Intelligence in the Internet Era

A. Denis Clift

"Actionable information from around the globe is today the air we breathe, essential to our national security and survival."

During the Napoleonic Wars, the French revolutionized land-based communications with the erection of semaphore towers bearing rotating arms to fashion coded signals that could speed by line-of-sight from tower to tower along the coast and across the country at some 200 miles an hour. The British quickly followed suit in that new era of signals intelligence. Theft of the enemy's semaphore codebooks became an important part of the business of war.[1]

During the war on terrorism in Afghanistan, "Predator" unmanned aerial vehicles (UAVs), flying lengthy missions at heights of some 25,000 feet, have been providing multi-hour surveillance of designated geography, installations, and activity. Tasking to the Predator, as well as electro-optical video and infrared images collected by its cameras, move near-instantaneously to and from the theater commanders and officials in Washington. Such communications flow through a secure network of ground stations and satellites, with part of the product traveling through a classified Internet counterpart.[2]

The episodic manned U-2 photography missions of the 1950s and the periodic evolutionary satellite photography missions proceeding from the 1960s have now been joined by the current generation of surveilling UAV eyes. Imaging, analyzing, and decisionmaking, which once proceeded in distinct, often lengthy, sequential steps, now occur almost simultaneously.

To leap thus across the centuries and the more recent decades is to realize in a glimpse the incredible dynamic involved in the world of intelligence and its supporting communications technologies. Actionable information from around the globe is today the air we breathe, essential to our national security and survival.

The Internet era brings an onrush of changes, both revolutionary and subtle, to the work of intelligence—changes in the doctrine and practice of collection, analysis, and dissemination; and changes in the mindsets and relationships between intelligence and law enforcement, intelligence and the policymaker, and intelligence and the military commander.

Internet Origins

In 1957, signals from the beeping Soviet satellite Sputnik I sounded the beginning of the highly visible superpower space

A. Denis Clift is President of the Joint Military Intelligence College.

[1] Stephen E. Maffeo, *Most Secret and Confidential* (Annapolis, MD: Naval Institute Press, 2000), pp 68-69.
[2] "Predator, A Global Option, General Atomics Aeronautical Systems Fact Sheet" (San Diego, CA: General Atomics Aeronautical Systems, Inc., 2001).

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence in the Internet Era	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for the Study of Intelligence,Central Intelligence Agency,Washington,DC,20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES
Studies in Intelligence, Volume 47, No. 3, 2003

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

race. That race produced some remarkable by-products, from cordless power tools and Teflon to CAT Scanners and Magnetic Resonance Imaging technology. Out of the public eye, the orbiting Sputnik launched other races by US scientists and engineers. The Office of Science Adviser was added to the White House, and, in 1958, President Eisenhower created the Advanced Research Project Agency (ARPA).

One of ARPA's earliest priorities was to tackle the challenge of linking research centers with one another and with their important sponsor, the Department of Defense. As this research evolved, the computer's initial role as arithmetic engine expanded to include the computer as communications medium. Pioneers in the work of data networking and packet switching applied their talents to create a government-supported computer data network: ARPANET. The developers of the first network in the late 1960s—at UCLA, the Stanford Research Institute, the University of California/Santa Barbara, and the University of Utah—could not have imagined that their work would spawn the global Internet of today.[3]

The work on ARPANET called attention to the vulnerability of the nation's strategic communications infrastructure. If the Soviets could orbit Sputnik, who was to say that they were not proceeding to develop the capability for a space-based missile attack? If a nuclear attack destroyed key command and control centers, it would eliminate our ability to assess the impact of the attack and to decide on and deliver the strategic response. Government attention turned to fashioning a survivable computer network linking the Pentagon and other national decisionmakers in Washington with the Cheyenne Mountain nuclear command and control center and the headquarters of the Strategic Air Command.[4]

“The work on ARPANET called attention to the vulnerability of the nation's strategic communications infrastructure.”

The Chairman of the Board of Visitors at the Joint Military Intelligence College, Dr. Anthony Oettinger, has written of the Information Technology/Internet era: "What it all boils down to is that faster, smaller, cheaper electro-optical digital technologies have put into our hands enormously powerful and varied, yet increasingly practical and economical, means for information processing, means that stimulate us to re-examine everything we do to information and with information, and then choose to do nothing, to reinforce the old ways, to modify them, or to abandon them altogether in favor of altogether new ways."[5] For US intelligence, it is increasingly an era of modifications and altogether new ways. The technologies supporting US intelligence develop in "Web years," with three months to the Web year. The year 2010 is 28 Web years away.

