Internet-Based Intelligence in Public Health Emergencies
E. Mordini and M. Green (Eds.)
IOS Press, 2013

Foreword

Robert David STEELE
CEO, Earth Intelligence Network

I am delighted to have an opportunity to welcome this book as a contribution to the growing body of work focused on the convergence of new technologies, new human possibilities, and new organizational forms and processes.

When I was asked to speak in 2000 to all of the generals and colonels, each commanding a national military intelligence organization, from across both the North Atlantic Treaty Organization (NATO) and the Partnership for Peace (PfP), I understood that NATO was then at the very beginning of a most difficult learning curve.[1]

NATO was created by governments, and governments are still today Industrial Era collections of bureaucracies accustomed to hoarding information, using secrecy to protect budgets and avoid accountability, and making decisions in isolation from other important but separate domains.

NATO, like the United Nations (UN) and most other international and non-governmental organization, continues to lack an organic intelligence capability. As I use it the word intelligence refers to the proven process of intelligence, which is not secret, and to outcomes in the form of decision-support, rather than inputs in the form of secret sources and methods.

This book, a decade after NATO first published *the Open Source Intelligence Handbook* (2001), the *Open Source Intelligence Reader* (2002), and the guide to *Intelligence Exploitation of the Internet* (2002), represents the beginning of a new period of innovation among both the traditional NATO elements, the military and diplomatic arms of the Member governments, and the long-ignored but now essential other six information and intelligence communities: academic, civil society, law enforcement, media, and non-governmental or non-profit. Put most directly, 90% or more of the information that NATO and its varied regional coalition partners need, is created, owned, stored, and understood by individuals and organizations with whom NATO has no official relations, no direct means of secure communication, and no concepts or doctrine with which to define needed information, get needed information, and convert needed information into intelligence – decision-support – useful to NATO and the Member governments in predicting and remediating instability.

1. Internet is a Communications Network

Internet-Based Intelligence must be understood as firmly founded on Human Intelligence (HUMINT), while enabling the rapid sharing, both at machine speed and at human speed, of multi-lingual multi-media data sets. The Internet cannot be controlled

[1] *ONE WORLD, READY OR NOT: From National Capabilities to Global Coverage Through a Virtual Intelligence Community Coordinated by NATO/PfP* (NATO, 2000).

by NATO and the Internet is not in and of itself a database to be exploited by NATO. What the Internet represents is a communications network that is open, infinitely agile and scalable, and inclusive – everything that NATO C4I is not.[2]

2. Public Health Represents All Non-Military Target Sets

This book is a very fine first attempt to get a grip on political and legal human issues, data and intelligence technical issues, and the larger strategic and operational issues of how NATO might approach Operations Other Than War (OOTW), or in the more recent parlance, Stabilization & Reconstruction (S&R) Operations.

Infectious Disease is high-level threat number two according to the United Nations High-Level Panel on Threats, Challenge, and Change.[3] Setting aside the four "military" threat domains that NATO already understands (Inter-State Conflict, Civil War, Proliferation, and Terrorism), this leaves us with five other unconventional non-military threats that join Infectious Disease to challenge NATO: Poverty, Environmental Degradation, Genocide, Other Atrocities, and Transnational Crime.

To address these six non-military threat areas, NATO and its Members must enter the third era of national intelligence, the era of the Smart Nation.

In this light, it is with admiration that I note the recent words of NATO Supreme Commander Admiral James Stavridis, who has called for "open-source security," and observed most wisely that the West is not going to achieve stability only through the barrel of a gun or by building walls. He has also noted the value of reaching out to people through social networks and providing services such as teaching….[4]

3. One World, Ready or Not

It will be difficult for the military and government officers who comprise the bulk of the NATO establishment to accept several facts about this new Internet-based multinational, multiagency information-sharing and sense-making environment.[5]

First, it cannot be commanded nor controlled. NATO must position itself to be the welcome recipient of information and intelligence created by others; information and intelligence that is neither secret nor expensive, but that must be volunteered by the originator.

Second, it will be multilingual in nature, and no amount of money or technical processing will be able to ingest and make-sense of all that can be known. The human factor is vastly more important in peace operations than in war operations. Not only will the timeliness, relevance, and connectedness of all needed information depend on specific human actors distributed across the eight information/intelligence communities, but so also will NATO be heavily dependent on "crowd-sourcing" such

---

[2] C4I: Command and control, communications, computers, and intelligence.

