Intelligence and National Security

Reflections on Technology and Intelligence Systems
Michael Warner
Published online: 24 Feb 2012.

To cite this article: Michael Warner (2012): Reflections on Technology and Intelligence Systems, Intelligence and National Security, 27:1, 133-153
To link to this article: http://dx.doi.org/10.1080/02684527.2012.621604

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Reflections on Technology and Intelligence Systems

MICHAEL WARNER*

ABSTRACT The impact of individual technological innovations on intelligence operations is often discussed, but the influence of technological change per se on intelligence systems remains less well understood. The historical literature on this topic is uneven – filled with detailed narratives on certain aspects, but also with surprisingly little attention to larger trends and their meaning. This is significant for two reasons. First, it means we have an incomplete understanding of what happened in the past, particularly for the ‘analog revolution’ in intelligence in the twentieth century. Second, it leaves us with few clues for understanding another wave of technological change washing over the intelligence profession at this time (a ‘digital revolution’). Looking at the second revolution in the light of the first can give us important clues to what to watch for in coming years.

Technology can be understood as the varying ways in which people consciously and more-or-less collectively create and use tools to manipulate their environment.¹ The basic features of technology for any society can be thought of as falling naturally into two rough categories: first, the society’s ‘means of production’ (the mechanisms and methods by which its members shape their physical surroundings and accumulate wealth); and second, its artificial means for recording and communicating information (i.e. its collective understanding of how to collect and use data in making decisions). The relative abilities of neighboring societies to employ both aspects of technology will be of obvious interest to any society desiring to divine their neighbors’ plans.

Despite this relevance, technology’s impact on intelligence has been incompletely examined. To be sure, there is no lack of interest in the topic. A quick Google search yields more than 9 million hits for the phrase ‘technology and intelligence’. Although most of these references seem to relate to topics in the field of technology and human cognition – and not to intelligence in international affairs – still the reading list for intelligence professionals and observers must be vast.

*Email: warner@american.edu

¹Wikipedia’s article on Technology tells us it is ‘the making, usage, and knowledge of tools, machines, techniques, crafts, systems or methods of organization in order to solve a problem or perform a specific function’ (accessed 8 December 2011).
If such a list could ever be compiled, however, the preponderance of the titles on it would surely pertain to ‘intelligence technology’. Hundreds of authors have discussed individual innovations used by intelligence officers and agencies; indeed, one need only recall the many popular books and articles on ‘spy gadgets’ to grasp this point. This literature has had a long life already. A collective fascination with the tricks of espionage seems to have been well noticed by the publishing trade as early as the 1930s. That vogue shows no signs of abating, as the popularity of the for-profit ‘International Spy Museum’ in Washington, DC, might attest.

A small but significant subset of the literature on gadgetry has sought by scholarly methods to explain the genesis and impact on intelligence operations of various innovations. The mathematical and computational wizardry employed by the Allies to break German and Japanese codes in World War II has attracted considerable interest from scholars. Reconnaissance by intelligence services and the aircraft and other systems they have used to conduct it has garnered steady attention as well. Both of these broad topics emerged as scholarly emphases after memoirs by participants helped prompt and guide the declassification of official histories and documentation that began in earnest during the 1970s. That release of selected facts and records took place chiefly as a result of actions taken by the American and British agencies that developed and utilized the tools in question during the world wars and the early Cold War. Although the new knowledge of how progress in signals and imagery intelligence affected the organizations that developed and used these techniques pertained largely in an Anglo-American historical context, some of the lessons to be drawn seemed applicable more broadly, if not universally.

An even smaller branch of the literature treats technology as an intelligence target. The best of these titles on ‘technology intelligence’ cover the use of secret sources and methods to understand the scientific and technological plans and capabilities of adversaries. R.V. Jones (1911–97) helped to pioneer this field, both as a scientific adviser to the British high command in World War II and later as a memoirist; his published reflections provide an excellent introduction to the principles and patterns of this sort of work. Narratives like his read almost like detective stories, in that they involved puzzles and clues and end in satisfying (or at least logical) solutions.

These different sorts of writings discuss technology as a tool – or a target – of intelligence. Some of them mention specific ways in which intelligence officers and agencies have had to shift talent or resources to new problems posed by an enemy’s technological innovation. Others discuss how new

---

2See, for instance, the breathless descriptions of real and fancied spy gear in Richard Wilmer Rowan, *Spies and the Next War* (Garden City, NJ: Garden City 1936).


offices and sometimes whole agencies came into being to develop, deploy, and exploit some breakthrough invention promising military or intelligence advantages over adversaries. The value of such studies cannot be disputed; they have opened new windows in the hitherto secret world of espionage. Nonetheless, that value has limits. Few works on technology and intelligence examine or add to our understanding of how technology affects intelligence ‘systems’ – the collective authorities, resources, personnel, and tasks that a nation allocates to using secret means against real and potential opponents. Here is a gap in the scholarship, and an opportunity.

