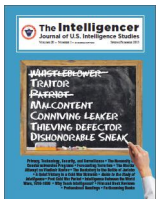


From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 20 • NUMBER 1 • $15 SINGLE COPY PRICE Spring/Summer 2013

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: www.afio.com, E-mail: afio@afio.com

Guide to the Study of Intelligence

Intelligence in the Post-Cold War Period

— Part II — The Impact of Technology

by Stephen H. Campbell, B.Sc., M.A.L.D.

The first part of this article explored how changes in geopolitics and economics have affected intelligence since the end of the Cold War. The implosion of the world's second superpower and the forces of globalization, however, have only so much explanatory power. In the two decades since the end of the Cold War, advances in technology have played a significant role in transforming the world of intelligence both externally (the threat environment) and internally (the intelligence process).

Technology has empowered adversaries with the ability to form virtual communities that erode state power. It has enabled the theft of secrets and the proliferation of dangerous knowledge over vast distances. Governments no longer have a monopoly over information. Secrets are harder to keep than ever before. At the same time, technology has made the dream of near real-time fusion of intelligence come true. It has revolutionized tradecraft. And it continues to hold out the promise of being able to detect dangerous substances.

This article explores these changes thematically, by examining the fields of imagery and geospatial technology, materials and weapons science, and information and communication technology, respectively.

IMAGERY AND GEOSPATIAL TECHNOLOGY

Advances in technology have enabled imagery to play a crucial role in tactical battlefield support, in contrast to the largely strategic role it played during the Cold War.[1] At the same time, the fusion of real-time imagery, GPS data and digital maps into Geographic Information Systems has forged a new discipline – "geospatial intelligence" – thereby revolutionizing military command and control.[2]

The Gulf War in 1991 heralded these changes with the use of unmanned aerial vehicles for reconnaissance, the first large-scale use of precision-guided munitions (PGMs), and the tactical use of radar from satellites and new JSTARS aircraft.[3] The war had a profound impact. Adversaries could not tackle the US on its own terms. US airpower drove Chinese war planners to put C4ISR at the heart of their military modernization strategy.[4] China and others began to move their weapons of mass destruction (WMD), missiles and military leadership underground.[5]

Compared to the Cold War, when satellites tracked targets such as airfields and warships, post-Cold War foes were low-contrast.[6] Satellites had trouble identifying an arms deal in a village square, a small fast-moving convoy of terrorists in the desert, or a training camp consisting of little more than tents and rifle ranges.[7] Military commanders turned to aerial

1. IMINT was critical to keeping the Cold War "cold." It kept a close eye on the stockpiles of Soviet missiles, helped to dispel the bomber and missile "gaps," and enabled the verification of arms control treaties. John M. Diamond, "Re-examining Problems and Prospects in U.S. Imagery Intelligence," *International Journal of Intelligence and Counterintelligence*, 14:1, Spring 2001.

2. Mark W. Corson and Eugene J. Palka, "Geotechnology, the U.S. Military, and War," in Brunn, Cutter and Harrington (Eds.), *Geography and Technology* (Dordrecht: Kluwer Academic Publishers, 2004).

3. PGMs accounted for 9% of weapons deployed in Desert Storm (Iraq, 1991). This increased to 29% in Allied Force (Kosovo, 1999) and to 70% in Enduring Freedom (Afghanistan, 2001). Ibid; Benjamin S. Lambeth, *Air Power Against Terror. America's Conduct of Operation Enduring Freedom* (Santa Monica, CA: RAND, 2005), xxii.

4. C4ISR stands for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance. For the Chinese the Gulf War "changed the world." There would be no repeat of the Red Army victories of the 1950s. PLA strategy evolved to combine network and electronic warfare against an adversary's information systems at the start of any conflict. Joel Brenner, *America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 120, 135; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington, DC: US-China Economic and Security Review Commission, 2012).

5. Jeffrey T. Richelson, "Unearthing Secrets," *C4ISR Journal*, August 1, 2008; W. Happer et. al., *Characterization of Underground Facilities* (McLean, VA: Mitre Corporation, 1999).

6. Michael T. Flynn, Rich Juergens, and Thomas L. Cantrell, "Employing ISR. SOF Best Practices," *Joint Forces Quarterly*, Issue 50, 3rd quarter 2008.

7. Patrick Radden Keefe, "A Shortsighted Eye in the Sky," *The New York Times*, February 5, 2005.

surveillance, increasingly unmanned, relying on satellites more for navigation and secure communication.[8] Full motion video sensors were introduced on UAVs in the Balkans in 1995, bringing improved spatiotemporal awareness.[9] A decade later this capability was honed in the US Army's "Constant Hawk" program to enable forensic backtracking of IED attacks in Iraq.[10]

A major development has been the arming of UAVs. Frustrated by the ineffectiveness of cruise missile strikes in retaliation for the 1998 Al Qaeda bombings in East Africa, the CIA and the US Air Force cooperated after 9/11 to arm the Predator UAV with Hellfire missiles.[11] Armed UAVs remove the "organizational blink" between sensors and shooters.[12] Primed by laser designators, armed UAVs reduced the sensor-shooter-cycle to an average of 20 minutes in Operation Enduring Freedom.[13] By the end of the decade drones had killed many of the CIA's most wanted high-value individuals.[14]

MATERIALS AND WEAPONS SCIENCE

Officially recognized by the US IC in 1986,[15] "Measurement and Signatures Intelligence" (MASINT) is the "CSI" of intelligence.[16] Like imagery intelligence, advances in technology have enabled MASINT to play a much more tactical role than it played during the Cold War.[17] Newer sensors equipped with miniaturized on-board processors and signature databases now enable near-instantaneous identification of battlefield entities.[18] Positive identification occurs at the sensor location, not in a laboratory thousands of miles from the operation.[19]

There have been particular advances in "imagery-derived MASINT."[20] Hyper-spectral remote sensing, developed in the 1980s,[21] has become important in supporting special operations, and in countering camouflage, narcotics, and proliferation.[22] Night-vision technology has given advantage to regular forces during desert operations and to special forces during raids.[23] And laser intelligence has become integral to the US Air Force's "kill chain."[24] In particular, the use of laser designators by forward air controllers to "paint" targets for laser-seeking missiles has had a profound effect on air-ground warfare in the new century.[25]

8. There are large, medium and small Unmanned Aerial Vehicles (UAVs). Large UAVs such as the Global Hawk are designed for long-term surveillance and are launched from air force bases. Medium UAVs such as the Predator and Reaper are designed for tactical surveillance and reconnaissance and require a runway for launch. Small UAVs such as the Raven are designed for tactical, over-the-hill visibility and can be launched by hand. Richard Best, Jr., *ISR Acquisition: Issues for Congress* (Washington, DC: Congressional Research Service, 2010).

