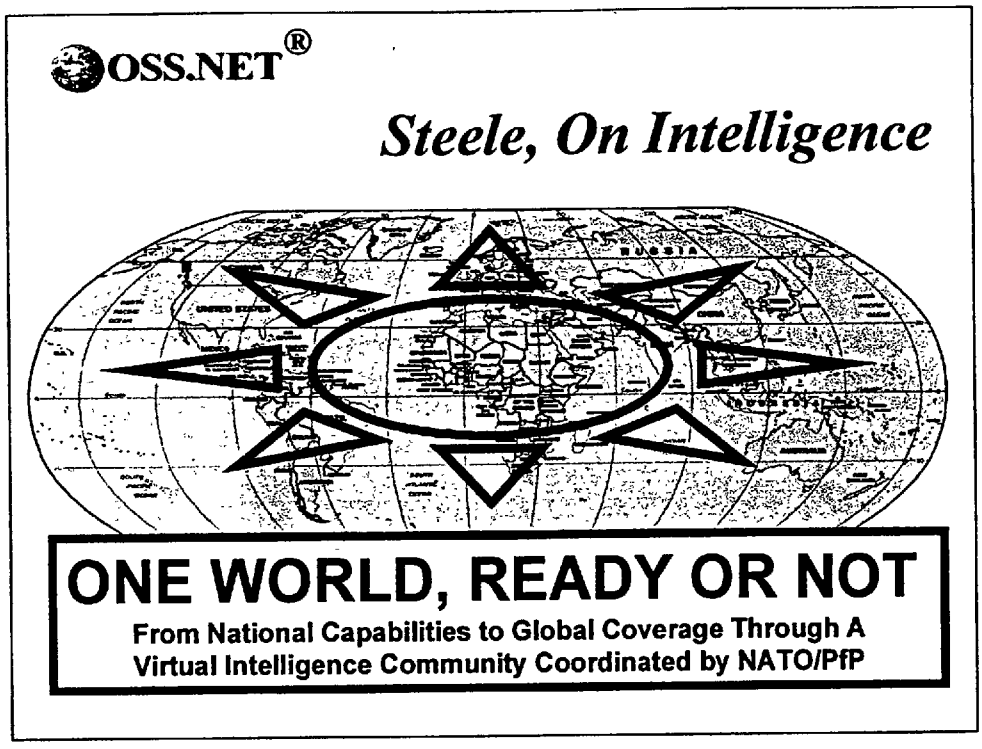


About the Author

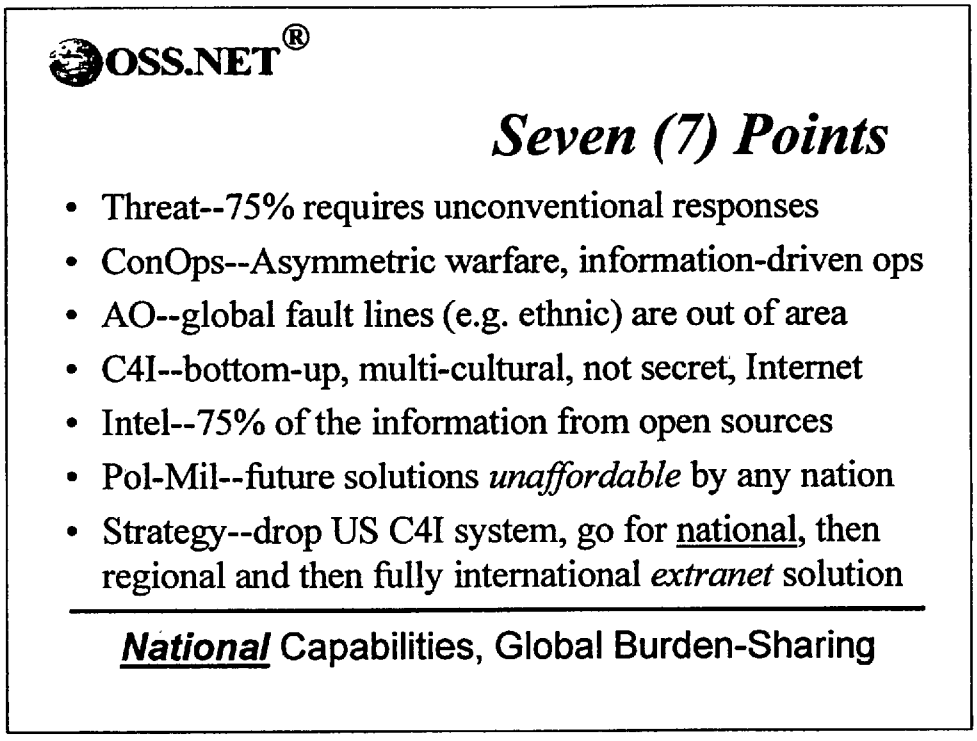
USMC Infantry command & staff

CIA clandestine operations, three back to back tours

Three Washington assignments including offensive counterintelligence for a denied area, programming of overhead satellites for future intelligence requirements, and advanced information technology applications for future intelligence needs.

USMC Intelligence Center--$20M to learn that 90% of what we need for military policy, acquisition, and operational intelligence support is not secret, not available from the US Intelligence Community, and yet is readily available from the private sector--but we lack the knowledge, funding, and doctrine for getting it. Little has changed in the US IC in this respect since 1988.

Focus of my presentation is on the creation of a Virtual Intelligence Community for NATO/PfP that significantly enhances *national* intelligence capabilities while setting the stage for a global burden-sharing and information-sharing *extranet* that no single country can afford by itself.



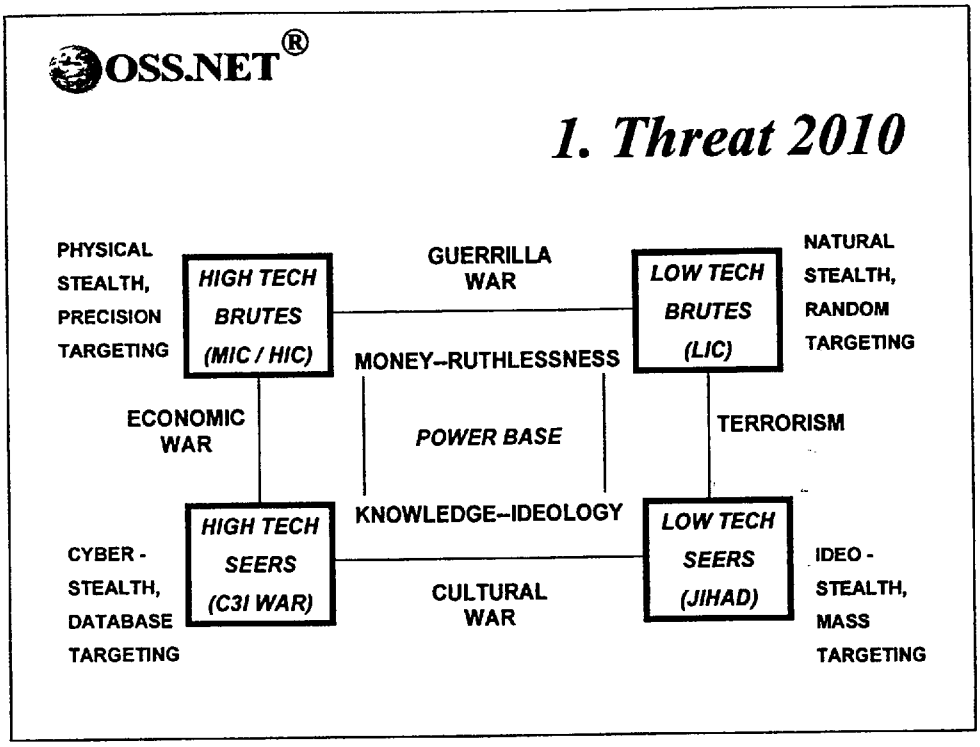
I will address the threat, 75% of which will require unconventional responses--forces that do not exist or are not trained, equipped, and organized for the kind of threat that will confront NATO/PfP in the future.

I will discuss how asymmetric warfare and information-driven operations, the two sides of future war, turn everything we have now on its head. Most of the challenges in the future will be *out of area.*

Then I will focus on the fact that C4I in the 21st Century will be completely different from the C4I architecture we built for the Cold War, and that intelligence will also be completely different, with 75% of our intelligence coming from open sources that we do not understand and exploit today.

Finally, I will end by discussing how the kinds of intelligence we need to be able to use in the future are unaffordable by any single country and unaffordable by NATO/PfP. I will recommend a strategy that disengages from the US C4I system and starts over with an Internet-based *extranet* that allows an infinite variety of players, including non-governmental players, to share information on a just enough, just in time, come as you are basis.

