Tomorrow's Spygames[1]

Jack Devine

In this globalized and rapidly changing world, the future of intelligence will be marked by significant strategic, tactical, and technologieal change over the ncxt quarter century. Near unimaginable advances in technology will alter the intelligence landscape, with innovation driving faster access to more accurate information by friends and foes. Partly in response to this more complex, interconnected environment, the American Intelligence Community will enter a period of consolidation as various agencies are further centralized under the leadership of a future secretary of intelligence. A consolidated intelligence entity with diverse capabilities, under the leadership of a cabinet level authority, and hopefully, somewhat more free from the bureaucracy, turf battles, and politics of today's Intelligence Community, will enhance America's ability ro protect its interests.

Despite the unavoidable, uncontrollable, and at times unpredictable tides of change, several key components of the intelligence business will remain constant – as they have throughout the history of organized society. Intelligence agencies will continue to rely on high quality agents to gain insight into the plans and intentions of enemies; sources will still have to be spotted, developed, recruited and run by operators in the field.

Economic intelligence will increase in importance as a top concern of businesses and nations. Objective analysis will remain paramount. Finally, intelligence sharing among allies will continue to be a vital aspect of the process.

Since the earliest days of America, spying has been used to gain unique insights. While the ethical challenges of deception and betrayal often make people uncomfortable, these are critical facets of human intelligence collection endeavors. Even our country's leaders have at times expressed discomfort. Former Secretary of State Henry L. Stimson once remarked: "Gentleman do not read each other's mail."[2] A noble thought, but not very relevant today since the reins of power are rarely in the hands of gentlemen, and since our adversaries have no compunction abont clandestine activities, including using teehnology to gain access to telephone and Internet communications.

Henry L. Stimson

In fact, globalization and technological advances have produced a major upswing in intelligence activities by virtually all nations. Never before have so many intelligence agencies – as well as individuals – had the technieal capability and skill to monitor and manipulate information. Advancing technology will only deepen the pool of information available to people who might use it to do harm or gain advantage.

The Internet already has revolutionized intelligence collection in ways that are not fully understood or appreciated. Virtually unlimited access to open source intelligence has leveled the playing field between traditionally strong and weak services, and has brought into the intelligence industry an army of analysts that share information on a real-time basis. The extraordinary accessibility of public information has placed a significant premium on nonpublic information – or "intelligence" – that fills in the vitally important data missing from the analytical mosaic. This is the task of spying.

As we look over the horizon to 2033, spying will remain a very robust business both in terms of human and signals intelligence, or in terms more familiar, in recruiting spies and secretly intercepting the communication of adversaries. So, too, will the practice of imagery collection, using satellites to photographically capture and record our enemies' activities and movements. Furthermore, we will continue to see striking juxtapositions between modern technology and the age old tactics of intelligence collection. Many of us who partieipated in the Afghan war in the 1980s are convinced that the introduction of the then

1. Article first appeared in the *World Policy Journal*, Fall 2008, Vol. 25, No. 3. It is reprinted here with permission. All rights reserved.

2. As secretary of state under Herbert Hoover, Stimson closed the Department of State's code-breaking office, the so-called Black Chamber, in 1929. He later justified his action with this remark.Stimson and McGeorge Bundy, *On Active Service in Peace and War*, p. 188 . Also see David Kahn, *Codebreakers*, p. 360.

"ultrasophisticated" Stinger missile broke the will of the Russians and led to their retreat from Afghanistan. Some even argue that the use of this technology was the straw that broke the camel's back, leading to the later fall of the Soviet Union entirely. It is interesting to note, however, that these high-tech weapons were transported across the rugged territory by mules herded from China. Remember, too, that though the Afghan mujaheddin were tough and determined fighters, very few of them had formal military training. The ability to adapt new technologies for use in places where transport and other infrastructure is nonexistent will continue to be a critical element of the intelligence future well into the twenty-first century.

