6

OPEN SOURCE INTELLIGENCE

ROBERT DAVID STEELE

OPEN SOURCE INTELLIGENCE (OSINT) IS THE ONLY discipline that is both a necessary foundation for effective classified intelligence collection and analysis and a full multimedia discipline in its own right, combining overt human intelligence from open sources, commercial imagery, foreign broadcast monitoring, and numerous other direct and localized information sources and methods not now properly exploited by the secret intelligence community. OSINT is uniquely important to the development of strategic intelligence not only for the government, but for the military, law enforcement, business, academia, nongovernmental organizations, the media, and civil societies including citizen advocacy groups, labor unions, and religions for the simple reason that its reliance on strictly legal and open sources and methods allows OSINT to be shared with anyone anywhere, and helps create broader communities of interest through structured information sharing.

It can be said that at the strategic level in particular, but at all four levels of analysis (strategic, operational, tactical, and technical) generally, the secret intelligence communities of the world are inside-out and upside-down. They are inside-out because they persist in trying to answer important questions with unilaterally collected secrets, rather than beginning with what they can learn from the outside-in: from the seven tribes[1] and the more than ninety nations that form the coalition. They are upside-down, at least in the case of the United States and selected other major powers, because they rely too much on expensive overhead satellite systems instead of bottom-up ground truth networks of humans with deep historical, cultural, and localized knowledge.

In the long-run, I anticipate that OSINT will displace 80 percent of the current manpower and dollars devoted to secret sources and methods, and that

Robert David Steele, "Open Source Intelligence," in Loch Johnson (ed), *Strategic Intelligence: The Intelligence Cycle* (Westport, CT: Praeger, 2007), Chapter 6 pp. 96-122

this will offer the taxpayers of the respective nations a return on investment at least one thousand times better than what is obtained now through secret sources and methods. A proper focus on OSINT will alter the definition of "national" intelligence to embrace all that can be known from the seven tribes across both the home nation and the coalition nations, and will dramatically reform intelligence, electoral processes, governance, and the application of the national, state, and local budgets in support of the public interest.

Strategically, OSINT will restore informed engaged democracy and moral capitalism, a new form of communal capitalism, in America and around the world. OSINT is, at root, the foundation for the emergence of the world brain, and the empowerment of the public.

The bulk of this chapter will focus on OSINT and intelligence reform at the strategic level, but it is essential that the reader appreciate the implications of OSINT for electoral, governance, and budgetary reform so as to better realize the enormous implications of the revolution in intelligence affairs[2] for which OSINT is the catalyst.

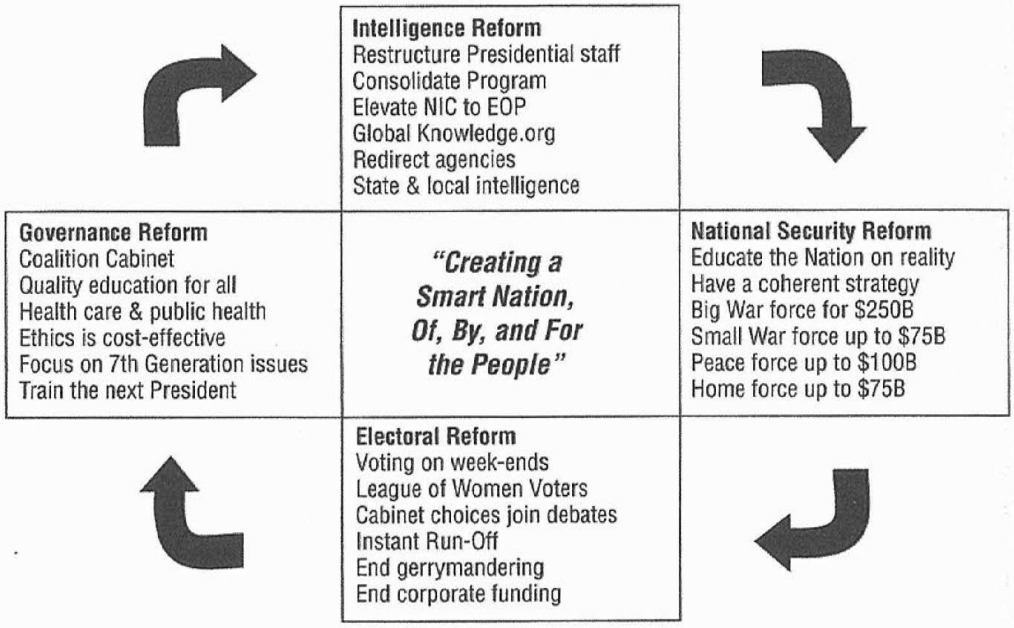

Figure 6-1. Four Strategic Domains for Reform Catalyzed by OSINT

Note: NIC = National Intelligence Council; EOP = Executive Office of the President. It is important to observe that the Global Knowledge organization, now called an Open Source Agency, is intended to be completely independent of both presidential and congressional manipulation. This chart is discussed in more detail in the final section of this chapter on governance reform.

Source: Drawn from "Citizen in Search of a Leader" as prepared 8 January 2003 and posted to http://www.oss.net. Additional detail on each reform domain can be found in that document.

The impetus for reform across all four strategic domains could emerge from within any one of the four. If the economy collapses and the war on Iraq combined with an attack on Iran cause a clear and present danger to emerge in the form of global Islamic counterattacks that are asymmetric and indiscriminate as well as widespread, we can anticipate not just the ejection of the extremist Republicans, but also of the complacent and equally corrupt and ignorant Democrats.[3]

There is a growing awareness within the public, described by some as "smart mobs," or "wisdom of the crowds," or—our preferred term—collective intelligence, that it is now possible for individuals to have better intelligence based on open sources and methods, that is being made available to, or acknowledged by, the president.[4] We will see, within the next four years, a dramatic increase in both historical accountability[5] and current accountability for actions impacting on future generations and other communities.

Electoral reform will be inspired by citizens realizing that both the Republican and Democratic parties have become corrupt as well as inept at representing the public interest.

Governance reform will be inspired by citizens realizing that in today's world, we need a networked model of governance that elevates intelligence to the forefront. Decisions must be made in the public interest and be sustainable by consensus and conformance to reality, not purchased by bribery from special interests who seek to loot the commonwealth and/or abuse their public power to pursue the ideological fantasies of an extremist minority.

Budgetary reform will be inspired by citizens who understand that we still need to be able to defend ourselves, but that waging peace worldwide is a much more cost-effective means of both deterring attacks and of stimulating sustainable indigenous wealth that is inherently stabilizing.

OSINT AND INTELLIGENCE REFORM

Open source intelligence (OSINT) should be, but is not, the foundation for all of the secret collection disciplines, and it could be, but is not, the foundation for a total reformation of both the governmental function of intelligence and the larger concept of national and global intelligence, what some call collective intelligence or the world brain.[6]

Secret intelligence, inclusive of covert action and counterintelligence, has failed in all substantive respects since the end of World War II and through the Cold War. In failing to meet the mandate to inform policy, acquisition, operations, and logistics, secret intelligence has contributed to the "50 Year Wound"[7] and failed to stimulate a redirection of national investments from military capabilities to what General Al Gray, then-Commandant of the Marine Corps, called "peaceful preventive measures."[8]

Secret intelligence became synonymous with clandestine and secret technical collection, with very little funding applied to either sense-making information

technologies, or to deep and distributed human expertise. The end result at the strategic level can be described by the following two observations, the first a quote and the second a recollected paraphrase: Daniel Ellsberg speaking to Henry Kissinger: "The danger is, you'll become like a moron. You'll become incapable of learning from most people in the world, no matter how much experience they have in their particular areas that may be much greater than yours" [because of your blind faith in the value of your narrow and often incorrect secret information].[9] Tony Zinni speaking to a senior national security manager: "80% of what I needed to know as CINCENT I got from open sources rather than classified reporting. And within the remaining 20%, if I knew what to look for, I found another 16%. At the end of it all, classified intelligence provided me, at best, with 4% of my command knowledge."[10]

Secret intelligence may legitimately claim some extraordinary successes, and we do not disagree with Richard Helms when he says that some of those successes more than justified the entire secret intelligence budget, for example, in relation to Soviet military capabilities and our countermeasures.[11] However, in the larger scheme of things, secret intelligence failed to render a strategic value to the nation, in part because it failed to establish a domestic constituency, and could be so easily ignored by Democratic presidents and both ignored and manipulated by Republican presidents.[12]

In this first section, we will briefly review both the failings of each aspect of the secret intelligence world, and summarize how OSINT can improve that specific aspect.