My recommended program will dramatically enhance and expand *national* capabilities while establishing a NATO/PfP "Virtual Intelligence Community" that is able to orchestrate global burden-sharing with respect to both open and closed sources of information.



The high-tech brute is the threat we understand, and it is the threat for which our militaries and their industrial partners build and lobby. I believe we will confront this kind of threat 20% of the time in the future.

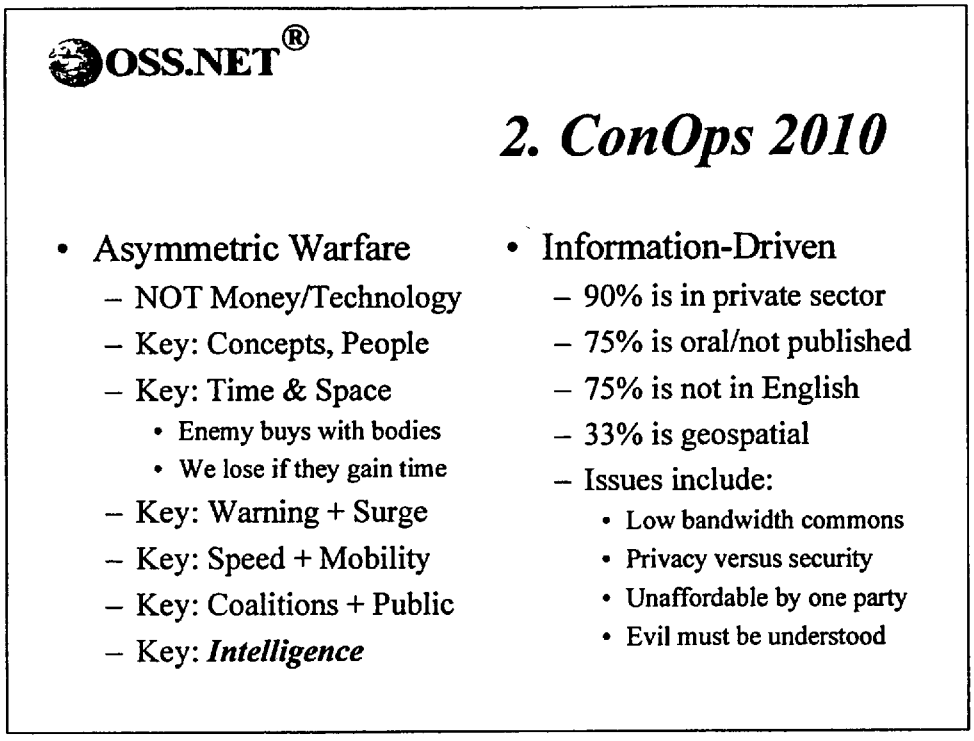
The low tech brutes, the low tech seers, and the high tech seers all merit careful consideration as separate threat categories because only by considering them separately can we understand how desperately unprepared we are for discovering, dissecting, and destroying these threats.

The low tech brute uses natural stealth and random targeting, and is therefore easily able to defeat our cumbersome technically-oriented intelligence community and our fixed defenses.

The low tech seer, masses of people with religious, political, or ideological motivations, is a pervasive and yet distributed kind of threat that requires deep understanding, both in terms of history and in terms of culture. We are not good at this.

Lastly, the high tech seers, a combination of information terrorists and vandals, and practitioners of economic espionage. We'll see more of them.

In short, neither our military capabilities nor our intelligence capabilities are suited for dealing with 75% of the threat forces that will confront us in the future.