Technology and Intelligence

A state’s technological environment will have both direct and indirect causal relationships with the ways in which a state tasks and organizes its intelligence offices. This relationship shows most acutely in military matters. Because so much intelligence work is devoted to managing competition or winning active and potential conflicts with other states, the way in which a state applies violence in an organized manner to achieve its objectives will shape, in important ways, its intelligence system. The organization, mobility, and lethality of a state’s military – and those of its adversaries – will dictate (among other factors) the timeliness and precision demanded of intelligence work, the expertise that must be devoted to understanding what intelligence collects, and possibly the relative importance of human versus technical means of collection and dissemination. Technological change shapes and reshapes both the threats to a state as well as the opportunities available to it in the international arena, and thus it plays a role in determining the targets of intelligence and the means that intelligence employs. It also helps to determine the numbers and sorts of intelligence officers hired to collect and analyze data as well as to disseminate the resulting reports to decision-makers. Finally, it has direct impacts on the structure of intelligence organizations and their institutional relationships.

Technology’s effects – and thus its influence as an independent variable in shaping a state’s intelligence system – can be seen best over time. Such effects upon intelligence systems manifest themselves most dramatically in the midst of rapid and profound technological change, and yet there is no William H. McNeill to explain how technology affects intelligence as such. McNeill’s 1982 classic *The Pursuit of Power* examined the sustained impacts of technological change on the military arts and the ways in which they expanded or altered the relative capacities of commanders and societies to impose their will on others. He was not the first or the last author to take such an approach; one thinks of Elting Morison before him, and other authors like Jared Diamond in recent years. Still, McNeill may be without superiors in his reflections on the complicated interplay between organizations, finance, innovation, and war-making, showing how technological

---

change made possible advances in armaments and tactics, which in turn forced revisions to national strategies – sometimes by opening significant opportunities for gains at the expense of rivals.

McNeill’s insight has its merit in showing how the advantages of technical innovation have tended to accrue to militaries and societies that are open to change and organized to take advantage of it. Those societies notice the value in a new device or technique – like cannons or close-order drill – because they already have pre-existing habits, institutions, or inclinations that can be adjusted to adapt and spread it. They are also the ones to take advantage of the new cycles of innovation and adaptation that some inventions initiate. When their openness to innovation reaches its limits – whether for cultural, religious, or material reasons – a society’s technological prowess can plateau, or even decline.

Several authors have provided hints of the insights that can follow from taking a similarly ‘systemic’ approach to studying the effects of technological change on intelligence. David Kahn’s seminal study *The Codebreakers* (1967) showed how the intelligence profession in the West followed innovations in communications technology, becoming mechanized and industrialized as nations shifted from couriers to telegraph to radio (and from amateurish codes to machine encipherment to protect their messages). Kahn devotes ample space to the geniuses and skullduggery that inevitably enliven this story, but the real point of *The Codebreakers* is that method usually trumps intuition; plodding and careful routine – endlessly repeated across an entire agency, service, or government – provides nations sufficient security for their communications and (occasionally) the ability to read the messages of their rivals. The organizations that can establish and replicate these methods are those that render the best service to the decision-makers who rely on them – and thus are more apt to be given the resources and authorities they can use to grow in size and influence.

Recent works by scholars such as Jonathan Winkler and David Nickles have added new depths of insight. Winkler and Nickles chose different vantage points to chart the emergence of global telecommunications and show its effects on both diplomacy and military command and control, and, most important, on national strategy. The opportunity to communicate more swiftly and more securely in the nineteenth century transformed itself almost overnight from a luxury for diplomats to a necessity for entire governments. That development in turn dictated a host of strategic consequences, from state investment in cable companies and raw materials to competition over the rights to beaches where undersea cables could ‘land’. Both Winkler’s and Nickles’ contributions illuminate the complex and inter-related ways in which technological innovation

---


affected diplomacy, operations, and strategy – and also intelligence gathering, organization, and planning more generally.

John Ferris has explored the impact of communications technology on intelligence more directly. Treating topics as varied as British air defense against Zeppelin raids and the concept and effects of ‘C4ISR’ in Operation Iraqi Freedom, he has demonstrated how new weapons, intelligence practices, and command and control systems can interact in ways their designers never expected.\(^8\) Once set in train by the exigencies of military campaigning and the need to counter enemy initiatives, these interactive processes transformed intelligence practices and intelligence agencies – particularly by making them demand, consume, and produce vastly more information faster than ever before.\(^9\) Information becomes – in Ferris’ larger narrative – the animating force behind military innovation and operations: to control its use (and deny it to enemies) became the object of a large share of the energies of modern business, government, and military systems. The intelligence systems of the states controlling such capabilities have been pulled along in the wake of this sweeping re-ordering of military (and hence national) priorities, growing and being transformed to support actual and potential combat operations.

The United States’ then-Director of National Intelligence, J. Michael McConnell, attempted in 2008 to address related issues from a different vantage point in a public document titled *Vision 2015*. His essay marked an unsystematic but thoughtful portrayal of the future that awaits the US Intelligence Community.\(^10\) *Vision 2015* attempted to foresee not the political and economic events that will affect various nations, movements, and regions, but rather the global trends that are changing the ways in which the Intelligence Community will collect, analyze, and share information. Those trends, said *Vision 2015*, will both challenge current practices and provide opportunities for new and better ones. The speed and volume of data flows – and the need to understand them faster than determined enemies or adverse trends can harm Americans or damage national interests – places an imperative on changing the ways in which the Intelligence Community organizes its people and efforts. In short, the US intelligence agencies that had been created, organized, and tasked

---


\(^9\)C4ISR signifies ‘command, control, communications, computers, intelligence, surveillance, and reconnaissance’.

along the lines of the various collection ‘disciplines’ (human intelligence, signals intelligence, and the like) and functions (collection, analysis, and dissemination) should find ways of training, equipping, and managing the bulk of their officers in networked (and ever-shifting) inter-agency and inter-disciplinary task forces dedicated to addressing particular intelligence targets.

