SCIENCE AND NATIONAL INTELLIGENCE

Richard L. Garwin[1]
IBM Fellow Emeritus
Thomas J. Watson Research Center
Yorktown Heights, NY 10598
RLG2@us.ibm.com

www.fas.org/RLG

Presented August 20, 2004 at the 32nd session of the
Erice International Seminars

Those who have followed the American scene in recent months have witnessed an extensive discussion of intelligence "failures" for lack of prevention of the September 11, 2001 attacks on the two World Trade Towers and the Pentagon, which killed 3000 people of many nationalities. An additional aircraft had been hijacked and would have been used, probably, to attack either the White House or the Capitol in Washington, DC.

Reports of other Commissions have been dedicated to failures of intelligence in regard to the weapons of mass destruction (WMD) in Iraq, and the reasons and logic for initiating war there. Of course, "WMD" is a term that makes little sense, since a nuclear explosion (even of the magnitude of the 1945 bombs used on Hiroshima and Nagasaki), if smuggled in and detonated near ground level, would kill 100,000 to 500,000 people in a densely populated city. Similarly, an appropriately chosen biological weapon such as anthrax, properly disseminated, or the smallpox virus, could kill as many, and perhaps far more. In comparison with these nuclear and biological threats, the current threat from chemical weapons such as Sarin is almost negligible. In fact, a reasonable rule of thumb is that there would be about as many deaths and non-fatal casualties from the use of a chemical weapon as from a modern high-explosive weapon such as cluster bombs, and the like.

By "WMD," therefore, we should understand nuclear and biological weapons, excluding radiological and chemical weapons.

Why "Science and National Intelligence," and what is "National Intelligence" anyhow?

National Intelligence is that information and interpretation that can guide decisions at the national level. This is distinct from Tactical Intelligence and Military Intelligence. Tactical Intelligence guides the actions of a platoon, company, brigade, or even of an army, as a result of knowledge and analysis of the deployment and capabilities of the opposing forces.

Military Intelligence provides additional information on the overall structure of opposing military forces, the characteristics and efficacy of the weapons with which they are provided, and the detailed information as to command structure, likely ability to carry out detailed and large-scale plans, and the like[2].

The point is that National Intelligence goes far beyond Military or Tactical Intelligence to inform the leadership of a country as to its options in

[1] Recipient in 1996 of the R.V. Jones Award for Scientific Intelligence, and in 2000 named one of ten Founders of National Intelligence.

[2] A useful source is the Center for Studies in Intelligence, operated by the US Government at http://www.cia.gov/csi/

negotiating, befriending, defending, or, for that matter, conducting military operations against another power.

At a time when US television channels (especially the Cable Satellite Public Affairs Networks (CSPAN)) are full of congressional hearings which feature former directors of (US) Central Intelligence and other experts, it may make some sense to consider the past and potential future contributions of science to National Intelligence.

Science enters not so much as science itself, which is, by definition, the acquisition of new insights and knowledge, but largely in the form of science codified in the form of technology and other tools. Just as the science of condensed matter physics has been incorporated into the miracles of this video projector, computers, and many of the amenities of modern life dating back to Galileo and even Archimedes, so science is taken for granted in the tools available for National Intelligence.

But it is there, as the finest flower of optics, of mathematics, chemistry, and, increasingly, of biology.

Intelligence involves the acquisition of information, its preservation and review, and its continual interpretation and reinterpretation in view of various hypotheses as to meaning and significance. In this it has a lot in common with the means by which we understand the secrets of the universe. Sometimes the information is in view for all to see, as was the case with the laws of falling bodies at the surface of the Earth, explored by Galileo and Newton. Sometimes it is hidden until a new tool makes it apparent, as is the case with the signals and "noise" in the radio spectrum, to which humans were blind and deaf until the advent of sensitive of radio receivers and amplifiers.