Intelligence Collection and Action

In addition to the well-known spying activities fictionally detailed by John le Carré and Ian Fleming, there are real operational heroes whose feats equally match the fictional Jason Bourne or James Bond. To cite but one case, the American, British, and French intelligence services have all paid homage in recent years to a heroic intelligence operator from the World War II era. Virginia Hall, British by birth, fluent in French, and an avid game hunter to boot, was one of the brave leaders of the organization of the French resistance to Nazi Germany. Of course, such activity for a young woman in these days was rare, risky, and courageous. Add to this the fact that she was an amputee who lost one of her legs in a hunting accident in Turkey, and you have the makings of a true legend. She parachuted into Nazi occupied France with her artificial leg strapped over her shoulder and went on to become the Nazi's "Most Wanted" resistance fighter in France.

Les Marguerites Fleurirent ce Soir
by Jeffrey W. Bass, Oil on Canvas, 2006
Collection of CIA.
The painting portrays Hall in the early morning hours, radioing London from an old barn near Le Chambon sur Ligon to request supplies and personnel. Power for her radio was provided by a discarded bicycle rigged to turn an electric generator, the clever invention of one of her captains, Edmund Lebrat. Coded messages such as "Les marguerites fleurirent ce soir" (the daisies will bloom at night) apprised Hall of what airdrops to expect from London and when. After D-Day, a Jedburgh team joined her, and together they trained resistance forces to wage guerrilla warfare. OSS Director William Donovan awarded Virginia Hall the Distinguished Service Cross—the only one given to a civilian woman during that war. Hall later worked for the CIA, serving in many jobs as one of CIA's first female operations officers.

Similar feats of duty and daring were replicated in allied intelligence services' more recent efforts in Afghanistan after the 9/11 attacks when, along with U.S. Special Forces, field operators and a small military contingent demolished the Taliban leadership and forces in a matter of days. That heroism is yet to be fully recorded, and it will be even longer before the details are declassified and made available to the public. Nonetheless, bold actions like these will be required by our Intelligence Community well into the future.

It is also worth mentioning lesser known intelligence activities, such as economic and counterintelligence, which will likewise remain a constant in the intelligence landscape for the next 25 years and beyond. The Office of the Director of National Intelligence now estimates that corporate America has been targeted by 140 countries for intelligence collection, and the number is expected to grow. Close to half of all Fortune 500 companies report some version of economic espionage against their assets, and the annual cost to American companies is estimated to be close to $20 billion.

The Chinese are well known for undertaking economic collection operations in the United States in support of their government's technological, financial, and military goals. The FBI reports that numerous Chinese front companies exist simply to collect overt economic and other types of intelligence on key international targets, both in the public and private sectors. According to a 2005 statement by an FBI official involved in combating these activities, one-third of all economic espionage investigations are linked to Chinese government agencies, research institutes, or businesses. Examples abound of both Chinese-Americans and expatriates under investigation for the alleged theft of trade secrets from shadowy, unknown Silicon Valley computer technology firms which are primarily conduits for information to major Chinese military and defense contractors. Moreover, suspects have been apprehended for espionage activities in places less obvious, including Louisiana, New Jersey, Virginia, New York, and Hawaii. Many of these suspected agents have been detained at airports in California, their luggage filled with computer chips and incriminating evidence of their activities, as they prepare to flee the country.

Among members of the global Intelligence Community, the French are similarly renowned for their economic collection capabilities and successes. In the late 1980s, according to media reports, the French intelligence service was reportedly engineering several

"blaek bag" jobs every day in fine hotels in Paris and Niee. The usual routine would eonsist of a elandestine break-in and entry, followed by the theft of a briefcase or computer. Given the types of people generally targeted for these operations, the information collected was likely highly sensitive and financially valuable. In fact, business executives, influential politicians and other leaders, even celebrities, are ofren subject to scruriny when traveling. Business travelers today are regularly advised to keep their laptops, mobile devices and documents locked away and to store sensitive data on external drives kept on their person ar all times. Despite new information seeurity precautions, these hotel room operations persist. Nor too many years ago while visiting the Middle East, one Central Intelligence Agency (CIA) offieer returned to his hotel room and observed a man's leg dangling from the ceiling as he struggled to exit before he was spotted. Under the cireumstances it was best to ignore the faux pas.