[3] High-Level Panel, *A More Secure World: Our Shared Responsibility* (New York, NY: United Nations, 2004).

[4] As cited by Richard Gannett, "What if you could make anything you wanted?," CNN.com, Mon July 9, 2012, accessed 9 July 2012. The Admiral's TED presentation in June 2012, "Open Source Security," is online as "James Stavridis: How NATO's Supreme Commander thinks about global security."

[5] My last book, *INTELLIGENCE for EARTH: Clarity, Diversity, Integrity, & Sustainability* (Oakton, VA: Earth Intelligence Network, 2010), provides my fully-developed views.

as found with the offerings of the International Crisis Mapping community that is able to organize – using volunteers – all tweets and Simple Message System (SMS) texts across the global diaspora – and also to visualize, with near-real-time translation, those texts on an open online map.

Third, NATO will find, as the US Central Command (CENTCOM) has learned, that classified information systems are not agile, do not scale, and are largely useless in OOTW or S&R Operations. NATO must adopt Open Source Technologies – not just open source software and open source hardware, but Open Base Transceiver Station (OpenBTS), Open Spectrum, and Open Standards. This will be culturally difficult for NATO, and will take over a decade. Integral to this change will be the realization by NATO that it and its Member governments must move as quickly as possible to Open Source Everything,[6] empowering the public with Internet-Based means of creating and sharing information, such that NATO can ride the wave of public intelligence.

Fourth and finally, NATO will find that the secret intelligence communities as well as the traditional policy communities are severely handicapped with respect to modern understanding. Governments are not good at appreciating ethnic minorities outside the nation-state context – witness how the USA and NATO failed to understand the implications for Mali of destroying stability in Libya: they have created a new haven for terrorism.

4. Riding the Wave – Leadership in the Open Era

If NATO desires to be effective in the 21st Century, it will have to transform its culture, its mind-set, and its methods to master what I have long called Information Peacekeeping (the avoidance of war through intelligence applied with integrity) and Peacekeeping Intelligence (the rapid stabilization of a violent environment through force of arms guided by intelligence applied with integrity). I personally believe that NATO could not only succeed at this endeavor, but could also be a model for the UN, which lacks both intelligence and integrity across all the Specialized Agencies (SA) as well as the central elements based in New York and Geneva. I am quite certain that if NATO does not adapt to the modern possibilities, that Brazil, China, India, Indonesia, Russia, Turkey, Venezuela and other demographic and cultural giants will create the default Internet and the default public information system of the 21st Century.

We all need a global public intelligence network that is rooted in an Autonomous Internet that cannot be shut down by any government or corporation, and that enables the public to have full and open access to budgets, facts, and systemic knowledge (if A then B). Such a network cannot be, will not be, controlled by NATO, but NATO will be helpless without such a network.

In war and peace in this century, "true cost" facts are the new bullets and the new gold. In the USA it has been established that 47% of all food is thrown away and 50% of every health dollar is fraud, waste, or abuse. At the same time, the U.S. Government has been deliberately releasing to the public false information about the health hazards of Fukushima and key economic statistics, while also concealing the monstrous health conditions suffered by the citizens of Iraq from depleted uranium, and by our veterans, 18 of them committing suicide each day of each year. The truth is the lever with which

---

[6] See my latest book, *THE OPEN SOURCE EVERYTHING MANIFESTO: Transparency, Truth & Trust* (Berkeley, CA: North Atlantic Books Evolver Editions, 2012)

great forces can be harnessed – however, absent morality, no endeavor is sustainable and no mastery of the truth will suffice.

Below is my favorite health slide, something I devised a few years ago while developing the Strategic Analytic Model for the Earth Intelligence Network, the 501c3 that I created to help move the world to the third stage of intelligence, the era of the Smart Nation.