9. Timothy R. Uecker, *Full Motion Video (FMV): The New Dimension of Imagery* (Maxwell AFB, AL: Air University, 2005).

10. Evan C. Dertien and Eric J. Felt, *Persistent Surveillance: Maximizing Airpower Effectiveness in Irregular Warfare* (Maxwell AFB, AL: Air University, 2007), 11.

11. Jeffrey T. Richelson, "Technical Collection in the Post-September 11 World," in Gregory F. Treverton, and Wilhelm Agrell, *National Intelligence Systems: Current Research and Future Prospects* (New York: Cambridge University Press, 2009).

12. Flynn, Juergens, and Cantrell, "Employing ISR. SOF Best Practices."

13. Anthony H. Cordesman, *The Lessons of Afghanistan: War Fighting, Intelligence, and Force Transformation* (Washington, DC: CSIS, 2002), 66.

14. Peter Bergen and Katherine Tiedemann, *The Year of the Drone. An Analysis of U.S. Drone Strikes in Pakistan, 2004-2010* (Washington, DC: New America Foundation, 2010).

15. John D. Macartney, "John, How Should We Explain MASINT?" *Intelligencer* 12, Summer 2001.

16. MASINT is based on "technically-derived measurements of physical phenomenon intrinsic to an object or event." David Bunker, Air Force Institute of Technology, *What is MASINT?*, March 2009; DoD Instruction 5105.58, *Measurement and Signature Intelligence* (MASINT), April 22, 2009.

17. Typical Cold War targets were submarines (acoustic) and nuclear tests (seismic). Most MASINT analysis required sophisticated database lookups and signature matching that took too long for use in tactical settings. Macartney, John, "How Should We Explain MASINT?."

18. William K. Moore, "MASINT: New Eyes in the Battlespace," *Military Intelligence*, Vol. 29, Jan-Mar 2003.

19. Ibid.

20. Sometimes now called "Advanced Geospatial Intelligence." National Geospatial Intelligence Agency, *National System for Geospatial Intelligence. Geospatial Intelligence (GEOINT) Basic Doctrine*, September 2006, 45.

21. The technology was pioneered by the Jet Propulsion Laboratory and enables collection from 200 or more spectral regions. James B. Campbell and Randolph H. Wayne, *Introduction to Remote Sensing*, Fifth Edition (New York, Guildford Press, 2011), 15-16.

22. Jeffrey T. Richelson, "MASINT The New Kid in Town," *International Journal of Intelligence and Counterintelligence*, 14:2, Summer 2001.

23. The technology was advantageous to US forces operating in the desert during the Gulf War. It has been pivotal in night raids against terrorists and insurgents since 9/11. Advances included improved image intensification and resolution using gallium arsenide photocathodes. US Army Night Vision and Electronic Sensors Directorate, *History*, *www.nvl.army.mil*, accessed May 8, 2012; Mark Urban, *Task Force Black. The Explosive True Story of the SAS and the Secret War in Iraq* (London: Little Brown, 2010).

24. Lambeth, *Air Power Against Terror*.

25. During Operation Enduring Freedom, the invisible laser beams emanating from the SOFLAM, or Special Operations Forces Laser Acquisition Marker, became known to Taliban and Al-Qaeda forces as the "Death Ray." Robin Moore, *The Hunt for Bin Laden. Task Force Dagger. On the Ground with the Special Forces in Afghanistan*, (New York: Ballantine Books, 2003), 2-5; Stephen Biddle, *Afghanistan and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle, PA: Strategic Studies Institute, 2002).

However, despite significant research, the promise of new methods of unambiguously detecting and characterizing lethal (CBRNE)[26] materials has not yet been realized. Controversy ensues when force is used preemptively, such as the US bombing of a pharmaceuticals factory in 1998 in Sudan, based on seemingly incomplete intelligence.[27] The identity of perpetrators, for example of the anthrax attacks in the US in October 2001, remains inconclusive.[28] New detectors at borders have been withdrawn for being too slow or producing too many false alarms.[29] Advances in cosmic ray and particle physics have yet to be incorporated into nuclear detectors.[30] And with the exception of robotics,[31] none of the exotic new technologies has yet been able to deliver standoff detection of improvised explosive devices.[32]

Some incremental improvements have been made. Polymerase chain reaction (PCR) technology, invented in 1983,[33] has become the standard method for detecting biological agents.[34] The technique was adopted by UN inspectors in 1996 to overcome Iraqi denial of its anthrax program,[35] and has since evolved to enable near "real-time" identification of pathogens.[36] Nevertheless most biological agents are colorless, odorless, do not exhibit a signature that can be remotely sensed,[37] and can easily be hidden.[38] Planners therefore regard pre-attack surveillance as unrealistic, and have instead designed systems such as BioWatch to provide warning of an attack in progress.[39]

While not officially a MASINT discipline, the science of identifying individuals has evolved significantly in the past twenty years. Before the introduction of digitized biometrics, criminals, terrorists and insurgents could hide behind a web of multiple iden-

26. Chemical, biological, radiological, nuclear and explosives.

27. A soil sample taken near the factory by a CIA agent was found to contain trace amounts of a chemical used in the production of VX nerve gas. Media reports suggested that the chemical could be the byproduct of the breakdown of an agricultural insecticide. Gregory Koblentz, "Countering Dual-Use Facilities: Lessons from Iraq and Sudan," *Jane's intelligence Review*, 11:3, March 1, 1999.

28. Following the attacks, the FBI launched one of the most expensive and manpower-intensive investigations in its history. Although it was able to match the anthrax to cultures in a flask belonging to US Army scientist Bruce Ivins, the FBI's genetic analysis "did not definitively demonstrate" that the mailed anthrax spores were grown from Dr. Ivins' flask, according to a review by the National Academy of Sciences. Scott Shane, "Colleague Disputes Case Against Anthrax Suspect," *The New York Times*, April 22, 2010; Scott Shane, "Expert Panel is Critical of F.B.I. Work in Investigating Anthrax Letters," *The New York Times*, February 15, 2011.