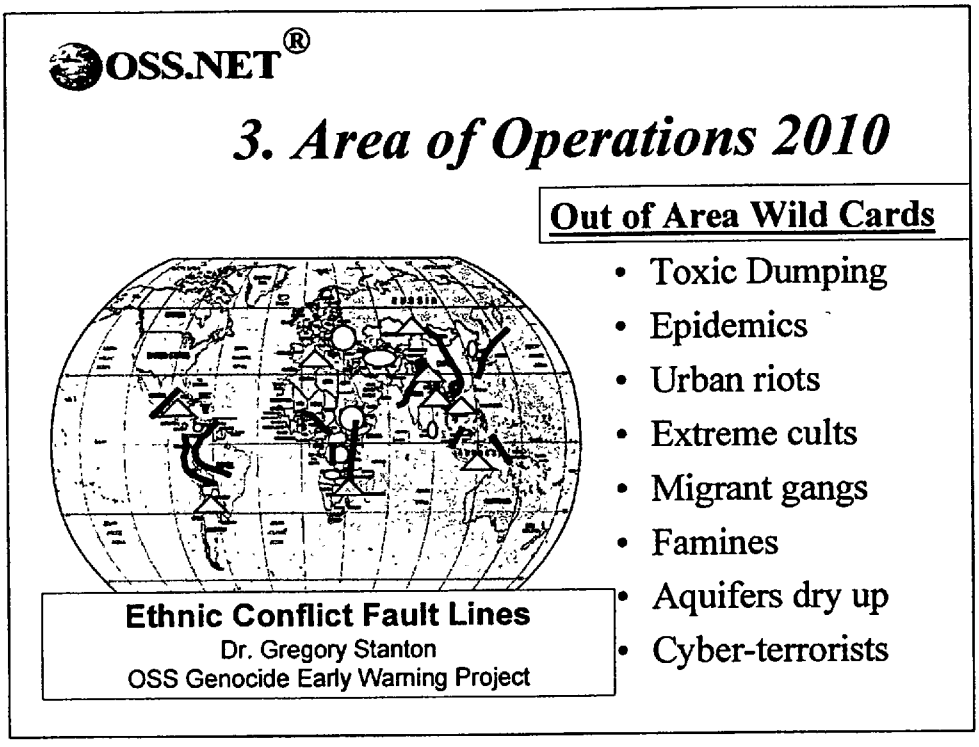


The two sides of future warfare are, on the one hand--the operational side--the asymmetric nature of confrontation, and on the other hand--the information side--the fact that information can and should drive most of what we do.

Asymmetric warfare is not about money or technology. If anything, our reliance on complex technologies places us at a disadvantage. Asymmetric warfare is about being open-minded. It is about having large flexible concepts of operation; about having the very best people who can adjust in real-time to the unforeseen. Above all, it is about time and space; about our ability to obtain warning and to react with forces that are both tailored to the mission and also able to move quickly.

The ability to create coalitions of the moment, to educate the public, and to reach a political consensus is the heart of our effectiveness, rather than the military order of battle. Intelligence will be more important than ever in the 21st Century.

Unfortunately, intelligence as we practice it today is not ready. Our intelligence and information concepts for the future must take into account the fact--the incontestable fact--that 90% of what we need to know to be effective is in the private sector; 75% is not in English, 75% has not been published, and 33% is geospatial information that we are not able to digest with today's systems. And we must be able to do all this at low bandwidth rates with many many different sources, each having a differing level of trust and access.