Sometimes it is necessary in the acquisition of Nature's secrets to travel to hostile environments, in order that the signal be received at all, or to be made more prominent against the local background noise. So it is in the sending of Soviet probes to the surface of Venus, or to the ocean depths in the exploration of the mid-oceanic ridge and the black smokers of recent decades.

So it was with the introduction of intelligence satellites, the first of which flew in June, 1960, in the form of a so-called "Galactic Radiation and Background ("GRAB") satellite, the real purpose of which was the acquisition of electronic intelligence on the radars of the world, and in August, 1960, the CORONA satellite to photograph the Earth from space. These early satellites have been fully declassified (that is, the information and in most cases the "product" made publicly available by the United States in 1995 in the case of CORONA, and in the year 2000 in the case of the GRAB satellite. They are discussed, for instance, in the article by Mark Moynihan[3].

The CORONA system was fully described in an article by Albert D. Wheelon[4] who as the first Deputy Director for Science and Technology of the Central Intelligence Agency, from 1962-1966 played a key role in the ongoing development of CORONA, as well as in the development of a titanium aircraft that traveled thousands of kilometers at a speed of Mach-3 (three times the speed of sound).

---

[3] Mark F. Moynihan, "The Scientific Community and Intelligence Collection," *Physics Today*, December 2000. (http://www.physicstoday.org/pt/vol-53/iss-12/p51.html)

[4] Albert D. Wheelon, "Corona: The First Reconnaissance Satellites," *Physics Today*, February 1997, pp. 24-30, ISSN 0031-9228. http://www.physicstoday.org/pt/vol-50/iss-2/vol50no2p24-30part1.pdf, http://www.physicstoday.org/pt/vol-50/iss-2/vol50no2p24-30part2.pdf

The imaging satellites (providing "image intelligence" or IMINT) and the Electronic Intelligence (ELINT) satellites had quite different origins. The first ELINT satellite was the product of the US Naval Research Laboratory, NRL, where scientists and engineers had the idea that they could obtain useful intelligence about the Soviet radar system for early warning against aircraft, by flying some relatively simple satellites. Recall that in the 1950s the state-of-the-art was vacuum tubes rather than transistors. Once these satellites were in operation, additional contributions were made, and additional launches of these relatively short-lived satellites could benefit from the rapid evolution of technology for military and civilian purposes, that have brought us from the first multi-million dollar digital computers of the 1950s to the $1000 marvel of today.

The modern imaging satellites took form in the minds of a few consultants to the President's Science Advisor in the 1954-1956 era, who had conceived the U-2 reconnaissance aircraft and persuaded President Dwight D. Eisenhower to develop it as a secret program assigned to the CIA. The subsonic jet-engine U-2 fleet first flew in 1956 through Soviet air space and that of other countries, publicly unacknowledged until May, 1960, when it was shot down by the SA-2 missile system near Sverdlovsk. These remarkable individuals included Edwin H. Land, inventor of polarizing film material and the Polaroid instant photographic system; Edward M. Purcell, Professor of Physics at Harvard University and Nobel Laureate for the invention of nuclear magnetic resonance; and James G. Baker, optical scientist and engineer par excellence, also of Harvard University.

Their observation was simple. It was that lenses of the 1950s could be built to provide resolution on the film comparable with the wavelength of light, and that ultra-fine grain film could also be made. So instead of the typical eight line pairs per millimeter (lp/mm) of military reconnaissance cameras flown by the US in the Korean War, one could build systems that would record information at 200 lp/mm. The difference made by the factor 25 is astonishing, since the amount of film required to record a given scene is reduced by a factor 625. Therefore, it makes sense to go to very thin-base film, and suddenly it is possible to record from a high flying aircraft at 20 km altitude horizon-to-horizon coverage continuously as the aircraft flies over the scene to be photographed.

Recognizing that aircraft would not long be invisible to radar (and, in fact, the U-2 was detected by Soviet radars from its first flight over the Soviet Union), the "Land Panel" conceived also the Mach-3 SR-71 aircraft, which brought entirely new challenges to the acquisition of IMINT. These included the extreme heat from the adiabatic compression of the air at this speed, bringing the surface temperature of the aircraft to the softening point of the titanium skin, and photography through the turbulence of the boundary layer adjacent to the aircraft.