Intelligence is too marginal and secretive to have sweeping effects on society writ large like those described by McNeill – the influence flows mostly the other way. Nonetheless, these explorations of McNeill, Kahn et al. collectively suggest that the evolution of technology should be a prime subject of intelligence studies. It is time to look more carefully at technology and intelligence systems. In theory, the technological ‘environment’ can affect the ways in which a state tasks and organizes intelligence systems in varying ways. Changes in technology, by altering both threats to the regime and opportunities available to it, help to determine the objects of intelligence, the means that intelligence employs, and the ways in which it organizes those means. The technological context of an intelligence system can be assessed with reference to several factors that are of particular relevance to what follows:

- the society’s means for producing and distributing goods and services; in short, the level and sophistication of its overall economy;
- the level and reach of a society’s methods for creating, sharing, and retaining information; and,
- the ways in which a society can employ to maintain order within its boundaries and impose its collective will on other societies; to wit, its military means and prowess.

These factors all affect the structure, tasks, instruments, and targets of an intelligence system in several ways, as can be seen in what are perhaps the two most important historical examples of discontinuous shifts in intelligence systems wrought by technological change.

**Learning By Example**

World War I precipitated what might be called the ‘analog revolution’ in intelligence. Before the invention of radio and aerial photography, intelligence could still be conducted in ways essentially unchanged since the beginning of history. Sun Tzu (ca. 300 BC) discussed how commanders could gain information on their enemies and use intelligence means to blind and mislead them. To cite another example, Kautilya (ca. 200 BC) explained how very similar methods could be used to guard the regime and allow a prince to confuse and defeat his domestic as well as his foreign

---

enemies. A very long period of military innovation and social change did not essentially alter this instrumental and very limited concept of intelligence. It is true that industrialization, mass armies, and steel ships created a hunger among nineteenth-century armies and navies for information on their real and potential enemies (and the locales where they might have to fight them). This need brought forth the initial, small military and naval intelligence bureaus that most Continental powers and the United States had created by 1900. The technological means for gathering such intelligence—and hence the sophistication of the staffs involved in it—was not *per se* different from what could have been done in Napoleonic (or Roman) times. One can glimpse this point by perusing an 1895 treatise published by a British staff officer, Col. George A. Furse. His discussion of intelligence added the telegraph, newspapers, and filing cabinets to the means available to the commander-in-chief and his intelligence officer—but did not differ in its essentials much from Sun Tzu.

Beginning in 1914, intelligence in the major European powers swiftly evolved from being a secret annex to the state’s security, diplomatic, and reconnaissance functions, and matured into its own quasi-profession, populated with specialists laboring in bureaus custom-organized for their work. Radio and aircraft observation were the chief spurs to this revolution as the fighting spread from the land and sea ‘domains’ to the air as well. War had become a vast consumer of materiel during the Industrial Revolution, and now seemingly overnight it became a geometrically greater consumer of information as well, with the possibility of real-time transmission of orders, reports, and data almost immediately becoming the imperative to do so faster and more accurately than one’s adversary—who was also racing to overtake his own adversaries. The sudden and urgent need to exploit radio signals and photographic images to learn the enemy’s disposition and divine his intent created wholly new intelligence disciplines. Men (and very soon women as well) with little or no prior training in these crafts became specialists, and the services that gathered them together to parse intercepted transmissions and scrutinize aerial photographs applied the maturing principles of organization to create, as it were out of whole cloth, entire new intelligence bureaucracies where nothing of the sort had ever existed before.

Each of the major powers in the conflict had to follow suit for their own protection. The new disciplines of signals intelligence and imagery intelligence led the way on the Western Front in France (and in an England at risk from German bombing raids on its cities). Their corps of analysts and technicians had to be organized in increasingly complex, industrial-age offices and staffs, complete with intricate divisions of labor, precise support and logistical services, hierarchical management structures (and sometimes

---

12I discuss both of these ancient authors in ‘The “Divine Skein”: Sun Tzu on Intelligence’, *Intelligence and National Security* 21/4 (2006).
with around-the-clock production cycles) to process data and disseminate their products to their patrons and ‘customers’. Furthermore, someone had to manage these workers and offices – hence American pioneer cryptologist Herbert Yardley’s lament that ‘it began to look as if the war had converted me into an executive instead of a cryptographer’.\textsuperscript{14}

The First World War set in motion changes that would carry themselves toward their logical conclusions in the other great conflicts of the twentieth century. By World War II, industrial-scale signals intelligence and imagery intelligence for commanders were supplemented by theater- and national-level signals intelligence (sigint) and imagery bureaus to produce intelligence for decision-makers far from any battlefield.\textsuperscript{15} As the central problem of intelligence turned from gleaning scarce clues to coping with the glut of data, this ‘analog revolution’ empowered the richer states that could afford the mass-production intelligence systems that it made possible, giving them distinct (if sometimes fleeting) diplomatic and military advantages over more backward allies and competitors.