29. The Obama administration quietly cancelled programs promoting the Advanced Spectroscopic Portal and the Cargo Advanced Automated Radiography System. In Los Angeles there were hundreds of false alarms per day, set off by Chinese toilets, granite countertops and bananas. David E. Sanger, "Nuclear-Detection Effort is Halted as Ineffective," *The New York Times*, July 29, 2011; Mickey McCarter, "DHS Cancels Next Generation Radiation Portal for Cargo Screening," *Homeland Security Today*, July 27, 2011.

30. For example, scientists are working on a transportable high energy linear accelerator that is apparently able to stimulate fission and detect "special nuclear material" from distances of 200 meters or more; "muon radiography" promises to penetrate shielding and detect dense, fissile material without being hazardous to human beings; and new superconducting "transition-edge" sensors are reputed to be so sensitive that they are able to overcome the false alarm problem. To bring these technologies from the lab into the field, engineers will need to overcome problems of size, cost, safety and power consumption. Jonathan Medalia, *CRS, Detection of Nuclear Weapons and Materials: Science, Technologies, Observations*, June 4, 2010; Kent D. Irwin, "Seeing with Superconductors," *Scientific American*, November, 2006.

31. Robots used in Iraq and Afghanistan such as the "PackBot" have come a long way since British forces first used a converted lawnmower in Ireland in the 1970s to defuse bombs. P.W. Singer, "War of the Machines," *Scientific American*, July, 2010; David Dugan, *Bomb Squad*, PBS Documentary, October 1997.

32. Despite investment in an array of new approaches, both trace detection (e.g. Laser-Induced Breakdown Spectroscopy, Raman Spectroscopy and Differential Reflection Spectroscopy) and bulk detection (e.g. Neutron, Nuclear Quadrupole Resonance and Millimeter/Terahertz sensors), few standoff techniques are able to detect explosives unambiguously and consistently at a distance of more than 10 meters. Detection at distances of 100 meters or more is beyond current science and technology concepts. Thus anomaly detection is still performed by visual observation, radar, infrared or canine detection (the most effective). John E. Parmeter, "The Challenge of Standoff Explosives Detection," *Proceedings of the 38th Annual International Carnahan Conference on Security Technology*, October 2004; Maurice Marshall and Jimmie C. Oxley (Eds.), Aspects of Explosives Detection (Amsterdam: Elsevier, 2009); Rowan Scarborough, "Pentagon may trim IED detector budget," *Washington Times*, September 7, 2010.

33. John M. S. Bartlett and David Sterling, "A Short History of the Polymerase Chain Reaction," *Methods in Molecular Biology, PCR Protocols*, Vol. 226, 2003.

34. Simon Labov and Tom Slezak, "The Indispensable Technology: Detectors for Nuclear, Biological, and Chemical WMD," in Stephen M. Maurer, *WMD Terrorism. Science and Policy Choices* (Cambridge, MA: MIT Press, 2009).

35. Using PCR inspectors found anthrax on equipment that had previously tested negative. Gregory Koblentz, *Living Weapons. Biological Warfare and International Security*, (Ithaca, NY: Cornell University Press, 2009), 98.

36. A process that used to take 6 to 12 hours in the laboratory now takes 20 to 40 minutes using portable DoD field kits. Jonathan Beard, "Overview of DARPA's Biological Warfare Defense Programs," in DARPA, *DARPA: 50 Years of Bridging the Gap*, (Arlington, VA: DARPA, 2008); Zygmunt F. Dembek (Ed.), *Medical Aspects of Biological Warfare*, (Washington, DC: Borden Institute, 2007), 404.

37. Robert M. Clark, *The Technical Collection of Intelligence* (Washington, DC; CQ Press, 2011), 13.

38. Labov and Slezak, "The Indispensable Technology."

39. BioWatch is a program operated by the Department of Homeland Security (DHS) in 30 cities in the United States designed to detect a biological attack. Ibid.

tities when they traveled.[40] The introduction of digital photographs and fingerprinting in programs such as US-VISIT has made such dissemblance much harder.[41] Similarly the introduction of handheld systems for collecting biometrics has proven vital to holding territory gained in counterinsurgencies.[42] Correlation of fingerprints collected abroad with databases used by US immigration has exposed high-profile terrorists and prevented enemies of the US from entering the country.[43] And "latent fingerprints" have been used by forensic scientists to track down bomb makers.[44]

DNA profiling, invented in 1983, has had a big impact on forensics, enabling the resolution of thousands of criminal cases.[45] Even without a precise match, "ancestral typing" and "familial DNA testing" have been used to track down serial killers and rapists.[46] DNA has been used to identify both the perpetrators and the victims of terrorist attacks.[47] It has also been used to confirm the identities of high value individuals killed in "targeted killings."[48]

INFORMATION AND COMMUNICATION TECHNOLOGY

At its core intelligence is about acquiring and processing information, much of it from communication, so the revolution in information and communication technology (ICT) has had a most profound effect on the intelligence world.

The External Impact of ICT

The internet has added a new "cyber" domain to the existing contested spaces of air, space, land and sea.[49] This seemingly benign communications medium[50] has altered the threat environment in several ways. Firstly, it has enabled a new form of sabotage. Cyber weapons can disrupt the command and control systems of decision-makers, as the Russian attacks on Estonia and Georgia in 2007 and 2008 demonstrated.[51] Or they can disrupt industrial control systems, as the sophisticated "Stuxnet" attacks on Iranian centrifuges

40. For example, the 19 hijackers from 9/11 used 364 aliases in their forms of identification, including different spellings of their names and "noms de guerres." At the time visa screening systems at consular offices was based on simple name checks. National Commission on Terrorist Attacks Upon the United States, *Monograph on 9/11 and Terrorist Travel*, August 2004.

41. Rey Koslowski, *Real Challenges for Virtual Borders: The Implementation of US-VISIT* (Washington, DC: Migration Policy Institute, 2005).

42. For example, in 2003 the Department of Defense began to collect biometrics in Iraq using systems such as the Biometric Automated Toolset and the Handheld Interagency Identity Detection Equipment. After the Marine Corps captured the town of Fallujah, the Marines issued identity cards with iris scans to the population, effectively walling off the city and making it difficult for insurgents to reestablish themselves. Jody Kieffer and Kevin Trissell, "DOD Biometrics – Lifting the Veil of Insurgent Identity," *US Army Acquisition, Logistics & Technology*, April-June 2010.