Of course, high-quality analysis of the intelligence collected from spies, whether human or technological, will also remain a vitally importanr feature of the intelligence landscape. Analyzing the behavior and activities of America's enemies has been, and will remain, a central elemenr of the political world. A tribute to human fallibility, analysis has not always been done with consistency and alacrity. Insighrful analysis stems from the quality of the analysts, their training, and importantly, their leaders. Leaders must continue to provide a consistent, analytical framework and professional culture characterized by objectivity and independenee.

As any national security decision-maker knows, independent analysis is critical to the integrity of the produet. Politicizarion must be absent from the process and policymakers must refrain from inrerfering for political gain. The need for reliable, insightful, and objective analysis is as important today as it will be a quarter century from now. To drive home this point, the founders of the CIA wisely etched inro the wall of Langley's entrance a quote from the New Testament: "For ye shall know the truth, and the truth shall make you free." The mantra is simple and spot on. The essence of good analysis is the ability and freedom to rake a tough-minded and objective view of reality. In the future, politieal leaders need to better understand that this serves their best interests and, above all, the interests of the American people.

The Inrelligence Community has just passed through an exrremely difficult period in this regard, bur there is growing and renewed appreciation of the principle. It is very likely that for many years to come there will be push-baek from the Intelligenee Community on any effort to undermine this analytieal discipline. There is a stronger, healthier mindset developing among members of the Intelligence Community who will not stand for political influence in the future.

Politics and Intel

On the political front, fairly predictable constants will continue to mark America's intelligence activiries abroad. First, let's look ar Russia, our foremost adversary in rhe last century who, particularly after its invasion of Georgia, seems increasingly likely to be a leading adversary over thc next 25 years. Russia's renewed nationalism represents the beginning of anothcr phase of the U.S.-Russia relationship. Oil wealth, the abandonment of socialist economic policies, and a restored but still-flawed political order have placed Russia back on the main stage. We can anticipatc that the Russians will assiduously guard their strategic interests, especially in border areas and former Soviet states.

But, we will not see a return of the Cold War. The revolutionary communist ideology rhat drove many Soviet leaders and rheir followers is dead. Russians have seen for themselves thc downside of a closed, Marxist economy. It is safe ro say that despite the economic troubles former Soviet states have experienced, rheir citizens prefer an economy in which they can participate in private enterprise and where market forces, not the whims of their leaders, govern.

A number of Russia watchers in the Intelligence Community believe we missed an opportunity in the aftermath of the Cold War to embrace Russia more vigorously and to draw it solidly into the Western camp. Whether or not this analysis is eorrect, the United Srates faces another turning point in its relationship with Moscow as the Kremlin leadership consolidates its reinvigorated power. We can choose a path of partnership or confrontarion.

In eirher case, high-quality intelligenee will be needed to gauge more effeetively Moscow's plans, intentions, and eapabiliries to avoid a confrontation. Moreover, we can expect Russia to continue to strongly support and grow its own intelligence capaeities. In the wake of rhe collapse of the USSR, the Russian inrelligence service fell into disarray, accompanied by an unpreeedented decline in the nation's labor force. Security and intelligence services have slowly reorganized and rebuilt themselves, most recently under rhe patronage of Prime Minister Vladimir Putin. The SVR (the renamed former KGB) is close to regaining

its precollapse influence and the FSB (the internal service, similar to the American FBI) has regained most of its power as well.

