error, the system would inevitably block access to legitimate content. This would create very considerable legal problems;
3. Filtering is a blunt instrument and blocks a URL entirely, which means that it is incapable of distinguishing an individual posting on a web forum from the entire web forum itself, which could include tens of thousands of legitimate messages;
4. Although hybrid URL filtering is cheaper than normal URL filtering when deployed on a suitable network, it would certainly increase the cost of internet access;
5. Filtering would introduce complexity to a very simple, robust system, thereby degrading the Internet's reliability;
6. Censorship could alter users behaviour. One of the benefits, whatever the drawbacks, of an open internet in which free users can express themselves without concern for authority, has been an unprecedented wave of bottom-up innovation. Governments should consider their long term economic outlook before they take any action that could have any negative impact on this process;
7. Finally, it is the sad irony of heavy handed measures that - unless entirely effective - they are prone to arousing the response they were intended to repress.

In short, effective censorship is not possible on the Internet, and a failed attempt to censor information will inevitably lend that information a new aura of attraction to young curious internet users. Taking down websites within one jurisdiction is irrelevant on a global internet, and requiring ISPs to filter their customers' access is expensive, porous, legally problematic, and damages the robust simplicity of the internet, and internet users attribute toward it.

<u>HOW: How OSCE members should take action</u>

It is essential to challenge the call to violence at the point of dissemination on the chatrooms and web forums, where government is unable to reach. To do so, ironically, this strategy suggests a local, lo-fi approach to a global communications problem.

A. Enabling stakeholders

An important question is who should the "enabling stakeholders" be? In the EU there a number of examples of governments that are involved in public-private partnership. In the UK the Department of Communities has a "Pathfinder Fund" supports a wide range of local initiatives, and it will be interesting to see which are successful and which are not as this process continues. The UK government also supports the radicalmiddleway.co.uk website, which aims to present a mainstream view of Islam by disseminating the sermons and articles of leading British Islamic scholars. In Germany, from September 2006, the national Islamic conference was initiated with the intention of hosting a national debate about Islam and its place in German society. In the Netherlands there are a number of local level initiatives including a community school that I visited last month where officers of the school intervene and engage in dialogue with young people who they fear are on the path towards radicalisation.

Enabling stakeholders will be different in each country. I do not intend to suggest to any government represented here which enabling stakeholders they should engage with, but from these example, it might seem sensible to suggest that enabling stakeholders should include educators, religious communities, and community organisations across society. I do, however, suggest a set of criteria that might be considered when governments begin to identify potential enabling stakeholders:

i) Enabling stakeholders should be trusted parts of the relevant community. It is essential that they be credible. Therefore, they must reflect opinion on the ground within their communities, even if this means that they may hold opinions that government may disapprove of (while not being illegal).

ii) Where possible and relevant, it might be useful if enabling stakeholders were in a position to offer what are becoming known as "exit routes" from radicalisation.

iii) Enabling stakeholders must be able to work with government in a two way process.

iv) Governments must afford enabling stakeholders within their societies the flexibility necessary to maintain their credibility. It is essential that enabling stakeholders should not appear as mouthpieces of official authority.

In addition, it will be important that governments engage with enabling stakeholders across society, rather than identify a single point of contact with a particular community. In the UK, the Blair Government found itself in difficulty because it had erroneously adopted the Muslim Council of Britain (MCB) as its principle point of contact with British Muslims. This was injurious for both government and for the MCB. Since convicted so-called "home grown" terrorists within Europe have been radicalised in video shops and gyms, it should be obvious that are numerous potential enabling stakeholders at all levels in society.

B. Cultural intelligence

The remaining question, as I reach the conclusion of my presentation, is "what do the enabling stakeholders do?" The role of the enabling stakeholder is to disseminate a counter narrative to militant call to violence among Internet users across society. Internet users can then determine for themselves whether to accept, debate or delete the militant message when they encounter it on the Internet. This counter narrative could be considered a form of cultural intelligence, and would enable internet users to identify the vulnerabilities and fallacies in militant material on the chat rooms and web forums where government cannot reach. This cultural intelligence might include four components:

1. Exploit the argument over what Ayman al-Zawahiri would call "offensive jihad".

It is useful to remember that al Qaeda was not the result of a consensus among the *mujahadeen* who fought the Soviets. Rather, al Qaeda emerged from a fundamental ideological rift between Abdullah Azzam, bin Laden's initial mentor, who believed jihad was only justified when defending land against invasion, and Ayman al-Zawahiri, bin Laden's present mentor, who argued the necessity to attack the distant Western enemy.

2. Challenge religious justifications of violence with counter arguments by credible Islamic scholars.
   Many young European Muslims have very limited religious knowledge and are particularly susceptible to the call to violence when issued with imprimatur of an apparent religious authority.

3. Undercut the fallacious historical narrative that underlies the militant call to violence.
   For example, al-Zawahiri's book Knights beneath the Prophet's banner states that every western leader since Napoleon has been part of a consistent single minded conspiracy to establish Israel and humiliate the Islamic world. Whatever emotions current events may arouse, simplistic historical narratives of century long conspiracies are demonstrably untrue. Improved historical awareness would make internet users less willing to instantaneously accept the simplistic version of "the West versus Islam" that is propounded on the Internet.

4. Finally, as Mr Perl, the Head of ATU, said in his introductory remarks yesterday, it is important to show the effects of terrorism on its victims.
   In the Ireland, our broadcasters are constrained in the level of bloodshed that they can show in the interests of good taste. Yet footage of grievous wounds that would be difficult viewing, prove nonetheless that actions – even if they appear heroic – have consequences.

Conclusion

The entire thrust of this strategy is to raise a question mark in the minds of internet users who might be sympathetic to the militant cause. In an era of user driven communications, where peer debate and peer recommendation governs the digestion of information, raising doubt and second thoughts about the justifications and effects of militant violence is crucial. By avoiding direct government involvement, this strategy avoids adding to the glamour of violence among those who would prefer to reject statements from authority. By opting for an open approach based on dialogue rather than regulation, this strategy leaves the Internet's social, cultural, and economic potential unharmed.

I have presented for your consideration a strategy that

i) puts the Internet user at the forefront;

ii) empowers the Internet user to challenge or reconsider the call to violence on the chatrooms and webforums where government is unable to reach, and which are so central in the Web 2.0 phase of the Internet's development; and

iii) disseminates information from government or through government support to Internet users through trusted enabling stakeholders across society.

It is up to governments to determine who these enabling stakeholders should be.

See http://www.iiea.com/publicationx.php?publication_id=25 for Johnny Ryan, *Countering Militant Islamist Radicalisation on the Internet: a User Driven Strategy to Recover the Web* (HARDBACK, ISBN: 1-874-109-86-9) pp 166.