43. For example, Mohamed al Kahtani was identified as the possible "20th hijacker" after he was captured in Afghanistan in December 2011. His fingerprints matched those of a man who was denied entry on August 3, at Orlando International Airport, where cameras captured Mohamed Atta, apparently waiting to pick him up. Hundreds of Iraqis have been denied US visas when their fingerprints have turned up in the DoD database of known insurgents. John D. Woodward, Jr., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism," *Military Review*, Sept-Oct, 2005; Ellen Nakashima, "Post-9/11 Dragnet Turns Up Surprises," *The Washington Post*, July 6, 2008.

44. Increasingly counterinsurgents perform the job of police investigators to collect evidence essential to the prosecution of captured personnel. The FBI set up the Terrorist Explosives Device Analytical Center in 2003 to handle the analysis of "latent fingerprints" found on IEDs. Within its first 5 years the center identified 56 bomb makers. Alan T. Ivy and Kenneth J. Hurst, *Formalizing Law Enforcement Procedures for DoD Units Conducting Combat Operations* (Quantico, VA: Marine Corps War College, 2008);

45. English geneticist Alex Jeffreys first used DNA in 1983 as a means of establishing personal identity. Sheldon Rimsky and Tania Simoncelli, *Genetic Justice. DNA Data Banks, Criminal Investigations, and Civil Liberties* (New York: Columbia University Press, 2011), 48.

46. In 2003, for example, the Baton Rouge serial killer was tracked down with the help of genetic ancestral typing. In 2006 the Deare Valley Shoe Rapist in Yorkshire, England, was tracked down via his sister, who had a drunk driving conviction, through familial DNA testing. Ibid, 66-67, 92-93; Dov Fox, "The Second Generation of Racial Profiling," *American Journal of Criminal Law*, Vol. 38, 2010.

47. For example, starting in the late 1980s the Royal Ulster Constabulary Special Branch was able to use DNA from hair follicles at bombing scenes to track down and incriminate members of the Provisional IRA. And as of February 1, 2009, 1,654 remains of those killed at the World Trade Center on 9/11 had been linked by DNA to known individuals. Tony Geraghty, *The Irish War*, 2000, 83-89; Office of the Chief Medical Examiner, New York, *Update on the Results of DNA Testing of Remains Recovered at the World Trade Center Site and Surrounding Area*, February 1, 2009.

48. The most famous example was the use of DNA to confirm the death of Osama bin Laden. Peter L. Bergen, *Manhunt. The Ten-Year Search for bin Laden from 9/11 to Abbottabad* (New York: Crown Publishers, 2012), 227, 242.

49. Rebecca Grant, *Victory in Cyberspace* (Arlington, VA: Air Force Association, 2007).

50. Frederick L. Wettering, "The Internet and the Spy Business," *International Journal of Intelligence and Counterintelligence*, 14:3, 2001.

51. The Russian attacks used a brute force method called "distributed denial of service" (DDOS). Hackers used DDOS in 2007 to shut down government ministries and banks after the Estonians announced plans to move a WWII memorial to their Russian "liberators." The following year the Russians used DDOS again to bring down Georgia's communications network to confuse the leadership as Russian troops entered the country. Joel Brenner, *America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 39-40.

by the US and Israel revealed in 2010.[52] Secondly, the new domain has enabled the mobilization of de-territorialized communities capable of challenging state and religious authority.[53] Thirdly, cyberspace has become a virtual sanctuary for terrorists and insurgents, a place where they can raise funds, recruit and educate members, plan and launch attacks, and publicize the results with impunity.[54] And lastly, it has created a "spy heaven" for malicious actors who steal massive quantities of data while remaining anonymous and hard to detect.[55]

The cyber domain has created an enormous target for criminals. The US, for example, spends in excess of $400B annually on R&D, the largest by far in the developed world.[56] Since much of the intellectual property from this investment is now stored on networked computers, US competitive advantage gained from years of research can vanish instantly.[57] The internet has enabled sophisticated remote theft.[58] Data can be acquired through pre-installed "trapdoors," "Trojan Horse" attacks, or direct "hacking" that exploits known system vulnerabilities.[59]

In the post-Cold War period Chinese actors have become "the world's most active and persistent perpetrators of economic espionage,"[60] and have amassed an impressive array of US defense technologies through espionage.[61] Chinese success is due to long-term planning, extensive grant-funded research and a huge pool of recruits.[62] While the Chinese rely on their network of émigrés for much of their military espionage,[63] they have increasingly turned to cyberspace for economic

52. The attack took out nearly 1,000 centrifuges through alternate acceleration and deceleration. It sent signals to the Natanz control room indicating normal operation. The result was a delay in the Iranian nuclear program of at least a year and a half. Spearheaded by US Strategic Command, the operation was called "Olympic Games." It was approved by President Bush in 2006 and continued by President Obama in 2008. The code was designed by the NSA in cooperation with Israeli intelligence, including Unit 8200. Due to a programming error it leaked onto the internet in 2010. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012.

53. For a general discussion see the trilogy by Manuel Castells, *The Information Age: Economy, Society and Culture* (Malden, MA: Blackwell Publishing, 2009-2010); for the impact of migration and the internet on political Islam see Olivier Roy, *Globalized Islam. The Search for a New Ummah* (New York: Columbia University Press, 2004) and Gary R. Bunt, *Islam in the Digital Age. E-Jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Press, 2003).

54. Magnus Ranstorp, "The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalization," in Johan Eriksson and Giampiero Giacomello (Eds.), *International Relations and Security in the Digital Age* (New York: Routledge, 2007); Gabriel Weimann, *Terror on the Internet. The New Arena, the New Challenges* (Washington, DC: US IOP, 2006).

55. Wettering, "The Internet and the Spy Business"; Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009 – 2011*, October 2011.

56. National Science Board, *Science and Engineering Indicators 2012* (Arlington, VA: National Science Foundation), 4-41.

57. Intellectual property has become a critical "factor of production" in post-industrial economies. Susan W. Brenner and Anthony C. Crescenzi, "State-Sponsored Crime: the Futility of the Economic Espionage Act," *Houston Journal of International Law*, Volume 389, 2006; Andrew Rathmell, "Towards Postmodern Intelligence," *Intelligence and National Security*, 17:3, 2002.