History

The history of secret intelligence may be concisely summarized in relation to three periods:

1. *Secret War.* For centuries intelligence, like war, was seen to be the prerogative of kings and states, and it was used as a form of "war by other means," with spies and counterspies, covert actions, and plausible deniability.[13]

2. *Strategic Analysis.* During and following World War II, Sherman Kent led a movement to emphasize strategic analysis. Despite his appreciation for open sources of information, and academic as well as other experts, the clandestine and covert action elements of the Office of Strategic Services (OSS) and the follow-on Central Intelligence Group (CIG) and then Central Intelligence Agency (CIA), grew out of control, well beyond what President Harry Truman had envisioned when he sponsored the National Security Act of 1947.[14]

3. *Smart Nation.* Since 1988 there has been an emergent movement, not yet successful, but increasingly taking on a life of its own in the private sector. Originally conceptualized as an adjunct to secret intelligence, a corrective focus on open sources long neglected, it was soon joined by the collective intelligence movement that has also been referred to as "smart mobs" or "wisdom of the crowds," or "world brain." H. G. Wells conceptualized a world brain in the

1930s. Quincy Wright conceptualized a world intelligence center in the 1950s. Others have written about smart nations, collective intelligence, global brain, and the seven tribes of intelligence.[15]

Although the U.S. intelligence community has individuals that respect the value of open sources of information, and every major commission since the 1940s has in some form or another called for improved access to foreign language information that is openly available, the reality is that today, in 2006, the United States continues to spend between $50 billion and $70 billion a year on secret collection, almost nothing on all-source sense-making or world-class analysis, and just over $250 million a year on OSINT. This is nothing less than institutionalized lunacy.

The future history of secret intelligence is likely to feature its demise, but only after a citizen's intelligence network is able to apply OSINT to achieve electoral, governance, and budgetary reform, with the result that secret intelligence waste and defense acquisition waste will be converted into "waging peace" with peaceful preventive measures and a massive focus on eliminating poverty, disease, and corruption, while enabling clean water, alternative energy, and collaborative behavior across all cultural boundaries.[16]

Requirements

Requirements, or requirements definition, is the single most important aspect of the all-source intelligence cycle, and the most neglected. Today, and going back into history, policy makers and commanders tend to ignore intelligence, ask the wrong questions, or ask questions in such a way as to prejudice the answers. There are three major problems that must be addressed if we are to improve all-source decision support to all relevant clients for intelligence:

1. *Scope.* We must acknowledge that all levels of all organizations need intelligence. We cannot limit ourselves to "secrets for the president." If we fail to acknowledge the needs of lower-level policy makers, including all Cabinet members and their Assistant Secretaries; all acquisition managers; all operational commanders down to civil affairs and military police units; all logisticians; and all allied coalition elements including nongovernmental organizations, then we are not being professional about applying the proven process of intelligence to the decision-support needs of key individuals responsible for national security and national prosperity.

2. *Competition.* We must acknowledge that open sources of information are vastly more influential in the domestic politics of all nations, and that it is not possible to be effective at defining requirements for secret intelligence decision-support in the absence of a complete grasp of what is impacting on the policy makers, managers, and commanders from the open sources world (see Figure 6-2).

3. *Focus.* Third, and finally, we must acknowledge that, at the strategic level, our focus must of necessity be on long-term threats and opportunities that are global, complex, interrelated, and desperately in need of public education, public

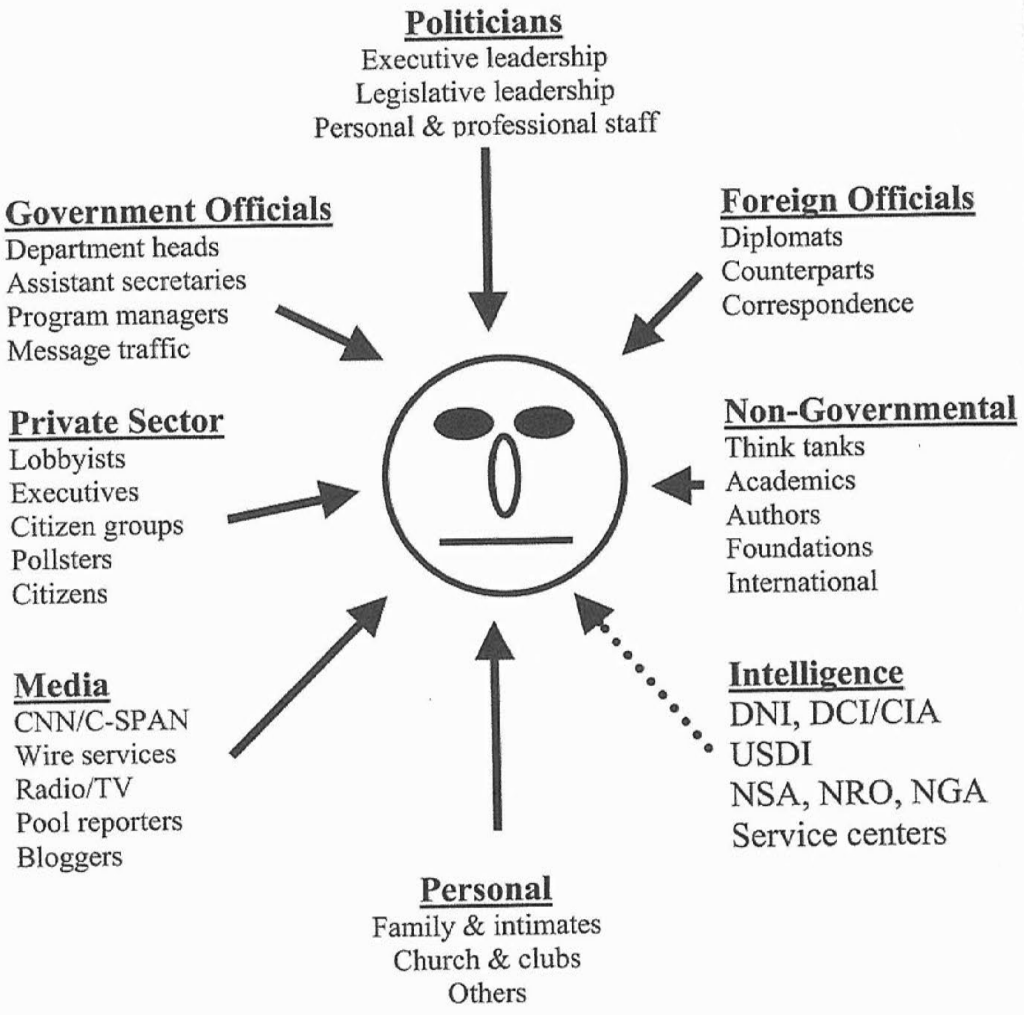

Figure 6-2. Competing Influences on the Intelligence Consumer

recognition, and public policy that is sustainable, which is to say, nonpartisan or bipartisan. Consider, for example, the findings shown in Figure 6-3 from the Report of the High-Level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility.*[17]

The average utility and relevance of OSINT to the global threats shown in Figure 6-3 is—on the basis of my informed estimate—82.5 percent, which comes very close to the generic "80-20" rule. We must conclude that any nation that persists in spending 99.9 percent of its intelligence funds on collecting secrets,[18] and less than one half of one percent of its intelligence funds on OSINT, is quite literally clinically insane (or insanely corrupt) at the highest levels.

In all three of the above cases, only OSINT can deliver a solution that is affordable, practical, and infinitely shareable with all stakeholders both in and out of government.

Economic and social threats, including	**95%**
• poverty	99%
• infectious disease	95%
• environmental degradation	90%
Interstate conflict	**75%**
Internal conflict, including	**90%**
• civil war	80%
• genocide	95%
• other large-scale atrocities	95%
Nuclear, radiological, chemical, and biological we	**75%**
Terrorism	**80%**
Transnational organized crime	**80%**

Figure 6-3. OSINT Relevance to Global Security Threats

Collection

Secret collection has made three fundamental mistakes across several generations of management:[19]

1. *Denigrated OSINT.* It chose to ignore open sources of information, assuming that the consumers of intelligence were responsible for their own OSINT, and that OSINT would not impact on secret collection. In fact, OSINT can dramatically reduce the cost and the risk, and increase the return on investment in secret sources and methods, simply by helping with targeting, spotting, assessment, validation, and the overall strategic context of what needs to be collected "by other means." It merits very strong emphasis that this failure to respect open sources of information falls into three distinct forms:

- Complete disrespect for history in all languages. There is no place within the U.S. government where one can "see" all Chinese statements on the Spratley Islands, or all Iranian statements on the competing Caliphate concept, or all Brazilian statements on alternative energy sources. We simply do not compute history, and consequently what little we know about current events and threats is known in isolated ignorance of history.