Ultimately, even the SR-71 would be vulnerable to being shot down, and so an additional secret program was instituted, that would record not from 25 km within the atmosphere but from 160 km altitude, outside the sensible atmosphere, from the first Earth satellites, dubbed CORONA.

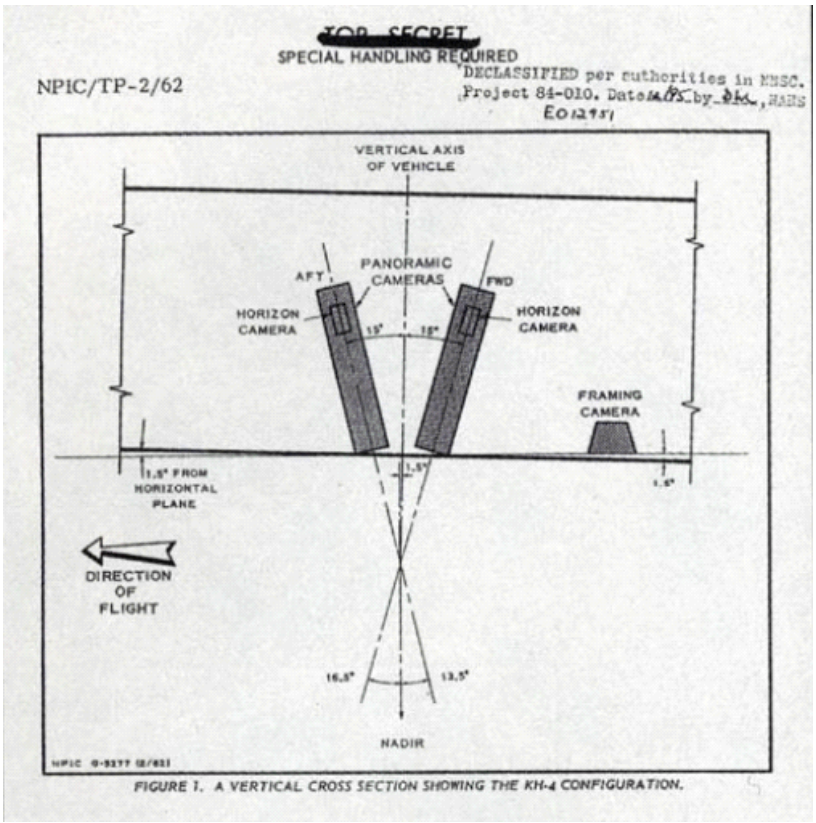
CORONA was initiated in the deepest secrecy, accompanying the cancellation of an Air Force program for the return of TV images from space. The technology of those days imposed stark limitations on what could be used in the satellite. There was essentially no "electronics" in CORONA. Rather, batteries operated electrical motors to drive the complicated film path, the rotating drums of the panoramic cameras, and the cams and switches of the timers that controlled the cycling and eventual reentry of the "bucket" containing the exposed film.

The first man-made objects retrieved from orbit were these reentry vehicles (RVs) of the CORONA system, that used ablative technology to survive the fiery heat of reentry. These packages were fitted with parachutes that would open at

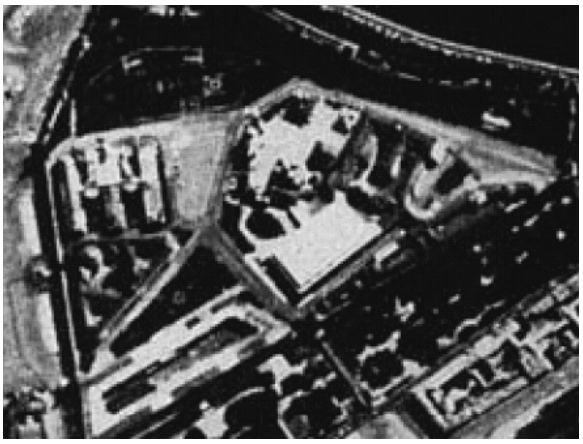
subsonic speed over the Pacific Ocean, so that the dangling film bucket could be retrieved by a kind of trapeze deployed from a C-119 aircraft of a special detachment operated for that purpose.