Intelink

If we are to consider key aspects of the play of intelligence in the Internet era, we should bear in mind at the outset that the US Intelligence Community has developed and implemented its own highly advanced, ever-evolving "intranet"—Intelink—which is a secure collection of networks employing Web-based technology and using standard Web browsers such as Navigator and Internet Explorer. Intelink applies advanced network technology to the collection, analysis, production, and dissemination of classified and unclassified multimedia data across the Intelligence Community.[6]

---

[3] "The Birth of Internet," Leonard Kleinrock, accessed on 2 April 2002 <http://www.lk.cs.ucla.edu/LK/Inet/birth.htm>.

[4] "The Living Internet," DARPA, accessed on 2 April 2002: <http://www.living-internet.com/i/ii_darpa.htm>, p.1.

[5] Benjamin M. Compaine and William H. Read, eds., *The Information Resources Policy Handbook* (Cambridge, MA: The MIT Press, 1999), p. 22.

[6] Fredrick Thomas Martin, *TOP SECRET INTRANET* (Upper Saddle River, NJ: Prentice Hall, 1999), pp. 6-7.

In the assessment of the former Deputy Director of Central Intelligence, Adm. William O. Studeman: "Application of evolving Internet technologies to intelligence applications in the form of Intelink has been a transcendent and farsighted strategy. . . . Its future application requirements parallel those of the global Internet, so that there is the expectation that, for continuing modest investment, intelligence can continue to ride the wave of Internet growth, with commensurate access to amazing and relevant commercial off-the-shelf (COTS) developments."[7]

The Intelink intranet provides connectivity to national, theater, and tactical levels of government and military operations. Taking into account the sensitivity of some of the intelligence data involved, the sensitivity of the sources and methods for acquiring such data, and the resulting "need to know" of those logging on the system, Intelink provides several separate classification families, and forms of services:

- Intelink-SCI, which operates at the Top Secret/Compartmented intelligence level.
- Intelink-PolicyNet, run by the Central Intelligence Agency as CIA's sole-source link to the White House and other high-level, intelligence consumers.
- Intelink-S, the SIPRnet at the Secret level—the main communications link for the military commands and those operating on land, sea, and air.
- Intelink Commonwealth, or Intelink-C, linking the United States, the United Kingdom, Canada, and Australia.[8]

"The US Intelligence Community has developed and implemented its own highly advanced, ever-evolving "intranet"—Intelink."

A steadily evolving suite of Intelink support services is available, including collaborative tools, search tools, and search engines. Multi-layered, comprehensive Intelink security policies and practices reserving the intranet for authorized users include encryption, passwords, user certifications, and audits.

In positioning itself for the Internet era, the Intelligence Community has gone beyond innovative use of the Worldwide Web and its engines, to the CIA's creation in 1999 of a private, not-for-profit company, In-Q-Tel, dedicated to spurring the development of information technologies to be used in the safeguarding of national security. As stated on In-Q-Tel's web page, " . . . the blistering pace at which the IT [information technology] economy is advancing has made it difficult for any government agency to access and incorporate the latest in information technology. In-Q-Tel strives to extend the Agency's access to new IT companies, solutions, and approaches to address their priority problems."[9]

By investing in technologies that can benefit the CIA and the rest of the US Intelligence Community at the same time that they become available commercially, In-Q-Tel underscores the value of such IT functions as data warehousing and mining, the profiling of search agents, statistical data analysis tools, imagery analysis and pattern recognition, language translation, strong encryption, data integrity, and authentication and access control. In-Q-Tel's unclassified work with commercial potential includes attention to such issues as secure receipt of internet information, non-observable surfing, hacker resistance, intrusion detection, data protection, and multimedia data fusion and integration.[10]

New Objectives

What are the goals being laid out for US intelligence in the face of this on-rushing development and

---

[7] *Ibid.*, p. xliii.

[8] *Ibid.*, pp 53-56.

[9] "About In-Q-Tel," accessed on 2 April 2002: <http://www.In-Q-Tel.com/about.htm>.

[10] Rick E. Yannuzzi, "In-Q-Tel: A New Partnership Between the CIA and the Private Sector," *Defense Intelligence Journal*, Vol. 9, No. 1, Winter 2000, pp. 29-30.

implementation of information technology? For the Director of Central Intelligence, the goal is for the Intelligence Community to provide a decisive information advantage to the President, the military, diplomats, law enforcement, and the Congress. For the Chairman of the Joint Chiefs of Staff, the goal, as stated in Joint Vision 2010, is information superiority—*i.e.*, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[11]

The need for information superiority is, in many instances, causing US intelligence to take dramatically new approaches. The Internet era has become the Intelligence Community's new strength as well as its new challenge. Cold War assumptions driving intelligence collection and analysis—that enemy targets were closed societies and that superpower rivalry trumped all other issues—are assumptions of the past.