The intelligence innovations of the Cold War, for the most part, deepened and broadened the changes that had been set in motion in 1914. The only real intelligence collection discipline to be added – ‘scientific intelligence’, or as it is sometimes called, ‘measures and signatures intelligence’ (MASINT) – was a refinement on the collection of data emitted in the electro-magnetic spectrum; thus it was closely related to signals intelligence and imagery intelligence. In addition, the sophisticated collection ‘platforms’ of the Cold War – U-2s, SR-71s, spy satellites – were just that: platforms. They carried cameras and instruments that had descended directly from their relatively crude ancestors deployed with the armies that fought in the First World War.

In sum, one can tally six major effects resulting from the analog revolution that began in World War I:

- A revolution, by definition, means there is no going back to old ways. After 1914, any nation desiring to project power beyond its borders had to build new, larger intelligence organizations based on industrial methods of resourcing, processing and distributing product. As a corollary, a revolution also entails the dynamic of ‘creative destruction’, in which rapid technological and organizational changes place a premium on agility, adaptability, and innovation. Those who cling to old ways, or fail to take appropriate countermeasures, are defeated or pushed aside as their decreasing effectiveness becomes ever more glaring (and dangerous). The aforementioned Herbert Yardley, ironically, fell victim to this himself in the 1920s, as new methods of machine

\textsuperscript{14}Herbert Yardley, \textit{The American Black Chamber} (Indianapolis, IN: Bobbs-Merrill 1931) p.48.

encipherment outstripped his essentially pencil-and-paper codebreaking operation.\(^{16}\)

- Making sense of large quantities of data as fast as possible suddenly became imperative, forcing the birth of something new: data management, with analysis and analysts. This soon began to revolutionize both military operations and military intelligence.\(^{17}\) Since for the most part the new organizations created to process signals or imagery were situated in military structures, this need for analysis and analysts caused something of a cultural shock to those same militaries, which were forced to hire and also to protect and promote all sorts of distinctly un-military persons.\(^{18}\) Official reflections on this topic during World War I sound amusing in hindsight. The head of the American Expeditionary Force’s sigint section (G-2/A-6), Frank Moorman, noted in 1917 that the Army suddenly needed men of the sort who had ‘spent their lives studying hieroglyphics, cuneiform characters and the like’.\(^{19}\) One can imagine how such advice must have struck some of his superiors and colleagues, trained as they were for an era of black powder and cavalry charges. In addition, the Commonwealth allies and the United States intelligence systems by the end of World War II had mobilized their universities to create a new institutional discipline – ‘all-source analysis’. These new analysts pieced together fragments of information to fashion mosaic pictures of the intentions and capabilities of opponents.

- Asymmetric progress between security measures and collection systems meant huge vulnerabilities suddenly opening and closing. That unevenness was the cause of both joy and grief. Particularly in wartime, victory could swing toward the first antagonist who identified and exploited (or closed) the breaches created by well-intentioned but flawed innovations in communications and operational security. Both sides drew lasting impressions from the battle of Tannenberg in 1914, at which German generals read Russian orders radioed *en clair* and used them to thrash


\(^{17}\)For an idea of the information revolution’s effects on operations, see Nicholas A. Lambert, ‘Strategic Command and Control for Maneuver Warfare: Creation of the Royal Navy’s “War Room” System, 1905–1915’, *Journal of Military History* 69/2 (April 2005).


\(^{19}\)Frank Moorman, Office of the Chief of Staff, American Expeditionary Force, ‘Notes on Personnel Required by Radio Intelligence Service, AEF’, no date [1917], National Archives and Records Administration, Record Group 120, American Expeditionary Force, Entry 105, Box 5765, unnamed folder. I am indebted to Mark Stout of the International Spy Museum for this reference and citation, as well as other insights he kindly shared with me in drafting this article.
two Russian armies before they could join forces. ‘We were always warned by the wireless messages of the Russian staff of the positions where troops were being concentrated for any new undertaking’, bragged German general Max Hoffmann in his 1924 memoir. ‘Only once during the entire war were we taken by surprise on the Eastern Front by a Russian attack’.20 The signals intelligence triumphs now known by the shorthands of ULTRA, MAGIC, and Venona are only three of many notable examples that need no elaboration here.

Intelligence sharing with industry and coalition partners became crucial to the performance of intelligence services for perhaps the first time in history. This phenomenon had both positive and negative aspects. Collection, processing, evaluation, and analysis all benefitted from the economies of scale and divisions of labor made possible if intelligence bureaus could acquire custom-built equipment and collaborate across national lines. In addition, allies had to have roughly parallel intelligence capabilities for their mutual protection. For instance, the British and French felt compelled to teach the new intelligence skills to their new allies as quickly as possible in 1917 as the American Expeditionary Force prepared to take over sectors of the Western Front. A senior American intelligence officer shortly after the war remembered that the British were very anxious that they would make us understand how serious all these things were. The French had the same solicitude but they were less tactful in expressing it . . . Their attitude was more ‘Well, this is the way it is, you can take it or leave it.’ The British attitude was ‘this is the way it is: for God’s sake take it, take our word for it’.21

The three-way sharing of intelligence that resulted – while crude by later standards – nonetheless benefitted all partners, and created precedents for the great Anglo-American intelligence alliance of World War II and beyond.22