58. Individual computers, of course, have always been subject to physical theft or borrowing (so-called "black jobs"). What makes internet espionage so effective is that the theft is achieved by "recruiting" operating systems, word processors or even firewalls with access to the information needed. Wettering, "The Internet and the Spy Business"; James R. Gosler, "The Digital Dimension," in Jennifer E. Sims and Burton Gerber (Eds.), *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005).

59. Ibid; for an introduction to cyber-theft see Joel McNamara, *Secrets of Computer Espionage: Tactics and Countermeasures* (Indianapolis, IN: Wiley Publishing, 2003); for a more advanced up-to-date survey see Stuart McClure, Joel Scambray and George Kurtz, *Hacking Exposed 7 Network Security Secrets & Solutions* (Emeryville, CA: McGraw-Hill Osborne Media, 2012).

60. Although many of the perpetrators are not government agencies, the PRC is clearly involved. State Department cables published by WikiLeaks in 2010 revealed that "Operation Aurora" had been directed by a senior member of the Politburo. The operation involved the cyber-theft of intellectual property from Google and thousands of other well-known US and European companies. Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*; Kim Zetter, "Report Details Hacks Targeting Google, Others," *Wired Magazine*, February 3, 2010; James Glanz and John Markoff, "Cables Discuss Vast Hacking by a China Fearful of the Web," *New York Times*, December 4, 2010; both cited in Brenner, *America the Vulnerable*, Chapter 3, "Bleeding Wealth."

61. China's triumphs include acquisition of design blueprints for the US built B-1 bomber, Northrop Grumman's B-2 stealth bomber, the US Navy's Quiet Electric Drive system and the W-88 miniature nuclear warhead. Joseph Fistanakis, "Is China the New Spy Superpower?," *Intel News*, December 16, 2011.

62. Until the 1980s the Chinese regime's spying was largely domestic in nature. But in the post-1980s era, as China increased its economic activity abroad, its Ministry of State Security began to focus on foreign commercial secrets, while the People's Liberation Army started acquiring foreign technology, much of it for weapons and military systems. The PRC uses at least five national grant programs to fund research related to information warfare: the 863 National High Technology R&D Program, the 973 National Key Research Program, the National 242 Information Security Program, the Ministry of State Security 115 Program, and the National 219 Information Security Application Demonstration Project. "China's Growing Spy Threat," *The Diplomat*, September 19, 2011; Peter Mattis, "Assessing the Foreign Policy Influence of the Ministry of State Security," *China Brief*, 11:1, January 14, 2011; Bill Gertz, "Chinese Spy Who Defected Tells All," *The Washington Times*, March 19, 2009; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington, DC: US-China Economic and Security Review Commission, 2012), 59-63.

63. Paul D. Moore, "How China Plays the Ethnic Card," *The Los Angeles Times*, June 24, 1999.

espionage.[64]

Information technology has eroded the monopoly that government agencies once enjoyed over intelligence. Public access to internet, database and search engine technology means that government analysts now have to compete with the media, academics and NGOs.[65] Of course, satellite and internet technologies from their earliest days have been exploited for commercial gain.[66] What is remarkable in the post-Cold War period is that commercial forces have driven the democratization of specific technologies such as satellite imagery and encryption hitherto reserved exclusively for the secret world of intelligence.[67] While such deregulations benefit millions, terrorists can now make full use of Google Earth and encrypted Voice over Internet Protocol (VoIP) to mount attacks.[68]

Democratization of ICT has increased transparency, making secrets harder to keep and intelligence agencies less effective.[69] In 2010 a young Army intelligence analyst working in Baghdad downloaded more than a quarter of a million US diplomatic cables and passed them to the whistle-blowing group WikiLeaks.[70] This incident, possibly the most massive unauthorized disclosure of classified documents in American history, illustrates the degree to which technology has turbocharged espionage.[71]

To be sure, technology has not been the only driver of transparency. Higher expectations concerning accountability,[72] and the need to preempt today's threats force agencies into the open.[73] When transatlantic flights are cancelled or armed police storm a private residence, liberal democratic publics want an explanation.[74] International politicians must also justify the preemptive use of force by revealing intelligence. Colin Powell's dramatic presentation at the UN in February 2002 was simply a global example of the public use of intelligence in a post-9/11 world.[75]

The Internal Impact of ICT

ICT has fundamentally reshaped the intelligence process. Advocates in the late 1990s suggested replacing the industrial-age assembly line model with a new information-age network approach.[76] The key was to

64. A report in 2009 determined that electronic media were involved in all ten recent cases involving foreign economic espionage that led to indictments, mostly involving Chinese companies. Derrick Spooner, Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzceciak, *Spotlight on Insider Theft of Intellectual Property Inside the U.S. Involving Foreign Governments or Organizations* (Pittsburgh, PA: Carnegie Mellon University CERT Program, 2009).

65. Policymakers are no longer living in an age of information scarcity. They no longer require their intelligence service to tell them what is going on in the world or how to interpret events, and they can no longer assume that proprietary intelligence is superior to open sources. Example: NGOs offering OSINT assessments include UK-based Oxford Analytica, Jane's Information Group, the International Institute for Strategic Studies, and Stratfor. Wesley K. Wark, "Learning to Live with Intelligence," *Intelligence and National Security*, 18:4, December 2003; Carmen A. Medina "What to Do When Traditional Models Fail. The Coming Revolution in Intelligence Analysis," *Studies in Intelligence*, 46:3, 2002; Alan Dupont, "Intelligence for the Twenty-First Century," *Intelligence and National Security*, 18:4, 2003.

66. The US launched the CORONA imagery and GRAB electronic intelligence satellites in 1960. AT&T followed by launching the first commercially funded communications satellite called "Telstar" in 1962. Robert A. McDonald and Sharon K. Morena, *Raising the Periscope. Grab and Poppy: America's Early ELINT Satellites* (Chantilly, VA: NRO, 2005); Air Command and Staff College, *AU-18 Space Primer* (Maxwell AFB, AL: Air University Press, 2009).