If the semaphore was the signals intelligence breakthrough at the time of Napoleon, the Internet and its communications channels are at the forefront of the signals intelligence challenges of the 21st century. With new transnational adversaries—international terrorists foremost among them—the flood of new information technologies, the easing of export controls on encryption technology, and global access to the Web, the National Security Agency (NSA) is charting new directions in the ways it identifies, gains access to, and successfully exploits target communications. It is also developing new ways of gauging our information security, given the openness of our society early in the cyber era, the global dimensions of that openness, and the enhanced exploitation capabilities that information technology and the Internet give our adversaries. NSA's Director, Lt. Gen. Michael Hayden, has placed this challenge in the following context: "Forty years ago, there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are over 180 million computers—most of them networked. There are roughly 14 million fax machines and 40 million cell phones, and those numbers continue to grow. The telecommunications industry is making a $1 trillion investment to encircle the world in millions of miles of high bandwidth fiber-optic cable."[12] At the same time, Gen. Hayden reminds, the new information technologies are an enhancement and an enabler, as NSA seeks outs and exploits the current era's targets.

> **"The Web . . . is an incredible enabler for an intelligence analyst, but at the same time a challenge with a thousand different shadings."**

Challenge to Analysts

The Web, with its related information technologies, is an incredible enabler for an intelligence analyst, but at the same time a challenge with a thousand different shadings, depending on the specific work of the analyst and the consumer being served. To cite an example, I draw on my experience as a policy-level consumer of intelligence.[13] As we pursued our nation's agenda with the USSR and the Warsaw Pact, we were dealing with closed societies. There was no Web. The information being volunteered by the USSR was not usually the information we required. Intelligence collection, analysis, and dissemination were geared to ascertaining the current state of play and estimating future developments behind the Iron Curtain. The role of the Intelligence Community's sovietologists, the analysts expert on the USSR,

[11] Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, DC: US Government Printing Office, 1996), p. 16.

[12] Lt. Gen. Michael V. Hayden, USAF, "Address to Kennedy Political Union of American University," 17 February 2000, p. 2.

[13] From 1974 to 1977, the author headed President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe.

was central. Not only could they divine the significance of any changes in the renowned line-up of the Soviet leadership atop Lenin's tomb, they often were the only source of information on developments of importance inside the Soviet Union.

Today, the analyst no longer sets the pace of the information flow. The sources of information now available to the policy-level consumer—whether dealing with the Russian Federation or with any of the remaining closed societies—are far, far greater than a quarter of a century ago. It is almost a given that today's policy-level consumer of intelligence is well informed in his or her area of interest and not dependent on an intelligence analyst for a continuing stream of routine, updating information. The Web, the media—electronic and hardcopy, US and foreign—the telephone, the fax, the interaction with US and foreign colleagues in the field, and intelligence reporting available at the touch of the Intelink keyboard all play a part.

It is not enough for today's analyst to have a sense of his or her consumer's level of knowledge of specific foreign issues. To provide value-added analysis, today's analyst must focus more sharply on the specific needs, and the best timing for meeting those needs, of the policy-level consumer. The analyst must seek specific tasking, analyze feedback from analysis already provided, and invite and tackle the consumer's hard questions demanding answers.[14]

"If the policy-level consumer is demanding in this new [IT] era, the military commander is more so."

Serving Military Needs

If the policy-level consumer is demanding in this new era, the military commander is more so. Since operations in the Balkans in the late 1990s, military commanders have been expecting the information superiority envisioned in Joint Vision 2010. The requirement, from mission planning through mission execution, is for intelligence to be able to locate and surveil targets—stationary or mobile, exposed or hidden—to obtain and provide to the commander a continuing picture of his entire field of operations in all its dimensions.

This extraordinary challenge requires intelligence to move fluidly among all levels—national, theater, and tactical. For any given requirement, the broadest capabilities of US intelligence are potentially available to contribute to the solution. Supporting today's commander requires a complex harnessing of collection, analysis, and dissemination across the disciplines of intelligence—imagery, measurements and signatures, signals, and human-source intelligence—to provide the best possible all-source intelligence products when and where needed.