- Complete abdication of any responsibility for monitoring, understanding, and engaging substate or transnational entities as major factors in international affairs, and as threats or potential allies in domestic security and prosperity.
- Finally, almost complete abdication for more nuanced topics other than standard political-military calculations, with very important sustained failures to collect information on socioeconomic, ideocultural, technodemographic, or natural-geographic matters. This has been compounded by an extraordinary laziness or ignorance in relying almost exclusively on what can be stolen or obtained readily in English—the United States simply does not "do" the key 31 languages,[20] much less the totality of 185 languages necessary to understand the substate threat and the global network of cause and effect.

2. *Official Cover.* We have relied almost exclusively, at least in the United States, on "official cover" for our spies, and known trajectories for our satellites. Non-Official Cover (NOC), which does not offer any form of diplomatic or other official immunity from incarceration or eviction, has been treated as too expensive, too complicated, and not worthy of full development. The result has been the almost total compromise of all U.S. secret agents and case officers overseas, as well as their varied not-so-secret thefts of the codebooks of other nations. We not only don't know what we don't know, we are in denial about the basic fact that what we do know has been compromised.

3. *Failure to Process.* Finally, and this applies to both clandestine human collection and secret technical collection, we have failed, with deliberate ignorance at the management level, to devote any resources of significance to processing—to sense-making. Today, eighteen years after the needed functionalities for an all-source analytic desktop toolkit were published, we still do not have a desktop analytic toolkit. Today, despite major advances in the private sector with respect to machine-speed translation, and machine-speed statistical, pattern, and predictive analysis, the large majority of our classified intelligence analysis is still done the old-fashioned way: reading at human speed, cutting and pasting, attempting to make sense of vast volumes of secret information while lacking equivalent access to vast volumes of open source information (and especially open source information in any language other than English), limited by the physics of the twenty-four-hour day.

OSINT combines the proven process of intelligence with the ability to collect, process, and analyze all information in all languages all the time. We collect, at best, 20 percent of what we need to collect, at 99 percent of the cost, and we spill most of that for lack of processing capabilities. It can be said, as an informed judgment, that Washington is operating on 2 percent of the relevant strategic information necessary to devise, implement, and adjust national strategy.[21] We should not be sending spies where schoolboys can go, nor should we be ignoring scholarship in all languages.

There will still be a need for selected clandestine human operations, especially against organized crime and translation terrorist groups, but they will need to shift toward NOC and multinational task forces. Secret technical collection will need to emphasize commercial collection first, dramatically refocus secret collection, and shift the bulk of the future resources toward processing—making sense of what we do collect—and toward close-in technical collection inclusive of beacons for tracking bad guys and bad things.

Collection management will require draconian reform. Instead of defaulting to the tasking of secret collection capabilities, an enlightened collection manager will first determine if they can *find* the information for free in their existing stores of knowledge; then determine if they can *get* the information for free from an allied government or any of the seven tribes; and then determine if they can *buy* the information from a commercial provider, ideally a localized provider with direct indigenous access, in the time and with the operational security (e.g., cover support plans) appropriate to the need. Only if the first three options are unsuited to the need should the collection manager be tasking secret sources and methods, and even that will have to change to accommodate new possibilities from multinational secret task forces able to leverage the collection capabilities of varied countries, many of them vastly superior to the United States when it comes to both deep-cover clandestine human penetrations, and the related ability to place close-in secret technical collection devises.[22]

OSINT is, without question, the catalyst for a revolution in how we collect intelligence.

Processing

Apart from our failure to actually invest in processing (known within the U.S. intelligence community as Tasking, Processing, Exploitation, and Dissemination, or TPED), we have made three consistent mistakes over time that have made it virtually impossible, and now unaffordable, to actually do automated all-source analysis:

1. *No Standards.* We failed to establish data standards that could be used at the point of entry for both secret and open sources of information. This applies to both information sources and information software. Not only was the intelligence community much too slow to adopt commons standards such as eXtended Markup Language (XML), Resource Description Framework (RDF), Web Ontology Language (OWL), and Simple Object Access Protocol (SOAP), today it is either ignorant of or reluctant to move ahead aggressively with Open Hypertextdocument System (OHS)[23] and eXtended Markup Language Geospatial (XML Geo). The obsession with security, and the pathology of limiting contracts to the established firms in the military-industrial complex who profit from proprietary software and human headcount rather than real-world low-cost answers, can be blamed for the chasm between the secret intelligence world and the real world of open sources and standards.

2. *No Geospatial Attributes.* In fall 1988 it was made known to the U.S. intelligence community and clearly articulated by the author to a meeting of the General Defense Intelligence Program (GDIP), that in the absence of geospatial attributes for every datum entering the all-source processing system (actually an archipelago of private databases), that machine-speed all-source analysis and fusion would be an impossibility. Despite this, the individual secret collection disciplines of clandestine human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT) refuse to do anything other than persist with their human analytic reporting that provides date-time-group (DTG) and geographic place names where known, but no standard geospatial attributes for relating information to a map. Today Google Earth is being used in extraordinary ways to visualize relationship databases of real estate, shipping, and other important topics, and the individual citizen is light years ahead of the average "cut-and-paste" analyst at the federal, state, and local levels.

3. *No Integration.* There is no single place where all known information comes together. Despite critical concerns raised by every congressional and presidential commission since the 1940s, the U.S. intelligence community has continued to be "flawed by design"[24] and has persisted in the turf wars between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), between the FBI and the Drug Enforcement Administration (DEA), between the FBI and the Department of Justice (DoJ), and between the Departments of State and Defense. Within the Department of Defense (DoD), the services have not only competed with one another but actively conspired to fabricate and manipulate intelligence to exaggerate the threats relevant to their budget share. A corollary of this abysmal situation is that processing within the stovepipes has been focused on the delivery of documents rather than on making sense of all of the information in the aggregate. With the exception of selected efforts at the National Security Agency, the Army's Intelligence and Security Command, and the U.S. Special Operations Command, virtually all civilian and military analysts are still in cut-and-paste mode, and do not have the tools for pattern or trend analysis or anomaly detection, much less predictive analysis.

In processing, it is machine speed translation and statistical analysis, based on standards and global distributed information integration, that permits early warning, anomaly detection, and structured analysis that can be completed in a timely—that is to say, relevant—manner. OSINT is where the real innovation is occurring, and I anticipate that within ten years the secret world will be sharply restricted to no more than 20 percent of its present cost and size, while the balance of the funding is redirected to a mix of OSINT that can be shared with anyone, with peaceful preventive measures in lieu of a heavy-metal military.

Among the corrective measures required in secret processing, which OSINT will facilitate, are a shift toward the Internet as the common operating environment; the adoption of open source software to provide a generic access and collaborative sharing environment for all seven tribes;[25] the development of 24/7 "plots" at every level of governance in which all information can be seen in time

and geospatial context;[26] and the creation of a national skunkworks with an antitrust waiver for the public testing and certification of all open sources, software, and services. Rapid promulgation of free wireless within urban areas and in the Third World will help accelerate both sharing in the North and West, and uploading of useful information from the East and South.

Analysis

In evaluating the failure of analysis, it is important to understand that most U.S. analysts are too young, too inexperienced in the real world, and too isolated from foreign or even U.S. private-sector experts, to realize that the secret information they are receiving is out of context, often wrong, and largely irrelevant to strategic analysis. Their managers are too busy trying to be promoted or to win bonuses or please the White House (or the representative of the White House, the Director of Central Intelligence [DCI]). As a result, the strategic analysis vision of Sherman Kent has been dishonored and largely set aside. There have been three major failures in analysis over time.