The CORONA system is well described in numerous articles following its 1995 declassification, not least by Wheelon in his 1997 article. Here are a few illustrations from that article:

Mid-air snatch of the parachute-borne CORONA film capsule by a C-117 aircraft.



Schematic of the two rotating-drum panoramic cameras in CORONA.



A view of the Kremlin. At the left is a narrow line of people awaiting entrance to Lenin's tomb.

The CORONA system was operated from 1960 to 1972, in more than 145 successful flights, returning almost 2000 km of film. By 1972, CORONA delivered a ground resolution of two meters (2 m), and was replaced by other systems, not yet declassified, both for broad area search and for high-resolution imaging from space.

Those now operating no longer depend on film return, but instead use imaging technology similar to that in your digital camera, typically employing charge-coupled devices (CCD) of silicon technology. The resulting images are returned in "near-real time" via radio downlinks from long-lived satellites in

space. Instead of mean mission duration on the order of one week for CORONA, the satellites provide images for many years.

For their part, ELINT satellites have evolved as well. The evolution of satellite technology no longer leads that of commercial applications, in view of the long lifetimes of satellites, and the special-purpose nature of their operation. Furthermore, there are limitations and hazards involved in the apparently benign space environment, since satellites are not shielded from cosmic ray radiation by the Earth's atmosphere, equivalent to a water depth of ten meters, nor from occasional collision with a micro meteor or piece of orbiting space debris.

The magnetic field that prevents most of the cosmic rays even from striking the atmosphere instead traps energetic electrons and protons that provide a heavy dose of radiation (on the order of a megarad over several years) to satellites in certain orbits.

Nevertheless, ELINT satellites have evolved to real-time return of information that not only pinpoints radars and other emitters on the Earth's surface, but also captures both Communications Intelligence (COMINT) and Signals Intelligence (SIGINT). The import of this is evident from the daily newspaper, with the implication that much useful information in the "global war on terrorism" is derived from such sources. Naturally, communications that travel via satellite (including some mobile systems) can be intercepted by ground-based antennas looking at the cell-phone relay satellites.

In this activity the US National Security Agency (NSA) plays an important role.

Accompanying the acquisition of intelligence is the required evolution of processing capability, dissemination, and the like. Ultimately, however, the intelligence product is reflected in various bulletins or estimates, that come to the desk of decision-makers at all levels and must result in national action or decision not to act, and be provided to other governments and to elements of the United Nations.

Unfortunately, many of those involved have little understanding either of the sources of the information or the limitations of the processes, including the possibility of denial and deception (D&D).

Thus the analyst assigned to watch for threats to the Information Technology infrastructure (IT) would have, in principle, access in this case not so much to IMINT, but to COMINT or SIGINT and would try to determine what resources are being expended by which foreign powers or terrorist groups, which individuals are involved, whom they communicate with, what test incursions have been made, and the like.

Another analyst looking for wayward nuclear explosives would concentrate on security of those sites where nuclear explosive materials are to be found in declared nuclear powers and in others. Most of the plutonium or highly enriched uranium exists in Russia or in the United States, so such an analyst would be alert to COMINT or suspect groups and nations traveling to Russia or dealing with middlemen in Russia. There might in addition be "sting" operations set up in order to determine interest in the acquisition of nuclear materials contrary to the Non-Proliferation Treaty (NPT).