67. In the early 1990s the US Congress passed legislation permitting private companies to operate satellites and sell high-resolution images on the global market. In the late 1990s intelligence and law enforcement agencies in the west also lost a complex battle in which high-grade encryption became available to private organizations and individuals. John C. Baker, *Trading Away Security? The Clinton Administration's 1994 Decision on Satellite Imaging Exports* (Washington, DC: Institute for the Study for Diplomacy, 1997); Aldrich, "Beyond the Vigilant State," *Review of International Studies*, 35:4, 2009; Whitfield Diffie and Susan Landau, *Privacy on the Line. The Politics of Wiretapping and Encryption* (Cambridge, MA: MIT Press, 2007).

68. In January 2008 Al-Qaeda's Global Islamic Media Front announced support for the Advanced Encryption Standard (AES) with its Mujahideen Secrets 2.0. In November of the same year Lashkar-e-Taiba planned and executed a successful terrorist attack in Mumbai using Google Earth and secure "Voice over IP" communication. Ellen Messmer, "Al-Qaeda group claims to have strengthened its encryption security," *Network World*, January 23, 2008; John Bumgarner and Michael Mylrea, "Jihad in Cyberspace," *The Counter Terrorist*, March 12, 2010.

69. Vast amounts of information can now be transferred and made instantly accessible to a global audience via the internet. Sir David Omand, "Can we have the Pleasure of the Grin without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light?," *Intelligence and National Security*, 23:5, October 2008.

70. Gabriel Liulevicius, *Espionage and Covert Operations: A Global History. Course Guidebook* (Chantilly, VA: The Great Courses, 2011), 186.

71. Ibid.

72. A. Denis Clift, "The Coin of Intelligence Accountability," Loch K. Johnson (Ed.), *Strategic Intelligence, Volume 5, Intelligence and Accountability. Safeguards Against the Abuse of Power* (Westport, CT: Praeger Security International, 2007).

73. David Omand, "Intelligence Secrets and Media Spotlights. Balancing Illumination and Dark Corners," in Dover and Goodman, *Spinning Intelligence. Why Intelligence Needs the Media, Why the Media Needs Intelligence* (New York: Columbia University Press, 2009).

74. Ibid.

75. Wark, "Learning to Live with Intelligence."

76. The way to become an "agile intelligence enterprise" was to adopt the private sector's "virtual corporation." Bruce D. Berkowitz, "Information Technology and Intelligence Reform," *Orbis*, Winter 1997; Bruce D. Berkowitz and Allan E. Goodman, *Best Truth. Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000).

embrace the open architectures, publish and subscribe protocols, and distributed database capabilities of the information revolution.[77] These aspirations were given fresh impetus in the aftermath of 9/11 when it became clear that the CIA and the FBI had failed to disseminate information on the run-up to the attacks.[78] Ten years later, despite ongoing bureaucratic resistance, the president of the Markle Foundation reports significant progress.[79] The disruption of several terrorist plots over the past decade demonstrates clear improvements in inter-agency information sharing.[80]

Others are less convinced that information sharing has made America safer. Paul Redmond, who led the investigation to find Aldrich Ames, warns that a blind focus on information sharing will inevitably ease the work of enemy spies and make the work of identifying them and neutralizing them more difficult.[81] The general increase in transparency has made other aspects of counterintelligence difficult. Creating deep and effective cover through "backstopping" that will stand up to intense electronic scrutiny is more difficult than ever.[82] And in an age of persistent surveillance, concealing sponsorship of covert operations is also getting harder, as demonstrated by the remarkable Dubai videos of the Mossad assassination of Hamas paramilitary Mahmoud al-Mabhouh in 2010.[83]

The flipside is that ICT has made spy handling and tradecraft easier and safer. Individuals with potential access to secrets can be "spotted" and their vulnerabilities identified by mining social networks, chat rooms, credit histories and spending habits.[84] Spy handlers no longer need to meet their spies face-to-face in safe houses but can meet virtually using secure video casting.[85] The secret documents that were photographed and dead-dropped during the Cold War are now likely to be imaged and transmitted electronically.[86] Easily concealed memory cards reduce the need for compromising devices to hide film or secret writing material.[87] And a Cold War "covcom" (covert communication) plan involving dangerous brush passes, car tosses or dead drops can now be completed safely in seconds over the internet.[88]

On balance ICT has not made analysis any easier, however. The information explosion makes it tougher to distinguish true signals from ambient noise.[89] Analysts simply cannot keep up with the flood of imagery intelligence collected by UAVs.[90] The problem is particularly acute in signals intelligence. By 1995 the NSA was vacuuming up the equivalent of the Library of

77. Ibid.

78. National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report* (New York: Barnes & Noble, 2006).

79. Zoe Baird Budinger and Jeffrey H. Smith, "A Lesson of 9/11: Washington Can Work," *The Washington Post*, August 26, 2011.

80. The Markle testimony cites the Najibullah Zazi plot. Zazi was arrested in September 2009 in connection with an al Qaeda plot to bomb the New York subway system. The plot was disrupted due to the collaborative efforts of the FBI, the DHS and the New York and Denver police. The sharing of information via state and local fusion centers and Joint Terrorism Task Forces was instrumental. Zoe Baird Budinger and Jeffrey H. Smith, *Ten Years After 9/11: A Status Report on Information Sharing*, Senate Committee on Homeland Security & Governmental Affairs, October 12, 2011.

81. Redmond fears that the interconnection of more and more networks will lead to a breakdown in compartmentation. Similarly Loch Johnson fears the possibility of a future Ames or Hanssen who not only steals from his own corner of the IC but has access to the full network of the IC's computers. Information experts counter that the solution is to apply policy-driven technologies to control, discover, access and use information, even as capabilities to share information are improved (admittedly an enormous task for an intelligence community the size of the US IC). Intelligence Community Directive 501, issued in 2009, describes the types of policies required. Paul J. Redmond, "The Challenges of Counterintelligence," in Loch K. Johnson, *The Oxford Handbook of National Security Intelligence* (Mew York: Oxford University Press, 2010); Loch K. Johnson, *National Security Intelligence. Secret Operations in Defense of the Democracies* (Cambridge, UK: Polity Press, 2012), 127-128; Budinger and Smith, *Ten Years After 9/11*.

82. Identity information such as address, profession, and association membership are immediately verifiable using search tools. Because so much personal information is available online it is almost impossible to remake a person's life history including records of education, credit cards, residence, family, children's schools, library cards, and driver's licenses. Robert Wallace and H. Keith Melton, *Spycraft. The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda* (New York: Penguin Group, 2009), Chapter 25, 'Spies and the Age of Information"; Brenner, *America the Vulnerable*, 190.