1. *Hire Young.* The intelligence management philosophy in both the national civilian hires and at the military theater and service center levels has combined "hire to payroll" with obsessive lazy security parameters that have resulted in an analytic population that is largely young, white, and mostly bereft of overseas experience and especially long-term residency in foreign countries. Budgets have been used to hire low and promote over time, treating analysis as an entry-level hiring challenge rather than a mid-career sabbatical challenge. This has been deeply and pathologically influenced by a low-rent security philosophy that has combined paranoia over foreign contacts (and relatives) with an unwillingness to spend the time and thoughtfulness necessary to clear complicated individuals who have led complicated lives. This personnel management failure stems from the larger philosophical management failure, which confuses secrets with intelligence, and thus demeans expertise from the open source world while assuming that young analysts will succeed because they have access to secrets, rather than because of any application of analytic tradecraft such as might take twenty years to refine.

2. *Hard Target Focus.* In keeping with the military-industrial complex and its desire to profit from the Cold War, the national and military intelligence communities devoted virtually their entire budgets and most of their manpower to the "hard targets" (generally, Russia, China, Iran, India, Pakistan, Libya, and—hard to believe, but true—Cuba). They ignored all of the "lower tier" issues and Third World countries,[27] and also focused only on very big threats, not on very big opportunities for peaceful preventive measures where a few dollars invested in the 1970s might have eradicated Anti-Immune Deficiency Syndrome (AIDS) or dependency on Middle Eastern oil. This was of course in keeping with policy preferences, and even when the CIA did excellent work (for example, accurately forecasting the global AIDS epidemic), it could safely be ignored because its

work was not available to the public or even to most members of Congress. A very important consequence of this narrow focus was the complete failure to ensure that all of the sources of national power—diplomatic, informational, military, economic (DIME)—were funded, acquired, fielded, and applied in a coherent and timely manner. The entire military-industrial-intelligence complex has been skewed toward a heavy-metal military—a few big platforms or big organizations—that are only relevant 10 percent of the time. We are not trained, equipped, or organized for small wars, waging peace, or homeland defense. This is still true—truer that ever—in the aftermath of 9/11 and the invasions and occupations of Afghanistan and Iraq.

3. *Local Now.* Finally, U.S. intelligence (and many foreign intelligence communities) focused on the local now instead of the global future. "Current intelligence" dominated the *President's Daily Brief* (PDB), and over time longer term research fell by the wayside. This problem was aggravated by a draconian editing process in both the national civilian and theater- or service-level military, where a twelve-month research project could be subject to eighteen-month editing cycles, such that the work was out of date or thoroughly corrupted by the time it was finally released to a relatively limited number of policy makers. With most of the intelligence products being released in hard copy, or messages that were printed out and not saved electronically, the overall impact of U.S. intelligence production, and especially Codeword production, must be judged as marginal.[28]

OSINT is "the rival store."[29] Whereas I spent the first eighteen years of my campaign to foster an appreciation on OSINT and focusing on the urgency of integrating OSINT into secret sources toward improved all-source analysis, I plan to spend the next eighteen years burying 80 percent of the classified world. They are too expensive, too irrelevant, and pathologically antithetical to the new and correct Swedish concept of Multinational, Multiagency, Multidisciplinary, Multidomain Information Sharing (M4IS).[30] OSINT analysis will in the future be the benchmark by which classified sources and methods are judged to be relevant and cost-effective, or not. The Director of National Intelligence (DNI) has chosen to remain focused on secrets for the president. So be it. OSINT, from a private-sector and nongovernmental foundation, will capture all the other consumers of intelligence. The day will come when "clearances" are severely devalued and open source access—international open source access in all languages all the time—is ascendant. The DCI must serve all levels of the government, all seven tribes, and must balance between open and closed sources so as to inform decision makers—and their publics—in order to preserve and enhance the long-term national security and prosperity of the United States. Secret sources and methods—and the existing military—have demonstrably failed in both regards.

Analytic tradecraft notes are available online and should be consulted.[31] All-source analysts should not be hired until they have first proven themselves as masters of all open sources in all languages relevant to their domain and not be considered for mid-career hire unless they are one of the top twenty-five cited

authorities in the field. They must know how to leverage their historian, their librarian, and the Internet. They must know how to identify and interact with the top 100 people in the world on their topic, regardless of citizenship or clearances. Finally, they must understand that they are—and must be trained to be—managers of customer relations and requirements definition, of open sources, of external experts, and of classified collection management. Analysts must know and practice the "new rules" for the new craft of intelligence, with specific reference to being able to actually do forecasting, establish strategic generalizations, and drill down to the neighborhood and tribal levels, not simply hover at the nation-state level.[32]

Covert Action

Covert action consists of agents of influence, media placement, and paramilitary operations. Covert action assumes two things that may once have been true but are no longer true: that an operation can be carried out without its being traced back to the United States as the sponsor, and that the fruits of the operation will be beneficial to the United States. In each of these three areas, the United States has acted with great disdain for the normal conventions of legitimacy, accountability, morality, and practicality, and today the United States is suffering from what is known as "blowback"—it is reaping the dividends from decades of unethical behavior justified in the name of national security but unfounded upon any substantive grasp of long-term reality.

1. *Agents of influence* are individuals bribed covertly who are charged with getting their governments or organizations to pursue a course of action that the United States deems to be necessary but that may not be in the best interests of the indigenous public or its government. Regardless of what one may think of the local country and its government and public, what this really means is that agents of influence are responsible for disconnecting local policies from local realities, and imposing instead a reality or choice selected by the U.S. government. This is inherently pathological. There are certainly some success stories—support to Solidarity in Poland, for example, but this was a capitalization on the fall of communism, not the cause.
2. *Media placement* uses individuals, generally foreign journalists, who are bribed covertly to create and publish stories that communicate an alternative view of reality, one sanctioned by the U.S. government but generally at odds with the actual facts of the matter. There is a constructive side to media placement, for example the promulgation of information about atrocities committed by dictators or Soviet forces, but generally the U.S. government supports most of the dictators it deals with, and reserves this tool for deposing individuals that dare to oppose predatory immoral capitalism or virtual colonialism. Consequently, most media placement

activities consist of propaganda seeking to manipulate rather than deliver the truth. Media placement by spies should not be confused with public diplomacy by diplomats or strategic communication by the military—the latter two are overt truth-telling missions, although misguided practitioners may occasionally stray into propaganda and the manipulation of the truth.[33]

3. *Paramilitary operations* are not only direct assaults on the sovereignty of other nations, but they tend to bring with them black markets, drug running, money laundering, corruption, and the proliferation of a culture of violence and the small arms with which to do indiscriminate violence. The Phoenix program of assassinations in Vietnam, the support to the *contras* and the mining of the Nicaraguan harbors (an act condemned by the World Court), the arming of the Islamic fundamentalists for jihad in Afghanistan, join the planned overthrows of the governments of Chile, Guatemala, Iran, as causes of long-term and costly "blowback." Of all of these, Iran is the most interesting. Had we allowed the nationalization of the oil in Iran and the fall of the Shah, we might today have both a nonfundamentalist Iran as a bulwark against the radicals from Saudi Arabia, but we might also be less dependent on oil, and less subject to the whims of the extraordinarily corrupt Saudi regime and its U.S. energy company allies.

OSINT is the antithesis of all three forms of covert action. As David Ignatius noted so wisely in the 1980s, overt action rather than covert action delivers the best value in both the short and the long run. Promulgating the tools for truth—cell phones, wireless access, access to the Internet—is a means of fostering informed democracy and responsible opposition. It is also a means of creating stabilizing indigenous wealth. OSINT provides a historical and cultural foundation for achieving multicultural consensus that is sustainable precisely because it is consensual. As Jonathan Schell documents so well in *The Unconquerable World: Power, Nonviolence, and the Will of the People*, there are not enough guns in the world to force our way or protect our borders.[34] Only by fostering legitimacy, morality, charity, and full participation of all can we stabilize the world to the mutual benefit of the United States and the rest of the world.

OSINT, in addition to being vastly superior to covert action as a means for establishing reasonable goals that are sustainable over time, is also very well suited to documenting the extraordinary costs of historical covert actions. Only now is the public beginning to understand the lasting damage caused by the U.S. sponsorship of assassination attempts against Fidel Castro, capabilities that were ultimately turned against the unwitting president, John F. Kennedy, and his brother Robert. We have sacrificed our national values and our international credibility at the alter of covert action, and we are long overdue for a deep "truth and reconciliation" commission that evaluates the true costs of covert action, and

that then defines much more narrowly the conditions and protocols for engaging in covert action in the future.