Another analyst might be assigned to look for preparations for military activity or for genocide in an African country. In all these cases, the analyst would be concerned with foreign newspapers, foreign broadcast information, as well as information regarded as secret by the group or nation that originated it. Here is a problem, since the state of Information Technology is such that in practice in the United States a person with a computer with access to a secret (classified) governmental network cannot use that same computer for access to unclassified information, such as the Internet.

For this reason, "air gaps" must be created. Officials have testified recently that they have four or even six computers under their desk, and can switch the keyboard and the display (monitor) from one to another. This is already an advance, because a few years ago it was necessary for each computer to have its own display and monitor. But copying from one network to another is typically forbidden, unless the material has been printed and then scanned optically for transfer to the other network. As one might expect, the efficiency of working under these conditions is much reduced, even though the IT tools, in principle, can be very powerful.

Insufficient effort has been invested to provide a secure computing framework that would allow flexible access to information at multiple levels, including unclassified and highly sensitive material in the same information system. It should be possible for information to be identified, with its security classification appended, and composite documents or files thus prepared for the analyst's display.

In any case, IT has brought us a long ways from the "shoe box" era (still occupied by some analysts) in which material on a given site or topic was filed in the form of clippings or images literally in a shoe box, for future access by the analyst.

Whatever the mechanization, however, an analyst must form hypotheses and then determine their probability. "Alternative Competing Hypotheses" is a summary term for this approach.

Is there to be a military attack tomorrow? If there was not one yesterday or the previous day or the previous year, it seems inherently unlikely that there will be one tomorrow. It is said that British intelligence charged with warning of a military attack was wrong only twice in 50 years, but such an error can be very significant.

In general, the most rigorous framework for determining the validity of a hypothesis in science or in intelligence comes down to Bayesian Analysis. Here one asks for the probability of a hypothesis given the prior probability before the most recent "fact" and the likelihood that the new intelligence datum is correct or that it is wrong. It can be wrong in one of two ways (for a "yes-no" decision): it can have a Type-1 error, in which the datum may say "no" but the hypothesis may be valid; or it may have a Type-2 error, for which the datum reads "yes" and the hypothesis is invalid.

An example of a Type-1 error is a bit of disinformation stating that all troops are in their rest areas, when in fact they have been mobilized. An example of Type-2 error is a finding that troops have been mobilized, when in fact the motion that was observed was from one rest area to another.

A recent article by Bruce Blair, President for the Center for Defense Information in the United States (www.cdi.org) nicely illustrates the details of Bayesian Analysis[5]. In this case, one assumes a prior probability (without any intelligence data) of 99.9% that an attack is in process. If one has then a bit of intelligence saying that it is, and one knows or assumes that the source of the intelligence is correct 50% or the time, incorrect 50% of the time (in the sense that 25% of the time it indicates an attack is in process if it isn't, and 25% of the time indicates that an attack is not in process when it is), then the likelihood according to Bayesian Analysis after 1,2,3,4 and so on negative intelligence alerts is as shown in "0.999" line of the table.

[5] Thomas Bayes, "An Essay towards Solving a Problem in the Doctrine of Chances", *Philosophical Transactions of the Royal Society of London* 53 (1764). Bayes (1702-1761) was a Presbyterian preacher and a member of the Royal Society. See http://www.bun.kyoto-u.ac.jp/phisci/Gallery/bayes_note.html,

The mechanism of Bayesian Analysis is shown in the first figure, with the symbols having the following meaning: a term P(A|W) signifies the probability *P* of an attack *A* given that the warning *W* has been received. Bayes taught that this can be obtained from the more physically determinable P(W|A), the probability that the warning signal would be received if the attack were really in process. Important is the initial "prior (A)", which is the assumed likelihood that an attack is in process, to be refined by intelligence data. The *a posteriori* probability "Post (A)" is then the Bayesian update of the probability before the most recent information.