The management of the relationships between the new intelligence collection and production offices also became very important. Large,

20Quoted by Kahn in The Codebreakers, p.633. American cryptologist William Friedman was still citing Tannenberg as an object lesson for National Security Agency employees more than four decades later; see the collection of his lectures published as The Friedman Legacy: A Tribute to William and Elizebeth Friedman (Ft. Meade, MD: National Security Agency 2006) p.123.


specialized organizations the world over tend to go rent-seeking; i.e. to channel resources to activities that bring in new resources at a minimum of risk and disruption, and the new intelligence bureaus were no exception. Methods and mechanisms for the internal oversight of secret activities thus needed to be created, with ‘metrics’ for assessing performance as well. Who best to manage such enterprises was another serious question: should the leadership ranks be staffed with the geniuses who made the breakthroughs in the first place, or with trained executives who could make the accounts balance (but who might be less sensitive to the operational or technological details)?

- Finally, nations that build technologically sophisticated, multi-agency intelligence systems sooner or later find that intelligence can never seem to meet all the needs placed on it by national, operational, and tactical decision-makers. The expense and difficulty of constant monitoring and collection, and the associated processing, analytical, and dissemination costs, made the new signals and imagery collection ‘architectures’ unique; they could not be replicated for multiple users. In other words, a single intelligence architecture had to serve both national and departmental customers. That meant there had to be an exquisite balancing of efforts, resources, and targets. How then to satisfy the competing needs of both national and sub-national officials and commanders for intelligence support capabilities that were too sensitive and expensive to duplicate for both sets of requirements? In the Cold War this problem of management became even more acute, especially for the United States with the development of satellite-based collection platforms. In addition, as technological sophistication in the intelligence field increased, the spiraling costs involved with deploying advanced collection systems grew to be another significant factor driving the administration of intelligence systems.23 The many issues involved in managing complex collection and analytic systems to support warfighters, ministers, and policymakers will continue to be felt for as long as collection technologies remain so costly and rare.

The Digital Revolution

The rapid development of the military art in the early twentieth century has significant parallels – and some instructive points of dissimilarity – with the revolution in information technology and intelligence now sweeping the globe. The rapid progress of science in modern times owed much to the realization that mathematics could play so much larger a role in helping mankind understand the natural world than had hitherto been suspected. Similarly, the information revolution took off in the 1940s with the realization that any task could be subjected to mathematical processes (with their accompanying speed, volume, and precision) if it could be

\[23\] I discuss an instance in which this dilemma had practical effects in ‘Reading the Riot Act: The 1971 Schlesinger Report’, Intelligence and National Security 24/3 (2009).
expressed in the form of an algorithm. The result has been an accelerating shift of work and communications tasks to computerized (i.e. digital) processes, swiftly followed by an equally momentous connecting of these processes to one another over networked channels. If the analog revolution was a discontinuous shift in the technology of acquiring and sharing information, then its digital counterpart represents yet another discontinuous shift in the technology of acquiring, sharing, and storing information. Its effects are still emerging and their outcome is difficult to predict, though their significance for intelligence systems can be expected to be profound.

The digital revolution’s impetus is the tectonic confluence of three developments in what we have collectively dubbed ‘cyberspace’: the interlinking of mankind via cheap and seemingly instant, relatively secure, and ubiquitous communications, the shift of humanity’s collective memory and data processing into increasingly capacious and accessible electronic archives, and the ‘democratization’ of innovations that can cause narrowly tailored or widespread economic or even physical harm (i.e. viruses, worms, and other forms of ‘malware’). Every government and intelligence system is feeling the effects of this digital revolution. Concepts, organizations, and doctrines that intelligence systems had created and maintained during the analog revolution of the twentieth century now have to be revised. Moreover, they have to be revised rapidly while the systems around them are still performing their intended missions. As one senior Bush administration official in Washington noted while the US Intelligence Community was being reformed in 2004, doing so is like undergoing surgery while galloping on a horse.24

To understand these changes and their effects, it might be useful to compare the impact of the current information revolution with that of the last one. Almost as soon as people began transmitting information via wireless, their adversaries began eavesdropping on and/or disrupting the transmissions, thereby forcing all sides to undertake to secure their own use of radio from foreign prying or tampering. These three activities – ‘exploit, attack, and defend’ – apply to the world of digital data transfers just as they apply to the realm of radio, with an added twist: radio signals exist only when they are transmitted, while data storage at both the sending and receiving ends means that data can be attacked or exploited (and therefore must be defended) when they are at rest as well as when they are in transit. These parallels between radio and cyberspace suggest that the points made above concerning the analog revolution have parallels today:

The digital revolution, like the analog, is at its root an irreversible transformation of how people acquire and use information. That fact has immediate ramifications for intelligence – much of which, after all, concerns the discovering of that which others know (or think they know). How those others acquire, store, transmit, and secure such information, therefore, is of fundamental importance to intelligence in all eras – indeed, it will dictate at a basic level the tactics and techniques of intelligence, which – in that sense – can be thought of as a function of the changes in information technology. Today the ‘things’ that people, enterprises, governments, and societies value are increasingly not things at all – but rather are units and arrangements of information – ones and zeroes – more and more often created, stored, moved, and shared by digital means. One particular aspect of this topic merits additional consideration. Intelligence naturally follows wealth: where value and hence wealth are created, stored, moved, and shared, there is where intelligence services will employ secret means to divert some of that value for their own purposes (and where the rightful owners will deploy overt and covert means of their own to stop such diversions). This is already happening on an impressive scale, if one credits press reports on the ‘GhostNet’ discovered by University of Toronto researchers; this operation, which the investigators deemed to be of Chinese origin, over a span of two years penetrated at least 1295 computers in 103 countries, ‘including many belonging to embassies, foreign ministries and other government offices’.26