Counterintelligence

Strategic counterintelligence is completely distinct from tactical counterintelligence.[35] In strategic counterintelligence, one is looking for emerging threats at the strategic level, not individual penetrations of specific organizations. This is an area where OSINT should, but does not, shine. The U.S. intelligence community—and consequently the U.S. policy community—have completely missed the end of cheap oil, the end of free water, the rise of bin Laden, and the rise of pandemic disease, even global warming, precisely because national counterintelligence was focused obsessively on penetrating foreign security services, and not on the strategic environment where natural and other threats of omission and commission were to be found. There are three areas in which strategic counterintelligence can benefit considerably from comprehensive OSINT, inclusive of the digitization and statistical analysis of all available historical information.

1. *National Education.* Thomas Jefferson said, "A Nation's best defense is an informed citizenry." This is absolutely correct, and even more so today, when central bureaucracies are no match for agile networked transnational groups. The United States has failed to understand the strategic implications of its lack of border control, its mediocre educational system designed to create docile factory workers, and the trends toward obesity, insularity, and indifference that characterize the bulk of the population today. We have gone hollow for lack of focus.

2. *Environment.* The Singapore military was stunned by the emergence of Severe Acute Respiratory Syndrome (SARS), but unlike the U.S. military they understood it. They realized they were responsible for defending Singapore against all threats, not just manmade or man-guided threats, and added national health and border security against airborne, waterborne, and human- or animal-borne diseases, to their charter. Similarly, the Singapore police have an extraordinarily nuanced and enlightened understanding of their global and regional information needs and responsibilities in relation to deterring and resolving all forms of crime impacting on Singapore. In the United States, and globally with dire consequences for the United States, there are threats associated with the environment and how it changes (including water, energy, and raw material resources) that are simply not understood, not acknowledged, and not being acted upon responsibly by any U.S. administration, be it Democratic or Republican.[36]

3. *Ideology.* There are two ideological threats to U.S. security today, one external, the other internal. The two together are very troubling. Externally, the radical and violent fundamentalist stream of Islam has been armed and energized by jihad in Afghanistan, in Chechnya, and in Iraq. Other small jihads in Indonesia, the Philippines, and southern Thailand, as well as selected locations in Muslim Africa, add to this threat. Internally, U.S. Christian fundamentalists have

assumed a terribly excessive importance in extremist Republican circles, in part because the Texas corporate energy interests chose to make common cause with them. The Middle East, oil, and the almost cultlike extreme religious right have hijacked American democracy. The American left, nominally but not intelligently led by the Democratic Party (which is as corrupt as the Republican Party, but more inept), meanwhile, abandoned faith and God and the sensible calming effect of religion as a foundation for community and ethics.[37] The American ideology of capitalism has also been corrupted. Immoral predatory capitalism, and pathologically inept formulas for "developmental economics" as imposed on failed states by the International Monetary Fund (IMF) and the World Bank have given rise to populism and other forms of indigenous resistance now witting of the collusion between their corrupt elite and immoral foreign capitalism that are in combination looting the commonwealth of many peoples.[38]

In all three of these cases, OSINT has an extraordinary role to play. Under the leadership of Congressman Rob Simmons (CT), a moderate Republican with an extraordinarily deep background in both intelligence and on the Hill, the campaign continues for a national Open Source Agency funded at $3 billion per year, under the auspices of the Department of State (as a sister agency to the Board of Governors that controls the Voice of America and other public diplomacy outlets). However, fully half the budget is intended to fund fifty Community Intelligence Centers and networks across the country (each receiving $30 million at full operating capability). These centers are needed for two reasons: first, to provide 119 and 114 numbers for citizen mobilization (119 alerts all cell phones within a 5 kilometer radius) and citizen neighborhood watch inputs (114 receives cell phone photos, text messages, any form of information, all with geospatial and time tags); and second, to serve as dissemination nodes for transmitting to all schools, chambers of commerce, churches/synagogues/mosques, labor unions, civil advocacy groups, and so on, the wealth of "real world" information to be collected, processed, and shared, free via the Internet, by the Open Source Agency. This will impact very favorably on the environment, as these centers will help citizens at the county, state, and regional levels understand, with precision, where each of them stands with respect to access to clean water, alternative energies and related lifestyle choices, and global threats to their children and grandchildren based on easy access to the actual U.S. federal budget in relation to real world threats and needs. Militarism can be reduced, poverty and disease can be eliminated, and the United States can rejoin the community of nations as a force for good. Finally, all competing ideologies can be subject to scrutiny and understanding, and the majority of Americans who are not part of the right can come together consensually to limit the damage these people can do to the republic, while also holding their political and corporate allies accountable for serving America as a whole rather than a fringe element.

Dramatically redirecting national intelligence toward OSINT will substantially reduce the cost of secrecy, estimated by the Moynihan Commission as being on the order of $6 billion a year (probably closer to $15 billion a year

today),[39] and will also eliminate perhaps 70 percent of the costs associated with establishing the trustworthiness of individuals being considered for clearances. The security and clearance system of the U.S. government is broken beyond repair. Not only does it take over two years for most investigations to be completed, but they are generally substandard investigations that go through the motions and generally do not detect basic aberrations, such as a fascination with child pornography and online molestation of children, as was the case recently with a senior manager in the Department of Homeland Security. The fact is that most sheriffs and other state and local officials are not "clearable" for a variety of reasons, and we may as well recognize that not only is OSINT better suited for most national intelligence information sharing, but we really do not need most of the grotesquely expensive and dysfunctional top-secret "compartments" (over 400 of them, half in the civilian world and half in the military world) and all the attendant costs, including the costs of ignorance stemming from compartmentalized information not being shared. At least at the strategic level we need a national intelligence system in which we are less concerned about betrayal from within, and more focused on emerging strategic threats to our long-term security and prosperity, threats that must not be limited to manmade capabilities, but include animal-borne diseases and other environmental conditions that tend to be shut out from national security decision processes.

Accountability, Civil Liberties, and Oversight

As all of the preceding sections should have made clear, OSINT is the essential contributing factor to dramatically improving the accountability and oversight of the U.S. intelligence community and the policy makers, acquisition managers, and operational commanders who respond to White House direction. OSINT is also a means of dramatically enhancing not just civil liberties, but civic engagement in the practice of democracy. By providing citizens at every level with structured OSINT on any issue for any zip code or other geographic grouping, and by making it possible for citizens to immediately connect with other like-minded citizens and with accountable officials, OSINT in practice is an enabler of a new form of constant engaged informed democracy. Civil liberty infractions will be broadcast or podcast, rapidly aggregated, and civil pressure brought to bear. By harnessing citizens as part of the "home guard" and empowering them with immediate and understandable access to indications and warning information, we will dramatically improve the reporting of relevant information, and—through the Community Intelligence Centers—be able to process, make sense of, and act on or discount the "bottom up" dots that I am convinced will comprise at least 50 percent of the relevant dots needed to prevent the next 9/11.

It is also important to emphasize that, at the strategic level, we need to be concerned not just with accountability and oversight of secret intelligence, but with the much larger issue of whether Congress and the Executive are being responsible in representing the public interest. For this reason are included very brief but vital

sections at the end of this chapter on OSINT and electoral reform, governance reform, and budgetary reform. OSINT is the ultimate resource for citizens to hold their government accountable, and to protect their civil liberties over time.

Strategic Warning

Although the CIA has done some fine work on global threats, and I particular like the work done under John Gannon as Assistant Director of Central Intelligence for Analysis & Production (*Global Trends 2015*, which led to *Global Trends 2020*),[40] on balance the U.S. intelligence community has failed abysmally at strategic warning because of some fundamental operational and philosophical failures.[41]

Operationally, despite fifty years of extraordinarily generous funding for multi-billion-dollar satellite systems, the U.S. intelligence community still cannot do wide area surveillance, real-time change detection, or "the last mile" inclusive of seeing into an urban area, under jungle canopy, and into the deep ravines of mountainous terrain.