Our application of Bayes theorem is as follows:

Definitions:
Prob (attack|warning) = P(A|W)
Prob (attack|no warning) = P(A|NW)
Prob (warning|attack) = P(W|A) = 1 - prob (type I error)
Prob (warning|no attack) = P(W|NA)→type II error
Prob (no warning|attack) = P(NW|A)→type II error
Prob (no warning|no attack) = P(NW|NA) = 1 - Prob (type II error)

Prior initial subjective expectation of an attack: prior (A)
Posterior subjective expectation of an attack after either receiving or not receiving warning: Post (A)

Formulas:
Given warning is received during warning report period:

$$\text{Post (A|W)} = \frac{\text{P(W|A) prior (A)}}{\text{P(W|A) prior (A)} + [\text{P(W|NA)(1 - prior(A)}]}$$

Given warning is not received during warning report period:

$$\text{Post (A|NW)} = \frac{\text{P(NW|A) prior (A)}}{\text{P(NW|A) prior (A)} + [\text{P(NW|NA)(1 - prior(A)}]}$$

From Bruce Blair, The Logic of Intelligence Failure,
http://www.cdi.org/blair/logic.cfm

In this case, nine successive negative reports are required to convert an initial 99.9% probability of attack to a 95% judgment of no attack. It is thus very hard for fact (even facts with a pretty good probability of being correct) to overcome an initial bias of this magnitude.

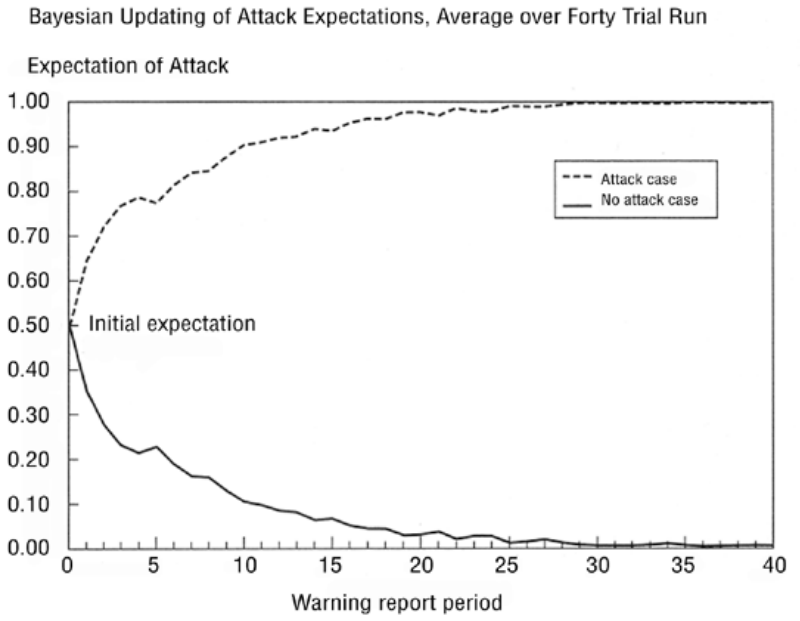
Initial and Revised Expectations of Hidden WMD (Given No Detection) Assuming a Detection System with 25 P
Types I and II Error Rates.

	Revised estimate given no detection													
Initial estimate [a]	Number of Negative reports: 1	2	3	4	5	6	7	8	9	10	11	12	13	14
0.0001	0.000													
0.001	0.000													
0.01	0.003	0.001	0.000											
0.05	0.017	0.006	0.002	0.001	0.000									
0.10	0.036	0.012	0.004	0.001	0.000									
0.20	0.077	0.027	0.009	0.003	0.001	0.000								
0.30	0.125	0.045	0.016	0.005	0.002	0.001								
0.40	0.182	0.069	0.024	0.008	0.003	0.001								
0.50	0.250	0.100	0.036	0.012	0.004	0.001								
0.60	0.333	0.143	0.053	0.018	0.006	0.002	0.001							
0.70	0.438	0.206	0.080	0.028	0.010	0.003	0.001							
0.80	0.571	0.308	0.129	0.047	0.016	0.005	0.002	0.001						
0.90	0.750	0.500	0.250	0.100	0.036	0.012	0.004	0.001						
0.95	0.864	0.679	0.413	0.190	0.073	0.025	0.009	0.003	0.001					
0.99	0.971	0.917	0.786	0.550	0.289	0.120	0.043	0.015	0.005	0.002	0.001			
0.999	0.997	0.991	0.974	0.925	0.804	0.578	0.314	0.132	0.048	0.017	0.006	0.002	0.001	
0.9999	0.999	0.997	0.992	0.976	0.932	0.821	0.604	0.337	0.145	0.053	0.016	0.006	0.002	0.00