83. Brenner, *America the Vulnerable*, 157-163.

84. Numerous data services will disclose a person's credit rating, mortgage payment, subscriptions to magazines, grocery purchases, car payments, society memberships etc. Robert Wallace, "A Time for Counterespionage," in Jennifer E. Sims and Burton Gerber (Eds.), *Vaults, Mirrors, and Masks. Rediscovering U.S. Counterintelligence* (Washington, DC: Georgetown University Press, 2009); Wettering, "The Internet and the Spy Business."

85. Wallace, "A Time for Counterespionage."

86. Wallace and Melton, "Spies and the Age of Information."

87. Ibid.

88. Digital dead drops are made by saving uncompleted emails on providers' hard drives; anonymous remailers and peer-to-peer services that bypass service provider hubs are used to communicate with sources; and messages are made secure with encryption and invisible with steganography or "chaffing" (the sender embeds bogus bits into the message and the receiver "winnows" out the chaff to reveal the message). Portable covert operating systems on USB sticks ensure that no traces of encrypted messages are left behind. Wallace and Melton, "Spies and the Age of Information;" Wettering, "The Internet and the Spy Business."

89. Wark, "Learning to Live with Intelligence."

90. According to Marine Corps General James Cartwright, it will require 2,000 analysts to process video feeds from a single Predator with next generation sensors. Eli Lake, "Drone Footage Overwhelms Analysts," *The Washington Times*, November 9, 2010.

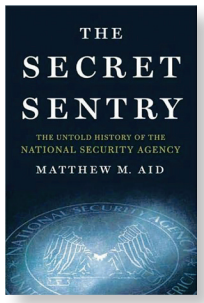
Congress every three hours.[91] By 2007 the amount that NSA analysts were able to process had fallen below 1%.[92] In addition to rebuilding their collection infrastructures to cope with the revolution in fiber optics,[93] UKUSA agencies are scrambling to find a solution to the volume problem. With a priori intelligence covert teams[94] can collect targeted close-in SIGINT. With an identifier they can use triangulation to geo-locate the source of signals from radios, satellite or cellular phones.[95] With a voiceprint they can home in on a suspect's communication.[96] Or with a phone captured from a raid, they can use "call chaining" or "link analysis" to track down accomplices.[97]

Without a lead, however, agencies have to turn to data mining, raising civil liberty concerns. In the past decade the US and the UK have had to cancel and replace Orwellian government projects, designed to capture and store private citizen data, with smaller, more private-sector initiatives.[98] In 2009 the Christmas Day bomber reminded the public of the need for advanced analytic tools, which are now popular with analysts in law enforcement and the military.[99] New tools to conduct "digital forensics" have also been developed to cope with the explosion of digital information being seized by investigators.[100]

READINGS FOR INSTRUCTORS

Agencies and Corporations

For a balanced look at the NSA after the Cold War see Matthew M. Aid, *The Secret Sentry. The Untold History of the National Security Agency* (New York: Bloomsbury Press, 2009). For a more critical take see James Bamford, *The Shadow Factory. The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Anchor Books, 2008) or the companion 2009 PBS film *The Spy Factory*. For a history of UK SIGINT see Richard Aldrich, *GCHQ. The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperPress, 2010).



The official history of the National Geospatial-Intelligence Agency (NGA) and predecessors is *Advent of the National Geospatial-Intelligence Agency*, September 2011,

91. Matthew M. Aid, "All Glory is Fleeting: SIGINT and the Fight Against International Terrorism," *Intelligence and National Security*, 18:4, 2003.

92. Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York, Simon and Schuster, 2008), 218.

93. The radome protected antennae of the global "Echelon" network have almost become redundant as companies like Global Crossing funnel the world's communication through optical fibers. By one estimate the volume of international communications transmitted over subsea cables increased from 2% in 1988 to 80% in 2000. To intercept the new cable traffic national SIGINT agencies have installed black boxes in the offices of international telecommunication carriers. Domestic agencies have solicited the same cooperation from ISPs. James Bamford, *The Shadow Factory. The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Anchor Books, 2008), "Book III: Cooperation."

94. Such as the US Army's Intelligence Support Activity or the CIA's Special Collection Service. Matthew M. Aid, "All Glory is Fleeting."

95. There are numerous examples. See, for example, "Suspect Tracked by Phone Calls," *B.B.C. News*, August 1, 2008.

96. US SIGINT technicians were able to develop a voiceprint of 9/11 mastermind, Khalid Sheikh Mohammad (KSM), from a recording of an interview conducted by Al Jazeera reporter, Yosri Fouda, in June 2002. The voiceprint was used to narrow the search for KSM, which ended in Rawalpindi on March 3, 2003. Robert N. Wesley, "Capturing Khalid Sheikh Mohammad," in James J. F. Forest (Ed.), *Countering Terrorism and Insurgency in the 21st Century, Volume 3*, Lessons from the Fight Against Terrorism (Westport, CT: Praeger Security International, 2007).

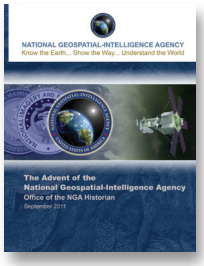
97. Bamford, *The Shadow Factory*, 149.

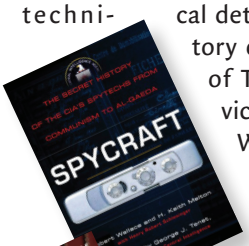
98. In the U.S. the ambitious DARPA project, "Total Information Awareness," was swiftly killed by Congress in 2003, while the NSA's "Trailblazer" was broken down into smaller projects in 2005. In the UK the equally ambitious GCHQ "Intercept Modernization Program" was revamped in 2009 to avoid a "single central store" by allowing government access to data stored by the communication providers themselves. Tim Shorrock, *Spies for Hire*, Chapter 6, "The NSA, 9/11, and the Business of Data Mining"; Siobhan Gorman, "NSA's Domestic Spying Grows As Agency Sweeps Up Data," *The Wall Street Journal*, March 10, 2008; Richard J. Aldrich, *GCHQ. The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperPress, 2010), 543-548; "Jacqui Smith Scraps Plan For Email Database," *The Telegraph*, April 27, 2009.