Philosophically U.S. intelligence has been a disaster in strategic terms. The cult of secrecy limited "intelligence" to "secrets for the president" and left everyone else, from Cabinet-level leaders to military acquisition manager and operational commanders, to governors and mayors, completely without "decision-support." Perhaps worse, the U.S. intelligence community has refused to recognize the seven tribes of intelligence, shutting out, for the most part, state and local officials with overseas knowledge, business travelers, academics, nongovernmental observers, journalists, labor union leaders, religious travelers, and so on. The obsession with government secrecy over public sharing has cost this nation fifty years of time—the one strategic factor that can be neither bought nor replaced[42]—and at least 3 billion souls of goodwill. U.S. intelligence is a small part of the overall federal government, and it merits comment that most of our problems today cannot be blamed on U.S. intelligence as much as on a corrupt Congress and Executive all too eager to ignore, for example, the Peak Oil warnings of 1974–79 in order to keep the bribes going and the public docile. This is not, however, to excuse the U.S. intelligence community, in as much a focus on OSINT from 1988 onwards would have done much to illuminate and correct the policy errors that benefited from secrecy, obscurity, and public inattentiveness.

Strategic Sharing

The U.S. intelligence community is incapable today, five years after 9/11, o creating a single consolidated watch list of suspected terrorists. The U.S. gov ernment as a whole is incapable of sharing everything that it knows for lack o collaborative mindsets, willing management, interoperable systems, and coheren data sets. There are three primary impediments to the U.S. intelligence commu nity ever being able to share readily:

1. *High Side Security.* The obsession with security is occasioned in part by the fact that the secret intelligence world, even though it has "compartments," has never learned to disaggregate secret from nonsecret information. Everything is stored at the "high side," at the highest possible level of security, meaning that nothing can be shared with anyone who is not cleared for the highest level of security, however unclassified the information might be.

2. *Third Party Rule.* The secret world has for decades operated under a "third party rule" that prohibits the sharing of any information received from one party with another party. This rule is extremely detrimental to multilateral sharing, and imposes enormous time, manpower, and dollar costs when something needs to be shared and the sharing must be coordinated. The default condition of the secret world is "do not share."

3. *Legacy Systems.* As John Perry Barlow noted in an article in *Forbes*,[43] if you want to see the last remnants of the Soviet Empire, go visit the CIA and look at their computer systems. The U.S. intelligence community as a whole is still mired in 1970s technology managed by 1950s mindsets, totally out of touch with 21st-century information networks, both machine and human.

OSINT is going to be the catalyst for M4IS and strategic sharing. OSINT is the only discipline that can easily distribute the collection, processing, and analysis burden across all coalition nations (i.e., the ninety nations comprising the U.S. Central Command coalition), and also the only discipline whose products can easily be shared with nongovernmental organizations as well as state and local authorities all over the world who will never qualify for "clearances." It will be our challenge in the next eighteen years to develop an alternative global intelligence community that relies almost exclusively on "good enough" open sources, and that consequently forces the secret world into proving its "added value" in relation to cost, risk, and time, on every topic, every day.

Emerging Prospects

Apart from increased public access to the Internet—inclusive of electronic mail, the deep web, and the dramatically increased availability of free multimedia communications and information sharing capabilities—several factors are supportive of a displacement of secret sources and methods by open sources and methods:

Digitization

It is a mistake to believe that all relevant information is being digitized today. Tribal histories (e.g., those from Iraq) and vast quantities of important information are still being produced in Industrial Era media, and Friday sermons by Islamic imans, as well as the sermons by all the other faiths, are not part of the digital revolution. In strategic terms, however, digitization is extremely important for three reasons:

1. Most current information from mainstream and niche media as well as individual publishers and bloggers, in all languages, is now available digitally.
2. Historical information, including policy and financial statements of great importance to specific nations, industries, organizations, and tribes can now be affordably and effectively digitized.
3. Hand-held devices are rapidly becoming a primary means of collecting and sharing information, with imminent prospects of being able to harness, selectively, all that any group of individuals can see and hear and think, and is willing to upload as needed.

VISUALIZATION

Digital information, including historical information, can now be visualized, not only in relation to content analysis and links between paragraphs and among individuals, but in relation to a geospatial foundation such as Google Earth provides in rudimentary but quite compelling terms. This is moving OSINT well beyond secret sources and methods because it can draw on a much greater body of information and expertise in real time, and apply all modern machine analytic tools with fewer security, legal, and policy constraints. The centralized, unilateral, secret bureaucracies are losing ground—rapidly—to distributed, open, multinational networks.

PEER-TO-PEER (P2P)

"Ground truth" is taking on a whole new meaning as individuals exercise the power to share complex information directly with one another, eliminating the intermediary journals, web sites, and government or media offices that in the past have played the role of editor, judge, and broker of meaning and value.

The power of OSINT at the strategic level can neither be exaggerated nor underestimated for the simple reason that it harnesses the distributed intelligence of the whole earth, in real time as well as in historical memory time, across all languages and cultures. There is not a bureaucracy in the world that can match its networked power. To drive that point home, consider the game of baseball. In today's secret environment, government bureaucrats accustomed to unlimited budgets and secret methods continue to try to win the game by bribing a player (clandestine intelligence), putting a "bug" in the dugout (signals intelligence), trying to "sniff " the direction and speed of the ball (measurements and signatures intelligence), or taking a satellite picture of the field every three days (imagery intelligence). The new craft of intelligence integrates the audience. It uses the collective wisdom of all the participants. It encourages the crowd to participate. Open source intelligence harnesses what everyone sees and knows. It changes the rules of the game. Any catch in the stands is an out. That is

how we win against asymmetric opponents who know our Achilles' heels all too well.

OSINT AND ELECTORAL REFORM

The United States is a republic. An extraordinary characteristic of republics is that voters have the power to dissolve the government should it become so ineffective or destructive as to warrant its termination. The Constitution, and the voters, are the foundation of the American democracy, not the three branches of government. If the Executive is mendacious, the Congress is corrupt, and the Judiciary is so unrepresentative of the values of the people as to be a mockery of justice, then the public has the power to change the rules of the game for elections. It is OSINT that can be used by citizens to break away from the Republican and Democratic parties, and develop new networked means of demanding minimalist changes such as suggested by Ralph Nader and enhanced by the author: voting on weekends so the poor do not lose work; restoring the League of Women Voters as the arbiters of multiparty debates; demanding that presidential candidates announce their Cabinets in advance of the election, and including at least the Secretaries of Defense and State, and the Attorney General, in Cabinet-level debates; applying the instant runoff concept to ensure a true majority election; and, of course, ending gerrymandering and corporate funding for any elected official.

OSINT AND GOVERNANCE REFORM

Government at the federal level has become incompetent, and is wasteful of the taxpayer dollar for two reasons: special interest corruption both in Congress (bribery) and in the Executive (revolving-door favoritism); and an industrial-era structure that is largely disconnected from reality to the point that ideological fantasy can supplant a reasoned policy process. At a minimum, the republic needs a coalition Cabinet and some means of assuring the citizenry that presidents will not be able to simply appoint cronies from their own party; the Executive needs to be restructured to provide for integrated policy development, not just national security policy development; strategic planning focused out seven generations (over 200 years) must be demanded and be publicly transparent and accountable; and the fundamentals of national power must be mandated: quality education for all, health care for all, and an end to poverty at home. Presidents and their teams must be elected for their ability to govern rather than campaign. OSINT will make all of this possible, sooner than later if a national Open Source Agency is created as a new fourth branch of government, independent of Congress and the Executive, with a lifetime appointment for its Director, and a Board of Directors composed of former presidents, leaders of the Senate and House, and retired Supreme Court justices.

OSINT AND STRATEGIC BUDGETARY REFORM

Finally, we come to budgetary reform. OSINT has already made it clear that we have a Department of Defense costing $500 billion a year (not counting the cost of the war in Iraq) that is relevant to only 10 percent of the threat (state-on-state warfare), that is largely incompetent at small wars and homeland defense, and that we are, as a republic, not investing properly in peaceful preventive measures inclusive of the spread of participatory democracy and moral capitalism. The return on investment on our "big war" military is not only not there, the existence of that big war force leads ignorant presidents and their mendacious vice-presidents to seek out wars as an option for capturing "cheap" oil (never mind the cost in blood, spirit, and treasure). The American republic, specifically, and all other countries are long overdue for what I call "reality-based budgeting." OSINT will restore sanity and sensibility to the public treasury and how it is applied.

There is, in the immortal words of Arnie Donahue[44] in 1992, "plenty of money for OSINT." There is also plenty of money for participatory democracy and moral capitalism. Our problem has been that we have allowed the mandarins of secrecy to pretend to be informing the president, rather narrowly and very expensively, while failing to demand that the republic develop a public intelligence capability suitable for directing public policy and public spending in an intelligent, sustainable manner.