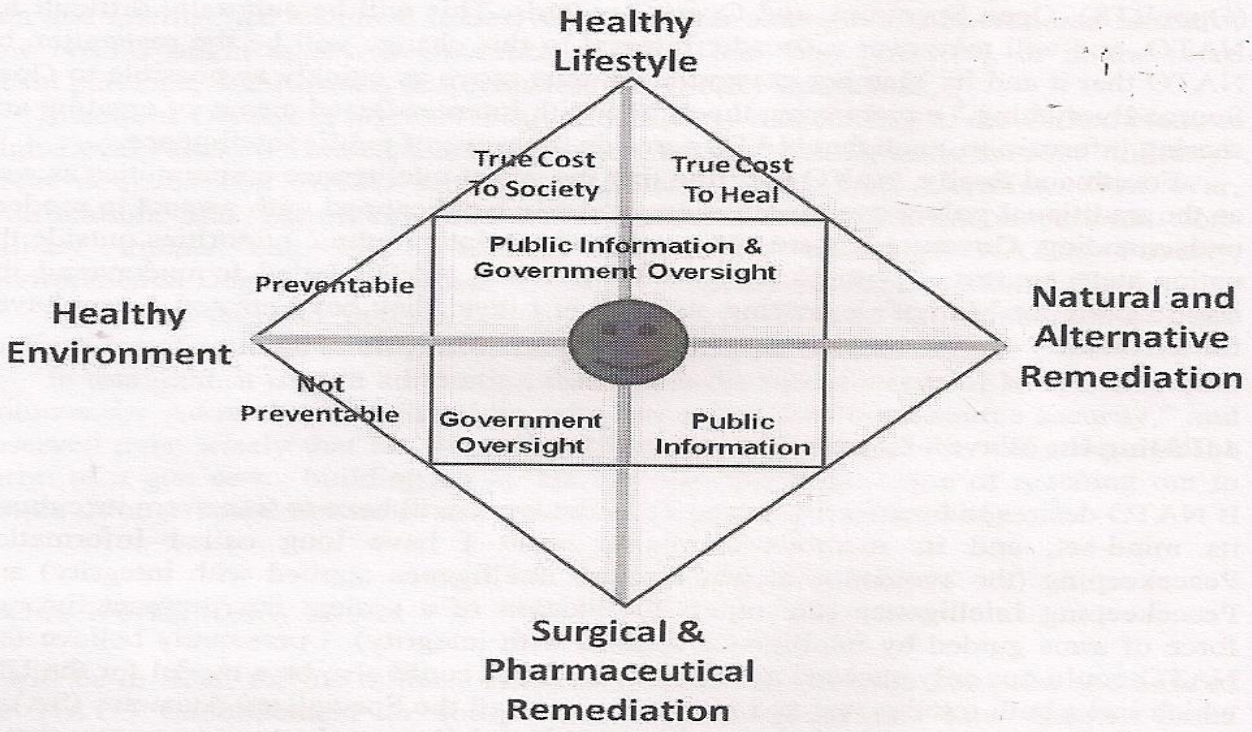

Figure 1. Health Analytics – 360 Degree Perspective.

Western governments have been corrupted by the medical industry that wishes only to focus on the Surgical and Pharmaceutical Remediation aspect of public health, because that is where the private profits are to be found. In fact, we must focus equally on individual lifestyles including the eradication of poverty; on assuring the public of healthy environments free of toxins and other carcinogens; and on alternative and natural cures. Health is an intelligence challenge. Absent a holistic analytic model, absent an appreciation for all eight information/intelligence communities, absent a commitment to "true cost" discovery, it will not be possible for NATO to adapt and excel in the 21st Century.

With that as an introduction, on the next two pages I present four graphics that could be useful in guiding NATO, the UN, and all Member states in developing what Col Jan-Inge Svensson (SE Land Forces Ret) and I call M4IS2: Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing and Sense-Making This is what lies beyond Open Source Intelligence (OSINT).