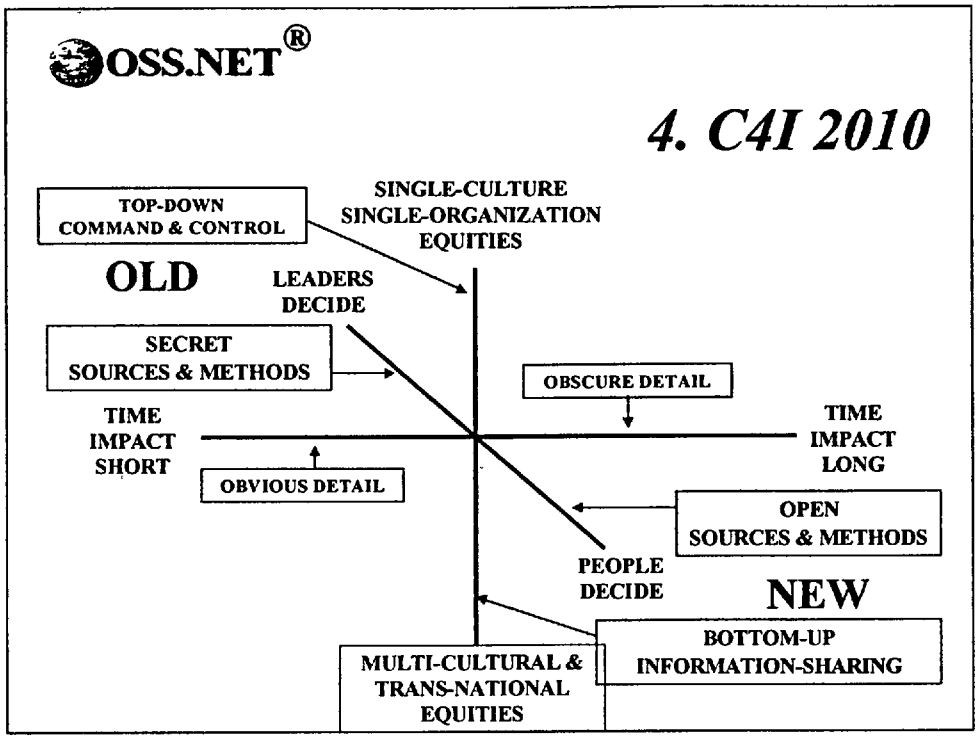


Like it or not, the future of NATO/PfP is an *out of area* future. Unless NATO/PfP becomes a domestic security force, which I consider highly unlikely, or it becomes a domestic disaster relief force, which I also consider highly unlikely but probably a good secondary mission, then one has only to look at the realities of the world to understand that the most serious threats to European stability are *out of area* threats.

I have two analysts who do nothing but monitor genocide and look for warnings of mass atrocities every day. We follow thirty-four (34) different genocidal campaigns every single day. There are in fact hundreds of ethnic fault lines around the world, and here I illustrate only the major ones.

Genocide does two things: it creates forced migrations that are disruptive of nations in its path--a new kind of domino effect--and it creates large piles of rotting bodies from which continental-wide epidemics might emerge.

When we add to this terrible *globally-distributed* threat of ethnic conflict at a mass atrocities scale, the normal wild cards of toxic dumping, epidemics from other causes, urban riots, the influence of cults and gangs, natural famines, the vanishing water supplies in the US as well as the Middle East, and our great vulnerability to anonymous electronic terrorism, you can see that national security in the 21st Century is a much more complex matter than during the Cold War--we must focus on *out of area* population, food, water, energy, and environmental issues, and these may often warrant *intervention.*



Command and control, communications, computing, and intelligence as we know it, the C4I of the Cold War, is an old paradigm.

We cannot afford the American penchant for very expensive complex information technology, nor is the American obsession with system-high security acceptable in this new world where the vast majority of both the knowledge and the influence resides with non-governmental organizations and multi-cultural individuals who insist on using and sharing open sources of information and on getting into all of the details, however obscure.

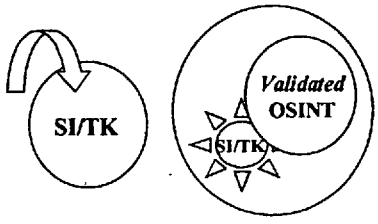
C4I in the 21st Century will turn all of our concepts and doctrine upside down. Instead of leaders deciding, the people will decide, and therefore the people will need the kind of intelligence or decision-support once reserved for Presidents and Prime Ministers and Parliaments. C4I in the 21st Century will place a very high value on historical and contextual and cultural knowledge, and it will be focused on long-term outcomes across national and cultural boundaries.

On balance, secret sources will be of limited value, and open sources will be of much greater value. You need to understand that the Internet permits Secret and Top Secret tunneling today, and will accommodate Codeword tunneling within 3-5 years. On that basis, I am confident in suggesting to you that we need to disengage from the American C4I system and start over on the basis of shifting all communications and computing to an Internet-based *extranet* where anyone and everyone can join in on a "come as you are" basis.

OSS.NET®

5. Intelligence 2010

Competing Models



Selective Importation

System High/Firewall

Just Enough, Just in Time From *All* Sources

Default to Validated OSINT

Burundi Benchmark

Six Phone Calls/Overnight

- Pol-Mil Summaries
- Top Ten Journalists
- Top Ten Academics
- Tribal OOB, History
- Russian Military Maps
- Commercial Imagery

Knowing who knows...