September 11, the Iraq War, and the varied accomplishments—or crimes—of the Bush administration may stand in history as a bright turning point in the history of the republic. One doubts that anything less might have awakened the somnolent public.

NOTES

1. The "seven tribes" is a concept developed by the author and includes government, military, law enforcement, business, academia, the ground-truth tribe (nongovernmental organizations and the media), and the civil-sector tribe (citizen advocacy groups and societies, labor unions, and religions).

2. This term, "Revolution in Intelligence Affairs," is abused by loosely educated individuals who know nothing of revolution and little of all-source intelligence. For a critique of the abuse of the term, and a discussion of the three options for intelligence reform, see the author's "Intelligence Affairs: Evolution, Revolution, or Reactionary Collapse," *International Journal of Intelligence and Counterintelligence* 19 (Spring 2006), pp. 187–189. In a forthcoming issue the author comments on "Intelligence in Denial."

3. This is a practical professional discourse on OSINT, not a political diatribe, but it is essential for those who have the most to gain from OSINT, citizens, to understand that the extremist Republicans have driven out the moderate Republicans (including the author) while the inept Democrats have alienated both the conservative Democrats and the

New Progressives. For an excellent and erudite discussion of why the prevailing mood of the country may well be "a pox on both parties," see Peter Peterson, *Running on Empty: How the Democratic and Republican Parties Are Bankrupting Our Future and What Americans Can Do About It* (New York: Farrar, Straus and Giroux, 2004). Peterson was a Cabinet Secretary under Nixon and Chairman of the Council on Foreign Relations. He joins numerous other moderate Republicans who have published books dismissive of the Republican Party as it has been hijacked by the religious extremists, the neo-conservatives, and corporate war-profiteers. The Democratic leadership is equally corrupt, but so inept as to be incapable of either governing or holding the Republicans accountable.

4. Howard Rheingold, *Smart Mobs: The Next Social Revolution* (New York: Basic Books, 2003); James Surowieki, *The Wisdom of the Crowds* (New York: Anchor, 2005); and Pierre Levy, *Collective Intelligence: Mankind's Emerging World in Cyberspace* (New York: Perseus, 2000). Three other essential references are H. G. Wells, *World Brain* (London: Ayer, 1938); Howard Bloom, *Global Brain: The Evolution of Mass Mind From the Big Bang to the 21st Century* (New York: Wiley, 2001); and Tom Atlee, *The Tao of Democracy: Using Co-Intelligence to Create a World That Works for All* (San Francisco:Writer's Collective, 2003). Robert Steele addresses the concepts and doctrine for actually "doing" collective public intelligence in *The New Craft of Intelligence: Personal, Public, and Political* (Oakton, VA: OSS, 2002).

5. It is now clearly documented that both the White House and the Senate knew that Peak Oil was upon us during varied hearings conducted from 1974–79, and deliberately concealed this fact from the public, and failed to alter energy policy, in order to avoid alarming citizens or angering them over prices, while continuing to reap the rich dividends of bribery from the oil companies. This is a single specific example of where retrospective impeachments would be appropriate as a means of putting all elected officials so that they will be held accountable not just today, but into the future as their treasonous betrayal of the public trust becomes known.

6. There are 20,000 pages on OSINT at http://www.oss.net, and a one-page list of key familiarization links covering history, context, practice, policy, and reference are at http://www.oss.net/BASIC. To this day, the secret intelligence world refers with disdain to OSINT as "Open Sores."

7. The single best book on the cost of the Cold War is Derek Leebaert's *The Fifty-Year Wound: How America's Cold War Victory Has Shaped Our World* (Boston: Back Bay Books, 2003). Chalmers Johnson has written two books in this genre, the first and most recent more methodical than the second: *The Sorrows of Empire: Militarism, Secrecy, and the End of the Republic* (New York: Metropolitan Books, 2004), and *Blowback: The Costs and Consequences of American Empire* (New York: Owl, 2004, reissue). See my partial list of books on blowback at http://tinyurl.com/qrcdu. An entire literature on "why people hate America" has been developing, along with U.S.-based critiques of immoral capitalism and virtual colonialism.

8. General Alfred M. Gray, Commandant of the Marine Corps, "Global Intelligence Challenges in the 1990s," in *American Intelligence Journal* (Winter 1988–89), pp. 37–41. Despite four years of effort by the Marine Corps, the National Foreign Intelligence Board (NFIB) and the Military Intelligence Board (MIB) refused to address General Gray's recommendations that we change our priorities from worst-case least probable to most probable emerging threats, and that we invest in open sources. Had we done so from 1988 to 2000, in those twelve years we would probably have collected enough open sources in

Arabic and other languages to understand the threat represented by bin Laden in terms compelling enough—because they were public—to mandate sustained effective action by all relevant national capabilities.

9. Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (London:Viking, 2002). This is his recollection of his words to Henry Kissinger, then National Security Advisor to President Richard Nixon. The three pages on the pathological effects of falling prey to the cult of secrecy, on pages 237–39, should be forced rote memorization for all who receive clearances.

10. General Tony Zinni, U.S.M.C. (Retired), former Commander-in-Chief, U.S. Central Command (CINCCENT), as recounted to the author on April 4, 2006, by a very prominent individual close to varied National Security Council and defense personalities, who desires to remain anonymous.

11. As recounted in Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003).

12. Cf. Robert Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, VA: AFCEA, 2000; Oakton, VA: OSS, 2003) with a Foreword by Senator David Boren (D-OK), whose efforts to reform national intelligence in 1992 were undone by a combination of Senator John Warner (R-VA) and Secretary of Defense Dick Cheney. The book remains the single most comprehensive public critique of the shortfalls of the secret world. For a list of other books critical of the past and offering a vision for the future, see my varied lists at Amazon.com.

13. Cf. Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books, 1985). Many other books give accounts of secret warfare going back in time, but culminating in the behind-the-lines operations in World War II, and then the "dirty tricks" of the 20th century.

14. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1948). This is a classic. In reality, Kent did not achieve his vision for two reasons: because the clandestine service took over the Central Intelligence Agency and subordinated the analysts, and because, in so doing, they cut the analysts off from the world of open sources that were the mainstay of Kent's vision in the first place.

15. Robert Steele is the primary author on the concept of "smart nation." Among the early works were "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare," in contributing eds., *Cyberwar: Security, Strategy, and Conflict in the Information Age*, contributing eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA, 1996), pp. 77–89; "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," *Government Information Quarterly* 13 (Summer 1996), pp. 159–173; "Reinventing Intelligence: The Vision and the Strategy," *International Defense & Technologies* (December 1995), bilingual in French and English; and "Private Enterprise Intelligence: Its Potential Contribution to National Security," paper presented to the Canadian Intelligence Community Conference on Intelligence Analysis and Assessment, October 29, 1994, reprinted in *Intelligence and National Security* (Special Issue, October 1995), and also in a book by the same name, 1996.

16. The sections that follow deliberately relate OSINT to reform of the secret elements of the intelligence cycle. Complete multimedia lectures, a total of eight, are easily accessed via http://www.oss.net/BASIC.

17. (New York: United Nations, 2004). The endeavor benefited from the participation of The Honorable Lieutenant General Dr. Brent Scowcroft, U.S.A.F. (Retired),

former national security advisor to President George Bush. Terrorism is ninth out of the ten high-level threats. The report, 262 pages in length, can be seen at http://www.un.org/secureworld/report2.pdf.

18. It merits comment that according to the *Report of the Commission on the National Imagery and Mapping Agency*, as published in December 1999, most of the intelligence money is spent on esoteric collection systems, and almost none at all is spent on actually making sense out of the collected information.

19. The author has served in the clandestine service (six tours, three overseas), supported strategic signals intelligence acquisition operations, and been a member of the Advanced Program and Evaluation Staff (APEG) with responsibilities for national-level validation of current and future secret imagery collection programs.

20. The languages that OSS and its partners use to follow terrorism and other topics properly are as follows: Arabic, Aramaic, Berber, Catelan, Chinese, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish, and Urdu. Arabic variations include Andalusi Arabic (extinct, but important role in literary history); Egyptian Arabic (Egypt), considered the most widely understood and used "second dialect"; Gulf Arabic (Gulf coast from Kuwait to Oman, and minorities on the other side); Hassaniiya (in Mauritania); Hijazi Arabic; Iraqi Arabic; Levantine Arabic (Syrian, Lebanese, Palestinian, and western Jordanian); Maghreb Arabic (Tunisian, Algerian, Moroccan, and western Libyan); Maltese; Najdi Arabic; Sudanese Arabic (with a dialect continuum into Chad); and Yemeni Arabic.