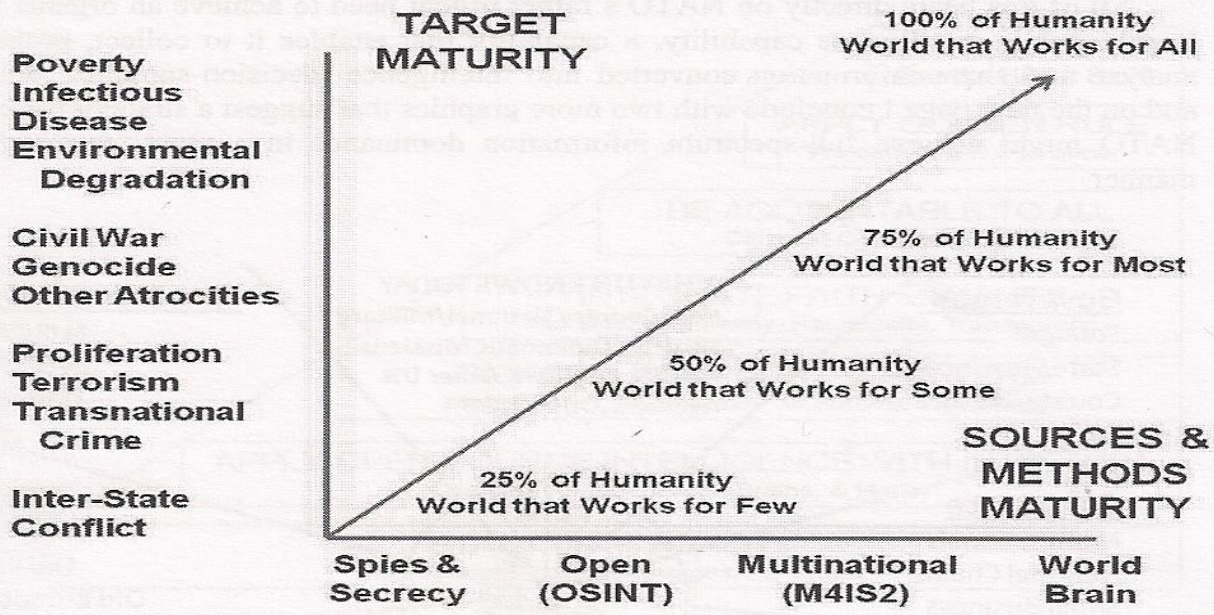

Figure 2. Understanding Modern Threats This is my newest graphic.[7] It was inspired by the United Nations.[8] For the first time in modern history, the nations of the world have agreed on both what comprise the top ten threats to humanity – and their priority order. The horizontal axis represents my work these past thirty years

Figure 3. Holistic Analytic Model Here I illuminate the strategic analytic model of Earth Intelligence Network, the non-profit that I founded in 2006 to develop new concepts and processes for achieving public intelligence. Please note both the centrality of Health as key policy number seven, and the need to address all twelve policies at once. The "health of nations" is itself a holistic analytic challenge.

---

[7] Forthcoming in "The New Craft of Intelligence," R.Dover, M. Goodman, and C. Hillebrand (eds.). *Routledge Companion to Intelligence Studies* (Routledge, February 2013).

[8] *Supra* note 3.

All of this bears directly on NATO's rather urgent need to achieve an organic but largely public intelligence capability, a capability that enables it to collect, process, analyze and share information converted into intelligence (decision-support). Below and on the next page I conclude with two more graphics that suggest a strategy for how NATO might achieve full-spectrum information dominance in a most constructive manner.