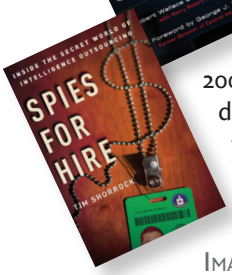
99. Nigerian Umar Farouk Abdulmutallab attempted to detonate a concealed explosive device on Northwest Airlines Flight 253 over Detroit on December 25, 2009. His name was already in the US Terrorist Identities Datamart Environment (TIDE) and a UK watch list, he had been refused a visa by Great Britain, his father had warned the US embassy in Nigeria that his son had become radicalized and had disowned his family, he had paid cash for his flight ticket, and he had boarded the plane with no luggage. Norbert E. Luongo, "Watchlists in United States and Canada: An Intricate Web," *Air and Space Law*, 34:3, Jan. 10, 2010; Ashlee Vance and Brad Stone, "Palantir, the War on Terror's Secret Weapon," *Bloomberg Businessweek*, November 22, 2011.

100. After the London bombings in 2005, the UK passed legislation extending the time that terrorism suspects could be held without being charged, in part because they needed more time to analyze the hard drives of the computers and CCTV systems seized after the attacks. Contemporary forensic tools include "EnCase" and "Forensic Toolkit." Simon L. Garfinkel, 'Document and Media Exploitation," *ACM Queue*, Nov/Dec 2007; Mark Pollitt, "A History of Digital Forensics," Chapter 1 in K.P.Chow, S. Shenoi (Eds.), *Advances in Digital Forensics VI, IFIP Advances in Information and Computer Technology*, Volume 337, 2010.

by the Office of the NGA Historian, available at *www.nga1.mil*. The agency's *Pathfinder* magazine provides technical details. For a history of CIA's Office of Technical Services see Robert Wallace and H. Keith Melton, *Spycraft. The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda* (New York: Penguin Group, 2009). For the rise of the US intelligence-industrial complex see Tim Shorrock's *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York: Simon and Schuster, 2008).

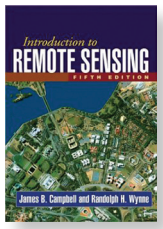




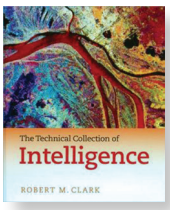


Imagery and Geospatial Technology

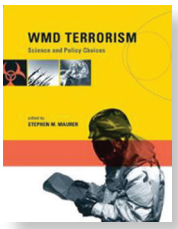
For a technical dive into imagery intelligence see James B. Campbell and Randolph H. Wayne, *Introduction to Remote Sensing*, Fifth Edition (New York, Guildford Press, 2011). One way to make the topic more accessible is to use short videos, such as Penn State's The Geospatial Revolution, available at *http://geospatialrevolution.psu.edu*.

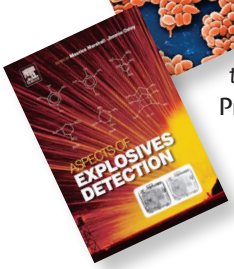


Materials and Weapons Science



The best book on MASINT is Robert M. Clark's *The Technical Collection of Intelligence* (Washington, DC: CQ Press, 2011). Teachers can use TV shows like 24, *Spooks* (MI5), or *CSI* to contrast "Spytainment"[101] and the real world.[102]

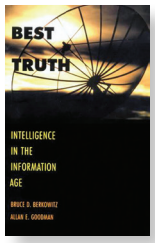


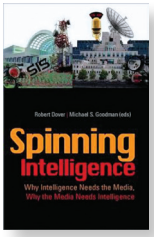


For an understanding of the science of weapons see Stephen M. Maurer, *WMD Terrorism: Science and Policy Choices* (Cambridge, MA: MIT Press, 2009); Gregory D. Koblentz, *Living Weapons: Biological Warfare and International Security* (Ithaca, NY: Cornell University Press, 2009); and Maurice Marshall and Jimmie C. Oxley (Eds.), *Aspects of Explosives Detection* (Amsterdam: Elsevier, 2009).

Information and Communications Technology

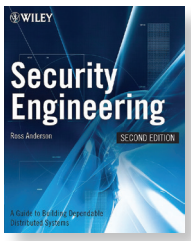
For a short analysis of the impact of ICT see Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000).

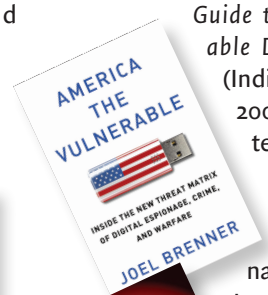


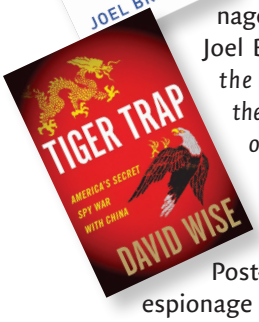


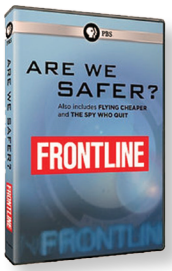
For the impact of the media see Robert Dover and Michael S. Goodman (Eds.), *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence* (New York: Columbia University Press, 2009).

For communication and cyber intelligence see Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Indianapolis, IN: Wiley, 2008). For surveillance technologies see the PBS film *Are We Safer* from 2011.[103] The rise of cyber-espionage is documented by Joel Brenner in *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011). Post-Cold War Chinese espionage is covered by David Wise's *Tiger Trap: America's Secret Spy War with China* (New York: Houghton Mifflin Harcourt, 2011).









Stephen H. Campbell is a Research Associate in the International Security Studies Program at the Fletcher School, Tufts University, where he specializes in intelligence and non-state armed groups. His career has included positions as analyst, consultant, educator, and marketing strategist in the information technology industry. Mr. Campbell earned a B.Sc. Honors First Class in Physics from the University of Glasgow and a Masters in Law and Diplomacy from the Fletcher School, Tufts University.

101. Amy Zegart, "Spytainment: The Real Influence of Fake Spies," *International Journal of Intelligence and Counterintelligence*, 24:3, June 2011.
102. Robert Dover, "From Vauxhall with Love. Intelligence in Popular Culture," in Dover and Goodman, *Spinning Intelligence*.
103. The film is based upon investigations published by Dana Priest and William M. Arkin in *The Washington Post*, and encapsulated in *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Company, 2011).