Likewise, we are at an important turning point in our relationship with China that will help to define our intelligence interests and capabilities over the next 25 years. The 2008 Olympics served Beijing's domestic aims of using patriotic nationalism to shore up the Communist Party's popularity and legitimacy but did not give China the boost in international prestige that it and many others expeeted. Pre-Olympic protests and violence in Tibet, denial of Internet access to the international press, and embarrassing flaps over digitized fireworks and a lip-synching little girl at the opening ceremony reminded the world in many ways of China's shortcomings. The Olympics were an important reminder that China's political system – still out of sync with democratic standards – will continue to be its Achilles' heel. Regrettably, the world has been fixated primarily on the huge economic opportunity that China represents and has turned a blind eye to its politics or its militaryintelligence capabilities and priorities.

As we move forward in this century, China's domestic politics will become inereasingly problematic, and internal opposition to the government could result in serious civil strife and unrest. China's state-run news agency reports more protests every year, with tens of thousands of "mass ineidents" – some of them violent – occurring in 2006. The U.S. Intelligence Community will remain alert for serious craeks in the system, watching for disruptions that could erupt with little warning and cause economic and politieal destabilization worldwide. To avoid this outcome, the Chinese leadership will have to open up their political system to the liberal ideals its citizens and foreign critics have lobbied for, or else it risks becoming inereasingly repressive, intent on quieting dissenters who will continue to undermine the country's eommunist foundation. Such a turn would undoubtedly result in investment flight and a major downturn in the Chinese economy that would have global financial repercussions.

In the same contcxt, Western intelligence services need to be alert to the very serious counterintelligence challenges that the Chinese represent. In 2001, the FBI tripled the size of its China unit. Of the many intelligence services operating in the United States, China's is pcrhaps the most worrisome. Numerous media reports detail the FBI's eoncerns about Chinese expatriates, visiting students, and even Chinese-Americans engaged in economic intelligence collcction either on behalf of the Chinese government, or organized criminal groups engaging in intellectual property theft, counterfeiting, and piracy.

High-tech Espionage

As we shift to the variable aspeets of the intelligence world over the next 25 years, clearly, the greatest changes will occur in the realm of technology as we advance further into the computer age, but other changes including the rise of energy and warer security issues, the restructuring of the Intelligence Community itself, and shifting multilateral eollaborations will also mark the future landscape.

We should anticipate that there will be extraordinary technological advances in the tools currently at the disposal of the analyst and the operator alike. "Spymasters," as case officers are known in the industry, will see an amazing array of miniaturized "nanogadgets" become available for use. We should anticipate that a Blackberry-type device will be encrypted and miniaturized to a point where it can be concealed in a writing pen or eyeglasses and that it will take verbal and digitally transmitted commands for the communication of data to an agent, who will likewise reeeive it on a similar device. These gadgets will enhance our abilities to encrypt and conceal all forms of eommunications with clandestine sources.

Technology will also improve the security of Ameriean intelligence officers, as communication with spies has always been the most difficult and dangerous aspect of agent handling. Historically, communicating with agents has often left an identifiable trail which could lead to an agent's arrest – the written record from which often provided the evidence to compromise the agent in court. In addition, old modes of communication often provided enemies with an opportunity to identify and harm individuals who assisted American intelligence officers.

Similarly, we should anticipate major breakthroughs in capturing communications to protect our national seeurity. We should expect the increasing use of potentially intrusive tools such as audio and visual devices that penetrate walls and allow sights and sounds to be captured undetected. The computer world is already susceptible to offsite penetration using such devices as "sniffers" (nearly invisible programs similar to eomputer worms that capture information transmitted in a network system). Advances made in malicious computer software and networking capabilities will likely result in the creation of "malware" that is virtually undetectable – and

our capacity to identify and eliminate these threats must grow as well.

New laws on wiretapping, signals intelligence and computer attaeks have come into play in recent months relating to collection and privacy. Government surveillance of American citizens suspected of being linked to terrorist groups, as well as activities including data mining and electronic wiretapping, which cast an even wider net, will continue to be a point of contention in the United States, both from a security perspective and from the perspective of civil liberties. Though laws are being revised and tightened to provide more effective oversight and authorization protocols, the civil liberties v. national security debate will likely persist for the next 25 years, especially as communications technology becomes more sophisticated, accessible, and undetectable. To avoid a loss on both fronts, American policymakers and intelligence professionals should harness such technological advances to develop surveillance techniques which can filter for false positives and exclude irrelevant data (or that protected by privacy laws), while at the same time strengthening oversight measures, authorization processes, and grievance procedures.