a. Degree of belief in the hypothesis "weapons of mass destruction exist."

Example 1 of Bayesian updating

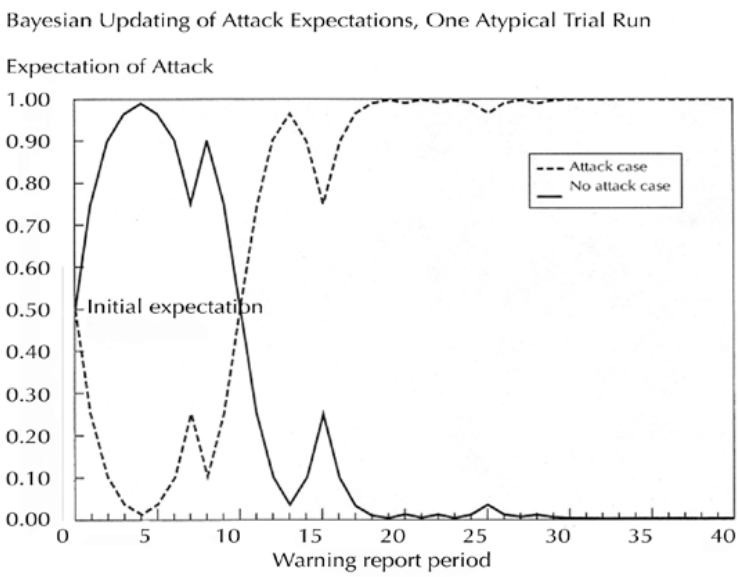
Perhaps one imagines that a decision-maker would do better never to have such a fixed idea with a probability of 99.9%. The second example illustrates graphically the degree of conviction he or she would properly infer, as intelligence data came in one at time, in the case of attack or no attack.



Example 2 of Bayesian updating

Even in this example, something like 17 data points would be required on the average to raise the expectation of attack from 50% to 95% (averages over a 40-trial run) if an attack were truly in process.

But these are only averages. If now one looks at an atypical trial run, one can see that in case of an attack, four data points, all reporting "no attack," reduce the inferred probability from 50% to only about 2%, whereas an attack was really in process, and the data ultimately (on the 17th repeated sampling) correspond to 99% probability of attack.



These are truly cautionary findings, little understood by analysts or decision-makers.

Indeed, not every piece of intelligence data has the same value or the same Type-1 and Type-2 error rate. All the more reason for each piece of data to be identified with its assumed rates, and the analyst and decision-maker should be able to use a simple tool such as a spreadsheet in order to determine not by "group think" but for himself or herself the likely spread of probabilities of what the intelligence data may seem so strongly to imply.

In conclusion, science and technology have revolutionized intelligence, as they have changed most aspects of modern life. At the national and international level, the consequence of actions that might be taken on the basis of intelligence (and the consequences of inaction) can be enormous, imposing a heavy load of responsibility on officials charged with the provision and interpretation of intelligence. Better preparation of such officials would be desirable, but is difficult because relatively few in the educated population are accustomed to dealing quantitatively with uncertainty, and there is the difficulty that persons who occupy a position of power are too busy exercising that power to take the time to learn something new or even vital. Perhaps new tools of simulation and video presentation might be devised to provide virtual experience with examples close to the problem at hand- attack or no attack; the decision to prevent a person from traveling on a commercial flight; the cancer risk posed by this or that environmental contaminant.