21. This is a very serious indictment of both the policy community and the intelligence community. It is based on direct observation in three embassies overseas (three tours), on a second graduate thesis on strategic and tactical information management for national security, and on eighteen years of advocacy during which over forty governments have been helped to enhance their access to and exploitation of open sources of information.

22. The author spent a tour in the Collection Requirements and Evaluations Staff (CRES) at the CIA, and also consulting in the 2000–1 timeframe to ICMAP, the attempt by the Deputy Director of Central Intelligence for Administration (DDCI/A) to reduce duplicative tasking of the varied classified collection disciplines. Neither the CIA nor the new Open Source Center have a full grasp of how to access all information in all languages all the time, and ICMAP continues to focus on triage among the classified systems, without regard for what can be found, gotten, or bought.

23. This is the only standard that may not be readily apparent when this chapter is published. Invented by Doug Englebart, also the inventor of the mouse and hypertext, this standard enables linkage of related content to take place at the paragraph level, which also allows copyright compliance to be executed at the paragraph level, for pennies instead of dollars.

24. Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Palo Alto: Stanford University Press, 2000).

25. It is a fact that 90 percent of the information that we need to gain access to is controlled or obtainable by nongovernmental, academic, civil, and generally foreign organizations that cannot afford the gold-plated and generally pathologically dysfunctional information technology systems that the beltway bandits have been selling to the secret world for decades. In order to create a global information sharing environment where we

can get much more than we give in the way of content (what we can provide is processing power), it is essential that we establish generic open source software suites of tools, such as the Defense Advanced Research Projects Agency (DARPA) has done with STRONG ANGEL, so that all relevant contributors can join the Open Source Information System (OSIS) via inexpensive collaborative toolkits and access ports.

26. Information technology has not been an obstacle to the creation of 24/7 "plots" but rather mindsets and bureaucratic inertia. For a stimulating and truly enlightening account of both the early mistakes and later successes of the British in World War II in using "plots" to track and anticipate the movements of submarines (a skill applicable to today's terrorists), see Patrick Beesley, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939–1945* (London: Greenhill, 2000). As with all books cited, a summative review by Robert Steele, with key points itemized, can be read at Amazon.com.

27. Despite General Gray's concern in 1988, and years of effort by the author that culminated in testimony to the Aspin-Brown Commission resulting in a finding that our access to open sources was "severely deficient" and should be a "top priority" for funding; and despite a report commissioned by DCI George Tenet and delivered by Boyd Sutton in July 1997 on "The Challenge of Global Coverage"—a report recommending that $1.5 billion a year be spent on open sources as an insurance policy, consisting of $10 million a year on each of 150 topics of lower tier countries spawning terrorism, crime, disease, and other ills—Tenet, his predecessors, and his successors have consistently refused to focus on anything other than secrets for the president. The Global Coverage report is easily accessible via http://www.oss.net/BASIC.

28. There are a handful of books that really emphasize the importance of history and the continuing strategy relevance of historical factors including morality and birth control (or not). Among them: Will and Ariel Durant, *The Lessons of History* (New York: Simon & Schuster, 1968); Richard Neustradt and Ernest May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1988); Stewart Brand, *The Clock of the Long Now: Time and Responsibility—The Ideas Behind the World's Slowest Computer* (New York: Basic, 2000); and John Lewis Gaddis, *The Landscape of History: How Historians Map the Past* (New York: Oxford, 2004). Included here are two books on the strategic implications of losing history, and failing to notice fact: Robert Perry, *Lost History: Contras, Cocaine, the Press & "Project Truth"* (San Francisco: Media Consortium, 1999), and Larry Beinhart, *Fog Facts: Searching for Truth in the Land of Spin* (New York: Nation Books, 2005).

29. This term was first used by Alvin Toffler to describe the author, his company, and OSINT. See the chapter on "The Future of the Spy" in which five of the twelve pages are focused on OSINT, in *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner, 1995). All of the books by the Tofflers, who now write as a team, are relevant to the information era, but *Powershift: Knowledge, Wealth, and Power at the Edge of the 21st Century* (New York: Bantam, 1991) is rather special.

30. This term (M4IS) was first introduced by the Swedes at the Third Peacekeeping Intelligence Conference held in Stockholm in December 2004. The Swedes have replaced the Canadians as the neutral third party of choice.

31. Googling for "analytic tradecraft" is always useful. The actual notes from Jack Davis can be accessed via http://www.oss.net/BASIC.

32. As with all observations in this chapter, the specifics are easily accessible via http://www.oss.net/BASIC, in this case as "New Rules for the New Craft of Intelligence," under Practice, where other guides to analytic tradecraft may also be found.

33. Cf. Robert Steele, *Information Operations: All Information, All Languages, All the Time* (Oakton, VA: OSS, 2006) and—more focused on the military as well as free—*Information Operations: Putting the I Back Into DIME* (Strategic Studies Institute, February 2006). The latter is easily found by Googling for the title.

34. Jonathan Schell, *The Unconquerable World: Power, Nonviolence, and the Will of the People* (New York: Owl, 2004).

35. The author spent a tour at the national level responsible for offensive counterintelligence against a denied area county, and was also responsible for global oversight of recruitment efforts against all representatives of the same government.

36. In general the reader is referred to the 770+ books reviewed by the author at Amazon.com over the past five years. Dr. Colonel Max Manwaring (Retired) has edited *Environmental Security and Global Stability: Problems and Responses* (Lanham, MD: Lexington, 2002) and there is an entire literature on ecological economics as well as on the health of nations, relating disease, poverty, and the environment.

37. On this vital topic, see on the internal threat, two books: Kevin Philips, *American Theocracy: The Peril and Politics of Radical Religion, Oil, and Borrowed Money in the 21st Century* (New York: Viking, 2006), and Michael Lerner, *The Left Hand of God: Taking Back Our Country From the Religious Right* (New York: Harpers, 2006). On the external threat, though there are numerous books on radical Islam, the best overall discussion of ideology as a means of changing the pecking order among social groups, and grabbing real estate and resources, is offered by Howard Bloom, *The Lucifer Principle: A Scientific Expedition Into the Forces of History* (Boston: Atlantic Monthly, 1997). The book includes a prescient discussion of Sunni versus Shiite, as well as of religion as an ideology used to capture resources.

38. Among the most obvious and hard-hitting current references on immoral capitalism are Clyde Prestowitz, *Rogue Nation: American Unilateralism and the Failure of Good Intentions* (New York: Basic, 2004); John Perkins, *Confessions of an Economic Hit Man* (New York: Plume, 2005); William Greider, *The Soul of Capitalism: Opening Paths to a Moral Economy* (New York: Simon & Schuster, 2004); and, most recently, Jeffrey Sachs, *The End of Poverty: Economic Possibilities for Our Time* (New York: Penguin, 2006). There is a separate literature on "virtual colonialism" and the inner anger that a U.S. military presence inspires, particularly in Muslim countries.

39. *Report of the Commission on Protecting and Reducing Government Secrecy* (GAO, 1997), available at http://www.fas.org/sgp/library/moynihan/.

40. Both are available online.

41. No disrespect is intended in neglecting to address the standard works on strategic warning. The author's concept of strategic warning is much broader than now exists within both the secret intelligence world and the academic world that writes about the secret intelligence world.

42. Colin Gray, *Modern Strategy* (New York: Oxford, 1999). An eight-point summary is at Amazon.com. A superb monograph on strategy (eighty-three pages) by Dr. Colonel Harry (Rich) Yarger (Retired), "Strategic Theory for the 21st Century," is easily found online by Googling the author and title.

43. John Perry Barlow, "Why Spy?" *Forbes* (October 7, 2002), available at http://www.forbes.com/asap/2002/1007/042.html.

44. At the time, Donahue was the ranking director with the Office of Management and Budget (OMB) for all Command and Control, Communications, Computing, and Intelligence (C4I), and one of a handful of individuals with all of the code-word clearances. His boss, Don Gessaman, the ranking civil servant at OMB for National Security inclusive of Programs 50 (International Relations) and 150 (Defense), guided the establishment of Code M320 for defense expenditures on OSINT in 2000. OSINT is seen by the intelligence community as a threat that should not be outsourced, and by OMB as a function that can be accomplished in the private sector and therefore should be outsourced to the fullest extent possible.