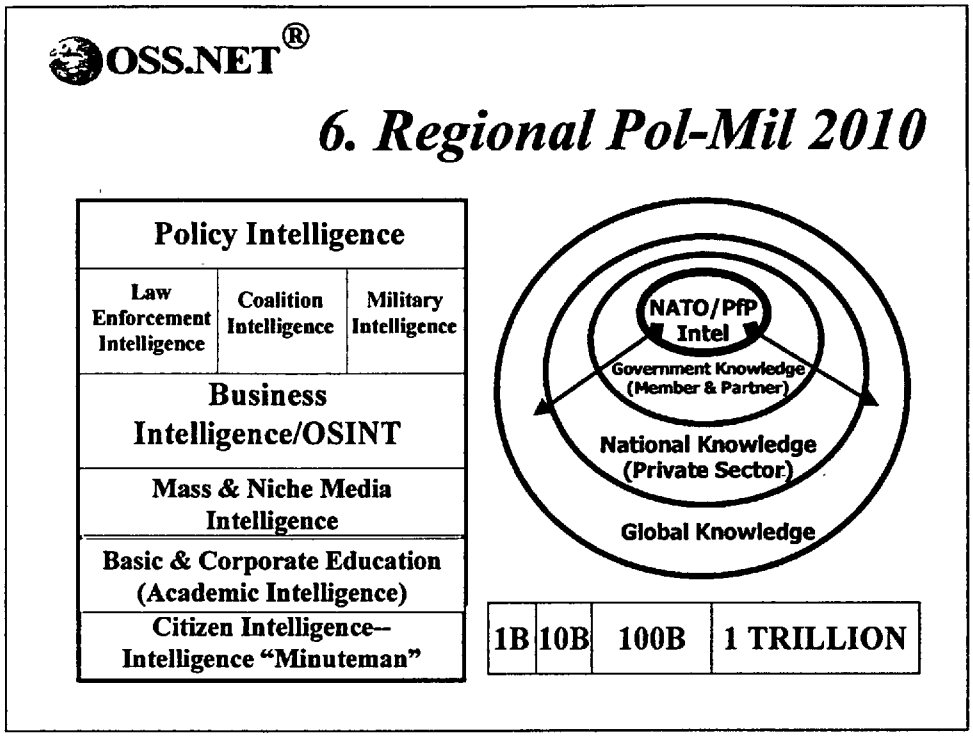
I will spend some extra time on the topic of intelligence, since that is the core competency that we are discussing at this event. I have five separate points I want to make, the first two of which are illustrated here.

First, there are two competing models for integrating open sources of information into the all-source intelligence environment, and you all know that the first model is the one currently being used by the Americans and their allies. It does not work and should be discarded immediately. The second model is vastly superior and is the only model that will support ad hoc coalitions including Partner for Peace operations.

Second, for those of you accustomed to receiving all of your information from classified or formal channels, I want to briefly describe a benchmark exercise in which I made six telephone calls and produced vastly more useful intelligence overnight than was available on such short notice from my $30B a year counterpart, the U.S. Intelligence Community. (Describe Sources). Third, and related to this example, I want to really stress that in my experience both government and corporate bureaucracies are incredibly ignorant of what is available from the private sector. We can come back to that in the Q&A.

Fourth, and as someone who has been a spy, stolen codebooks, programmed imagery satellites, and stood up a national production facility, I can say this with deep knowledge, open sources are extraordinarily valuable to the all source process: open sources can provide History & Context, Warning & Awareness, Key Personalities, Imagery & Maps, Translation Support, Critical Technologies, Alternative Outcomes, Public Relations, and Ground Reconnaissance. I can put boots on the ground with a digital camara and a combat engineering background anywhere in the world within 48 hours of notice, pictures back to you upon arrival.

Fifth and finally, and I have a book on this listed at amazon.com called *ON INTELLIGENCE: Spies and Secrecy in an Open World*, classified intelligence in the 21st Century is going to be about trade-offs: about Less Satellite Collection, Less Technology, Less Spying & Secrecy, More Open Collection, More Processing, More Analysis, More Sharing, Greater Value.



This is the most important slide in my presentation because it illustrates in two different ways my vision for a vastly larger and more effective *national* intelligence community, as well as my vision for how these national intelligence communities can come together to create a global "virtual intelligence community" that brings to bear $1 TRILLION dollars a year in information collection, processing, analysis, and dissemination.

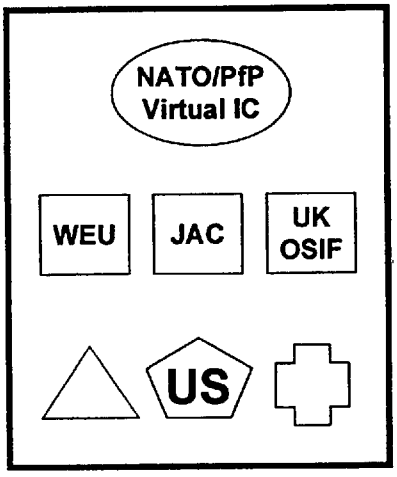
Intelligence in the 21st Century is *unaffordable* by any single military service, government agency, or even any government as a whole. I will go so far as to say that intelligence in the 21st Century is *unaffordable* even by a single nation that is able to fully harness the distributed information resources of its policy, law enforcement, military, business, media, academy, and citizen groups.