The digital revolution creates everywhere a much greater demand for analysis, and analysts. The volumes of data that can be moved, stored, or stolen, are simply astronomical – they can barely be comprehended, let alone utilized by current methods. In short, the collection of digital information by digital means can easily outstrip the ability of analysts to sort through the take. For instance, Maj. Gen. William Lord, then of the US Air Force’s Office of Warfighting Integration, claimed at a public conference in August 2006 that Chinese hackers had downloaded ten to 20 terabytes (TB) of data from the Department of Defense’s Non-Classified IP Router Network (NIPRNet).27 Such a statistic is both

awe-inspiring and puzzling. Who can possibly digest 10–20 TB, which at a good reading speed of 200 words per minute (or 25kb of file space in text files) might take 3333 to 6666 work years (each of 50 work-weeks of 40 hours each) just to read? The answer is that analytical processes themselves are being swept along in the digital tide. They began to be automated (or at least assisted by desktop computing) in the 1980s, and now are being compelled to become much faster and more capable to keep up with the volume produced by automation elsewhere. There is already a vast literature on the technical and social factors involved in linking databases within and across organizations and the sorting and searching of their contents – the imperative to accomplish these feats with ever-greater speed and accuracy is now demanding a high share of mankind’s creative energies. The fact that intelligence professionals and their agencies are decidedly not among the leaders of this movement suggests that commercial firms like Google may well foster and train the next generation of path-breaking intelligence analysts – many of whom might not place their skills at the service of their respective governments.

- Organizational reshuffling is being forced by technological shifts as the preponderance of resources, taskings, and authorizations shift from older intelligence targets and methods to newer ones. The digital revolution radically compresses the time intervals available for recognition, decision, discrimination, and action – sometimes to milliseconds. A race is on to figure out intelligence organizations and doctrines for the digital age. That management challenge transcends all intelligence systems and indeed touches every large knowledge-based enterprise in the post-industrial age. No nation or enterprise has fully solved the problems of productivity and accountability associated with the new digital means, so it is doubtful that intelligence agencies, which typically take on their organizational models from their social contexts (rather than vice versa) will innovate for the whole of post-industrial society in this case.

- As with the analog revolution, success favors coalitions. Though there is little information publicly available on transnational intelligence partnerships in cyberspace, one could probably argue cogently from the precedent of the analog revolution that any strictly ‘national’ intelligence system (one with no significant liaison partners) is by nature at a serious

---

28Some idea of the magnitude of this literature can be gained from a quick perusal of Wikipedia’s listings under the Category ‘Databases’, which holds 13 sub-categories and 186 separate ‘pages’ (i.e. individual articles). Choosing only a single one of those sub-categories, ‘Knowledge discovery in databases’, one finds under it a further two sub-categories and 15 pages.

29Another question also arises: could the tools those analysts employ subtly constrain their thinking and thus their analyses? This is no trivial matter in an intellectual milieu in which ideas are typically expressed in formats dictated by (or compatible with) Microsoft Office software. I thank Martin Alexander for raising this issue, which might one day demand considerably more attention and insight than the present author can bring to it.
disadvantage against sets of intelligence systems that collaborate against common targets.

- Another parallel can be seen in the rapid spread of general knowledge about the new changes. We noted above Max Hoffmann’s boast about German exploitation of Russian wireless. His memoir was one of several accounts published in the 1920s that publicly revealed the importance of signals intelligence in World War I. The digital revolution in intelligence has had a similar run of early publicity. Der Spiegel noted in 1969 what might have been the first example of computer espionage (perpetrated by the ubiquitous Markus Wolf); Clifford Stoll’s The Cuckoo’s Egg (1989) remains a classic and timely account of a remote access operation; and James Adams explained in 2001 how foreign hackers had seemingly taken up residence in sensitive US government networks. What seems new can be much older than commonly thought.

- Finally, and despite the general knowledge of what is happening, progress in particular areas can be quite asymmetric. Just because something is ‘public’ does not mean everyone has noticed it or realized its implications. This probably does not need elaboration; as science-fiction writer William Gibson likes to say, ‘the future is already here. It’s just not very evenly distributed’. As in the two world wars, the intelligence system that spots its own vulnerabilities and those of adversaries (assuming it patches the former and exploits the latter) is going to have clear advantages. Success in this realm probably favors the side that is more self-critical and more open to external oversight.