Like Mount Everest, the challenge of providing such support to the military commander is there, and US intelligence is ascending, month after month, year after year; however, the summit has not been attained. Nonetheless, since the mid-1980s, the global reach of US intelligence has been strengthened by Intelink, by the accessibility of growing amounts of information in cyber databases, and by the near-real-time links of communications satellites. These capabilities have helped bring into being the Joint Worldwide Intelligence Communications System (JWICS) and the companion analyst's desktop Joint Deployable Intelligence Support System (JDISS). The JWICS system allows video teleconferencing, imagery transfer, electronic data transfer, publishing, and video broadcasting—all up to the highest levels of classification. The system, first tested in 1991, is

---

[14] See Carmen A. Medina, "The Coming Revolution in Intelligence Analysis: What To Do When Traditional Models Fail," *Studies in Intelligence*, Vol. 46, No. 3, 2002, pp. 23-28.

now installed at more than 125 defense and intelligence locations worldwide.

Lessons learned from US participation in the DESERT STORM operation that expelled Iraq from Kuwait in 1991 led to the creation of National Intelligence Support Teams (NISTs). NISTs are fast-response, rapidly deployable intelligence cells made up of personnel from CIA, NSA. DIA, and the National Imagery and Mapping Agency (NIMA). They are formally subordinate to the Chairman of the Joint Chiefs of Staff's Director of Intelligence, but when they deploy, they are attached to the commander in the field. The idea is to provide a Joint Task Force commander with the ability to reach back swiftly, efficiently, and expertly to the national-level agencies for answers to questions unanswerable in the field, and to receive warnings of threats that otherwise could not be received. Using light-weight, high-technology, multi-media communications flowing via Intelink and satellite, a NIST is able to bring the very best intelligence available to the commander in the field.[15] Truly, the NIST is a remarkable advance in intelligence doctrine and methodology in the Internet era.

"The Internet era challenges the Intelligence Community to set aside old practices in favor of dramatically new ways of doing business."

I have mentioned, more than once, the national, theater, and tactical levels. The world of the analyst in the Internet era is one in which collection, analysis, and dissemination of the analytic product are no longer restricted to flowing up and down hierarchical lines but can move horizontally and diagonally to selected nodes of the global intranet. The expert at the Joint Intelligence Center/Pacific in Hawaii, for example, may be in Intelink contact routinely with counterparts in a carrier battle group in the Indian Ocean and at the National Military Joint Intelligence Center in the Pentagon.

Looking Ahead

Collaborative tools using commercial web technologies are being developed through the Joint Intelligence Virtual Architecture program to assist today's analyst in locating and accessing valuable data, assessing such data, producing an informed analytic product, and moving that product to where it will be of value. Such tools, for example, provide search and discovery protocols allowing the automatic extraction of relevant data from classified and unclassified sources. This data mining can be applied not only to data from sources that the analyst already values, but also to new sources that might be of importance. Such tools can also support the analyst in making rapid assessments and developing time-critical reporting using streaming media, such as video and audio tapes.

If a commander is to have a continuing picture of his or her entire field of operations, adding the enabling strengths of Web-based information technology to the analyst's kit is of importance for military intelligence, too. New tools are of vital importance for analysts addressing asymmetric threats such as terrorism, where disparate data must be located and mined, not only from classified and unclassified intelligence sources, but also from worldwide open sources. And all must be accomplished in collaboration with the FBI, INS, Customs, and law enforcement, both US and international.

In 1899, Commissioner of Patents Charles Duell urged President William McKinley to abolish the Patent Office saying: "Everything that can be invented

---

[15] James M. Lose, "National Intelligence Support Teams," *Studies in Intelligence*, Winter 1999-2000, Unclassified Edition, pp. 87-88.

has been invented." Those fearless words have always appealed to me, as have those of Dr. Dionysus Lardner, who in 1823 advised that: "Rail travel at high speed is not possible because passengers, unable to breathe, would die of asphyxia."[16]

I quote these gentlemen to remind that we cannot begin to imagine or comprehend where the onward march of discovery and technology will take us in the decades ahead. These words offer a snapshot of the remarkable doors that the Internet has opened and the formidable new challenges that the Internet era poses for the work of intelligence. It is an era in which the US Intelligence Community continues to set aside old practices in favor of dramatically new ways of doing business. This comes at a time when both decisionmakers and military commanders recognize the heightened priority and the central importance of good intelligence in providing for the well being, the security, and the defense of the United States.

[16] Norman R. Augustine, "Socio-engineering (And Augustine's Second Law Thereof)," lecture presented at the University of Colorado Engineering Centennial Convention, 1 October 1993, p. 1.