Intelligence in the 21st Century is going to be about creating a global *extranet* in which all of these communities can work together across national and cultural boundaries to share--to distribute the cost in dollars and time and knowledge--the burden of collecting, processing, analyzing, and disseminating useful knowledge.

If the national members and national partners of NATO/PfP approach their future intelligence planning, programming, and budgeting in this light, then it will be possible for NATO/PfP to create a very small cadre to help coordinate independent *national* investments into a larger and very robust Virtual Intelligence Community.

OSS.NET®

7. Strategy 2010



- *Extranet*, dump C4I legacy system from US into ocean
- Security spending shifts to 1+iii strategy (*four* forces)
- Environmental and cultural issues are core to security
- Will be *out of area* and out of box more often than not
- Virtual NATO/PfP intelligence *network* and planned burden-sharing

And now my final slide less the list of references.

It is not necessary, and it may well be highly undesirable, for NATO/PfP to have its own intelligence army. Indeed, many nations are finding today that they have too many people doing the wrong things, often duplicating one another's activities.

Instead, I would suggest that NATO/PfP adopt the proven NATO approach of establishing standards and cooperative agreements centered around a commitment to use the Internet--not the US C4I legacy system--as the common carrier for both permanent and *ad hoc* information-sharing arrangements.

Environmental and cultural security issues will be of paramount importance, and therefore non-governmental players will be at least as important, and sometimes more important, than national military players. An extranet approach that is founded on validated open source intelligence as its primary medium of exchange can effectively meet both national and regional needs.

A virtual NATO/PfP *network* would at a minimum want to include the WEU Satellite Centre; the Joint Analysis Center at Molesworth; the UK Open Source Information Centre; a new NGO Liaison Facility; and a new NATO Open Source Intelligence Coordination Centre.

OSS.NET®

References

- " Towards a European intelligence policy" by Alessandro Politi (IT), advisor to the Minister of Defence, Italy and others
- "Open Source Intelligence: The Challenge for NATO" by Commodore (then Captain) Patrick Tyrrell (UK), OBE MA LLB RN
- "Open Source Intelligence: the Lingua Franca for regional intelligence co-ordination and information sharing" by General Director S. J. van Hulst (NL), National Security Service (BVD), The Netherlands
- "Open Source Intelligence: Foundation for Regional Co-operation in Fighting Crime and Establishing a Regional Intelligence Community" by Jurgen Storbeck (GE), Director, EUROPOL
- *Open Source Intelligence: Executive Overview*, OSS Academy
- www.oss.net (5000 pages from 500 authorities, two handbooks, free)
- This brief is at <www.oss.net/Papers/white/SHAPE.ppt>.

Here are a few references. You should all have a booklet with copies of these slides with my text, copies of the four European references listed here, and a copy as well as my 76-page executive overview on open source intelligence for executives.

There is a wealth of material on open sources now available through my web site, and I am indebted to the 40 governments that have supported my work over time, including a number of European and Nordic countries.

It has been my experience that most of you are unaware of what is going on in your own country with respect to open source intelligence initiatives, and I therefore will conclude with one simple suggestion: that you all immediately convene a NATO/PfP Open Source Intelligence Working Group, and that you identify a single field-grade officer who can represent you in dealing with the recently formed CINC OSINT Working Group in the US, and with the NGO OSINT Working Group that I am hoping to see emerge from the UN's Office for the Coordination of Humanitarian Assistance. I will help this group by identifying to them key points of contact within your governments that I know.

This working group, by becoming fully familiar with what is available from the private sector, but from a military and all-source perspective, would be well-suited to helping you think about the European regional intelligence network of the future, and would assure your success by ensuring that you keep an open channel to the private sector, and an open mind about just how we define "intelligence" in the 21st Century.

OSS 21 PRIMER Essential Elements of Information Joint Planning, Operations Other Than War and Open Source Intelligence - Link Page

Previous	An Alternative View On The Future Of Intelligence
Next	Spies and Secrecy in an Open World

Return to Electronic Index Page