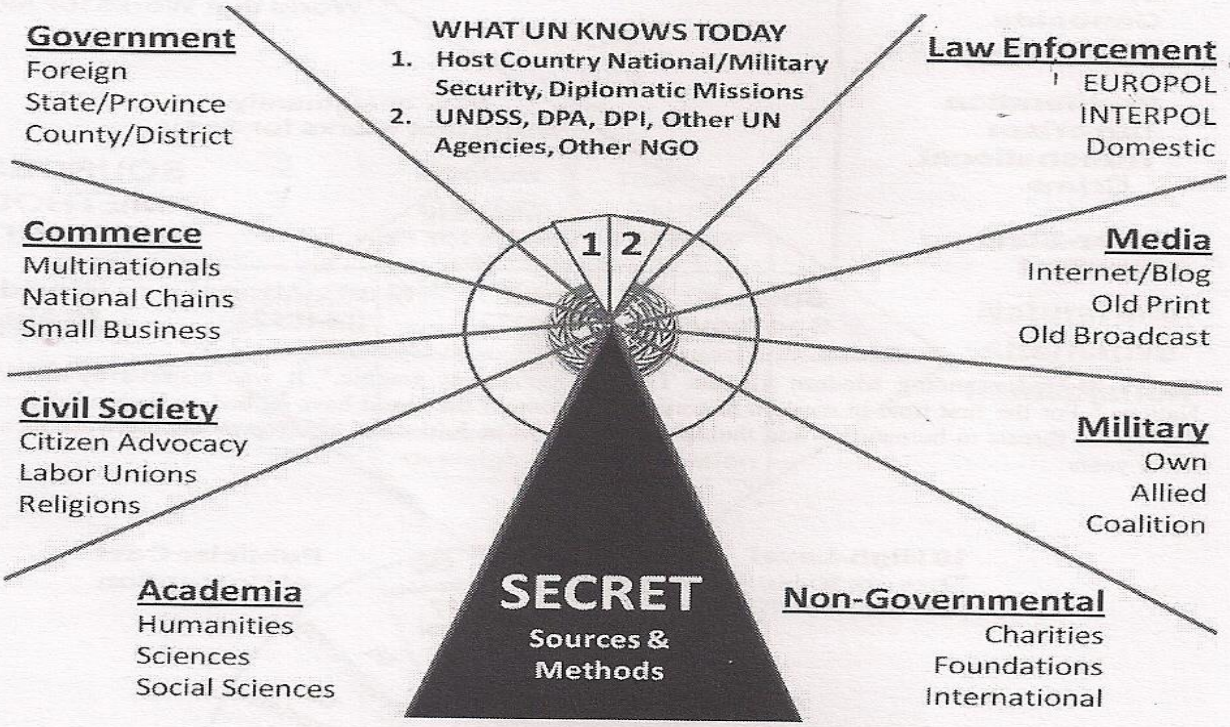

Figure 3. Achieving Access to All Information.

I developed this graphic while trying to help the UN develop a legal and ethical intelligence capability. It also appears in my last book.[9] Until and unless NATO develops an M4IS2 capability that fully embraces the other seven "tribes" of information and intelligence, NATO will be a dinosaur groping in uninformed darkness, and hence ineffective

[9] *Supra* note 5.

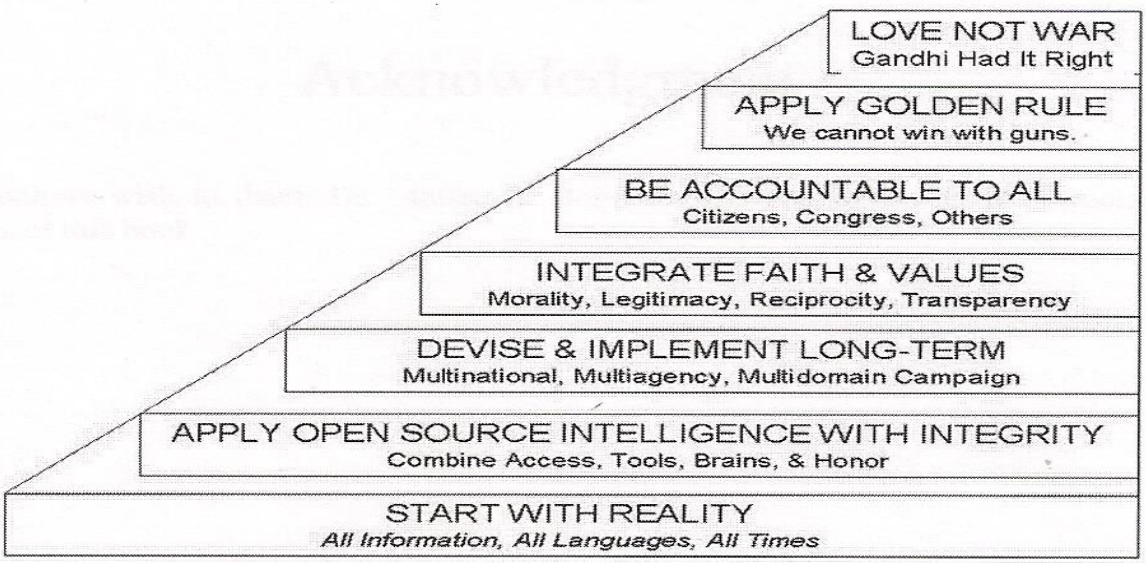

Figure 4. From Truth, Peace.

NATO is in the process of transforming itself from an Industrial Era network that orchestrates "heavy metal militaries" to a modern network that uses shared information to harmonize understanding as well as spending and behavior – to do Information Peacekeeping or Peace-keeping Intelligence.[10]

This first book is a very fine start toward the objective of making NATO a network of Smart Nations able to use Information Operations (IO) as a substitute for violence, as a means of creating a prosperous world at peace. This will require a considerable change in the NATO culture and the NATO mind-set. I helped inspire a partial change in 2000; this book and the recent statements of Admiral James Stavridis suggest that change is indeed occurring.

[10] Definitions and related references are online at "Robert Steele Answers PhD Questions," *Phi Beta Iota the Public Intelligence Blog*, 16 July 2012.