Two Disparities

To grasp the implications of new information technology (and the whole panoply of social and economic changes it has wrought) on intelligence structures, one might also consider two developments that do not seem to be well explained by the above parallels between the analog and digital revolutions:


First, the new course of technology seems to be erasing the already blurry state/non-state actor line, putting powerful and stealthy weapons in private or non-state hands. Digital technology has given virtually all nations – and even angry and determined groups and individuals – suites of intelligence capabilities that since the dawn of the analog revolution had been virtually monopolized by the richer and more advanced states (and their clients). Today the digital revolution makes some forms of intelligence and security more expensive; witness the fanfare that greeted the announcement in October 2009 that the US National Security Agency (NSA) would build another large data center – this one a $1.5 billion effort in the state of Utah. At the same time, however, it makes other forms of intelligence much cheaper; small states and non-state actors can now practice espionage and covert-action against the largest states, with comparatively little expense and minimal risk to themselves. Attacks can be very difficult to attribute to specific attackers, who can mobilize vast numbers of computers owned by unwitting bystanders into ‘botnets’ that support specific activities. This lowering of what economists call the barriers-to-entry for intelligence trends in the opposite direction from the changes set in motion during World War I, which had concentrated information power and destructive weaponry in state hands. Here is another effect of the digital revolution that may merit two considerations from future students of comparative intelligence systems. First, are we approaching a time when it is possible to duplicate ‘national-level’ collection capabilities for each department or agency that wants them? Perhaps not, but that does not mean that some ministries or departments


34James Gosler explains the problem of attribution thus: ‘For low-level threats, such as hackers, the combination of a connected target and an inherent vulnerability is sufficient to exploit targets … In the recent past, US adversaries have collected and exfiltrated several terabytes of data from key Department of Defense networks. The apparent inability to patch US systems in a timely manner provides opponents with ample opportunities for access to our information systems. While we are aware of these operations, we do not appear to have the technical ability to close the access holes or to clearly attribute these operations to the perpetrator(s)’ [punctuation in original]. See Gosler’s ‘Counterintelligence: Too Narrowly Practiced’ in Jennifer E. Sims and Burton Gerber (eds.) Vaults, Mirrors, and Masks: Rediscovering US Counterintelligence (Washington, DC: Georgetown University Press 2008) pp.181–2.

might not attempt to create their intelligence capabilities for their own specialized needs in cyberspace. Second, will we see more ‘super-empowered’ individuals like Henry Okah, the Nigerian warlord who from South Africa and other nations used his cellphone and the internet to build, arm, command, and advertise the Movement for the Emancipation of the Niger Delta (MEND)?

It is not difficult to imagine such entrepreneurs of violence building their own sophisticated intelligence operations to support their plans; one might argue that Al Qaeda already has.

- Second, leaders and communicators during the analog revolution did not have to worry as much as they do now about the integrity of the data being transmitted. The fact that our computers now transmit and store data means that those data can be stolen or corrupted whether in motion or at rest. Then-US National Counterintelligence Executive Joel Brenner indirectly reflected on this in a 2009 speech, noting that

> We’re also seeing counterfeit routers and chips, and some of those chips have made their way into US military fighter aircraft... you don’t sneak counterfeit chips into another nation’s aircraft to steal data. When it’s done intentionally, it’s done to degrade systems, or to have the ability to do so at a time of one’s choosing. There is no longer a meaningful difference between data security and operational security. Our operations depend on our networks – the same networks on which we create, move, and store data.


In fact, you don’t have to corrupt any information to corrupt all of it. The nasty side of the integrity breach is that all the code/data contained within the system is rendered suspect. Just the fact that an adversary has been present in your system makes the entire system suspect. The depth of the risks associated with the integrity issue and the potential costs for recovery are frightening.

Levels and Domains

A decade ago strategists and military historians debated whether digital technology and networking had fostered a ‘Revolution in Military Affairs’. Networks would soon fight networks in non-kinetic conflicts, it appeared; and where live forces engaged, intelligence, command, and action would be fused by all-but omniscient sensors and instant and ubiquitous control. The wars in Iraq and Afghanistan, however, seemed to have settled the issue in the pessimists’ favor. War had not changed – it was still the same gritty business it had always been, albeit with more accurate weaponry and timelier communications.

This verdict would seem just if ‘cyberspace’ is considered as merely a domain of military operations, resembling the land, sea, and air domains as spaces through which forces assemble, communicate, and move, and in which they engage one another. That is indeed how the Joint Chiefs of Staff now views it, as evidenced in their 2004 National Military Strategy, which asserts ‘The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace’.

Indeed, the US military’s new Cyber Command – with its commander serving simultaneously as the Director of the National Security Agency – will be the entity charged with ensuring such freedom of action for the United States in the cyber domain.

42According to Ellen Nakashima in the Washington Post, the new US Cyber Command would ‘merge the Pentagon’s defensive unit, Joint Task Force-Global Network Operations, with its offensive outfit, the Joint Functional Command Component-Network Warfare, at Fort Meade, home to the NSA. The new command, which would include about 500 staffers, would leverage the NSA’s technical capabilities but fall under the Pentagon’s Strategic Command’; see ‘Pentagon Computer-network Defense Command Delayed by Congressional Concerns’, Washington Post, 3 January 2010, p.A04. See also Lieutenant General Keith B. Alexander’s answers submitted before his 15 April 2010 Senate confirmation hearing to be the first commander of Cyber Command, <http://www.fas.org/irp/congress/2010_hr/ 041510alexander-qfr.pdf> (accessed 24 April 2010). Israel’s chief of military intelligence,
But cyberspace is not a place at all, and thus cannot be considered simply as a domain for military activities (useful as that insight can be). Every bit or byte exists because someone directly or indirectly created it. Cyberspace is the product of human action, a realm for human action, and the current expression of those actions. Unlike the traditional military domains, it has its being outside of time – there is no past or future in cyberspace, there exists only the activities that people have individually and collectively caused to be happening at this instant. Those activities and the events they cause can manifest themselves as hostile acts, in that they cheapen and sometimes destroy the value of information and networks. Such acts need to be regarded as points on the continuum of conflict that ranges from diplomacy through coercion, terrorism, asymmetric warfare, and conventional warfare, to the ultimate use of weapons of mass destruction. They would seem to lie mostly on the less-destructive end of the conflict continuum, but that should give no comfort to statesmen and intelligence directors charged with monitoring and responding to them, for the volume of activity in cyberspace and the number of ‘attacks’ is staggering. 43 The constant daily assaults on governments and the industries, services, and people they guard might not constitute war in a strictly Clausewitzian sense, but they are indeed hostile, and often dangerous.

Regarding cyberspace operations as a niche on the level of international conflict should have profound if still uncertain implications for the ways in which statesmen task and organize their intelligence systems. In particular, the digital revolution may be eroding the proverbial wall between ‘operations’ and ‘intelligence’ – at least in cyberspace. Military staff charts from the early twentieth century that formally separated ‘ops’ (S-3) from intelligence (S-2) could be obsolete where collection is action and action is collection. Technology changes war and intelligence together, for the digital revolution is blurring the definition of destruction and thus of force, in that it amplifies or at least confuses the effectiveness of weapons that destroy value rather than people. If conflict is largely about being able to control and move value, and if secret means become the primary ways for guarding and taking value, then the historic closeness of war and intelligence becomes even closer. 44 The digital revolution might be moving the world to the verge of

---


44 Media speculation hints that this might have already happened at the turning point of the Iraq War in 2007; see Shane Harris, ‘The Cyberwar Plan’, National Journal, 14 November 2009.
something genuinely new, or actually very old, as the S-2/S-3 wall that was put in place a century or more ago teeters toward collapse. At least in cyberspace, we might be as close as anyone has ever come to Sun Tzu’s ideal commander, who with god-like foreknowledge and cunning divines his enemy’s plans, confounds his strategy, and renders him helpless without ever striking him.\(^45\)

Conclusion

Technological change will continue to be comparatively rapid and profound for the lives and institutions of people the world over. This preliminary comparison of two intelligence revolutions might help us understand the vector, pace, and scope of that change, and also let us glimpse how intelligence systems might change in the future. Two particular trends bear watching. For all intelligence systems, the digital revolution places an even higher premium on ‘all-source’ analysis, for it is one thing to steal reams of digital data – it is quite another to understand what in all that newly acquired data is meaningful and important. Second, as with the race to field and exploit machine-enciphered cryptographic systems in the twentieth century, states and non-states that organize, task, and oversee their intelligence officers to solve communications and security problems first and (relatively) best will have significant advantages over those that lag behind. These developments make the study of how states and non-states organize and task their intelligence systems ever more important. The final trend to anticipate under this heading is new thinking. Cyberspace is both a level of conflict and a domain for waging it. The result so far has been uncertainty. Intelligence systems and nations that sort out their thoughts first and best may gain real advantage over those that lag behind.

Another issue for the foreseeable future is whether the big organizations and large systems originally built during the Cold War will continue to retain their advantages over the smaller upstarts. Size can be a real disadvantage, if it makes an organization clumsy and resistant to innovation. Then again, large organizations have their strengths as well as their weaknesses. As Wilhelm Agrell has noted, intelligence organizations for a range of reasons (including secrecy and mission) are among the most durable and enduring institutions in any governmental system.\(^46\)

\(^{45}\) ‘Thus, those skilled in war subdue the enemy’s army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations. Your aim must be to take All-under-Heaven intact. Thus your troops are not worn out and your gains will be complete. This is the art of offensive strategy.’ Sun Tzu, *The Art of War*, III:10-11 (as translated in Samuel B. Griffith’s edition, Oxford: Oxford University Press 1963).

\(^{46}\) Professor Agrell made this comment at the conference on ‘100 Years of British Intelligence: From Empire to Cold War to Globalisation’, Aberystwyth University, 2 May 2009.
cells’ and link them together in ways that smaller intelligence systems cannot. What makes these new dilemmas more difficult for some state intelligence systems is that they are layered over the very same unresolved dilemmas that bedeviled those systems in the analog age. This is particularly acute for the nations that built the biggest collection systems. The old style of targets have not gone away, the older collection technologies still have value, and those technologies remain just as difficult to manage so as to serve national and departmental customers. Seemingly obsolete intelligence programs can rarely be simply switched off, and in the absence of major disasters will not be, because they consume significant resources and occupy people who cannot easily be sacked or shifted to new jobs. The smaller intelligence systems that never built up such capabilities in the first place may be swifter to spot opportunities and adapt to the new digital age. At any rate, organizational change is already occurring, although for the most part it has taken place within the structures of earlier organizations rather than by toppling those organizations and erecting new ones in their places.

Acknowledgements

The author is an historian with the US Department of Defense (DoD). The views expressed are those of the author alone and should in no way be interpreted as conveying official positions of the DoD or any other US government entity.