Cyber Warfare

Returning to the theme of computers' role in the future, it is noteworthy that 15 years ago, the Intelligence Community began to appreciate fully the impact that modern technology would have on intelligence, and the threats and opportunities it represented. This awareness as well as the resources committed to technology has greatly increased, along with parallel gains in the collection of sensitive high-value intelligence. Recently, members of the Intelligence Community have expressed growing concern about how technological advances, especially in the arena of the Internet, impact military warfare. We don't have to fast forward very far to recognize the important role that cyber warfare will play in future wars.

Indeed, the 2008 Russia-Georgia conflict represents the first time cyber attacks accompanied an actual armed conflict, and there have been several other incidents since. Various nonprofit groups that monitor the Internet for malicious activity, as well as private sector and official agencies, reported significant attacks on various Georgian government websites in the weeks leading up to the outbreak of armed conflict. In some cases, government websites were in a sense hijacked, with hackers replacing official government communications with what some analysts believed was Russian propaganda. In 2007, Russia and Estonia fought a war entirely in cyberspace, with high-volume attacks effectively overwhelming Estonian systems – virtually shutting down networks at the prime minister's office and at the Defense Ministry. Though the technology employed in both cases did not appear highly advanced, these cyber attacks are only the tip of a rapidly developing iceberg. In the future, cyber attacks that disable an adversary's communications, weapons, and other systems will have the potential to determine the outcome of wars.

It is important to recognize that cyber war will also extend beyond government entities, as 90 percent of our national security infrastrueture is in the hands of the private sector. Addressing cyber threats to America's infrastructure will necessarily require a new collaboration between the Intelligence Community and the businesses that help run the country's roads, mobile phone networks, bridges and electricity grids. *National Journal* reported last year that, as far back as 2005, the Department of Homeland Security, the agency responsible for protecting America's civilian computer systems, suffered nearly 850 attacks over a two-year period. Two of the agency's unclassified network servers were found to have been breached by a program designed to steal passwords.

In late 2007, the Bush administration asked NSA and DHS to protect government and civilian communication networks from hackers, especially Chinese, and gave the initiative a $144 million budget. In January 2008, President George W. Bush signed two presidential directives that called for the establishment of a concrete, comprehensive cybersecurity plan. President Bush's 2009 budget asked for close to $6 billion to be used to develop a highly confidential system that would protect national cyber security, and President Obama has continued this initiative. The resources devoted to strengthening America's security in terms of technology and cyber threats will increase exponentially in the coming quarter century. In this case, thankfully, the Intelligence Community has recognized the threat early on, before a catastrophic event centers attention on the issue. Over the next 25 years, it can be expected that the United States will retain its leading edge, developing and implementing revolutionary technologies to bolster domestic security and national interests abroad.

Security and Civil Liberties

In terms of human intelligence, major changes loom on the horizon. Databases of all sorts are

expanding at an exponential rate and it will only be a matter of years before analysts and operators will be able to review complete and comprehensive personal profilcs of their targets. From these advanced databases, we will be able to determine not only a target's basic biographieal data, but also day-to-day living patterns – shopping, reading, entertainment, and travel habits, as well as sensitive medical histories, and personal routines. We also will see commercial initiatives to imbed global positioning systems (GPS) and medieal data chips into the human body for personal safety and medical reasons. Inevitably, this new teehnology will be applied in the government arena as well – as a means of tracking citizens and their personal data.

While today there are powerful database tools, such as *LexisNexis*, most of this databasc information is eoncerned with commercial property, litigation, and media records. There are no databases whieh incorporate the private data that is so revealing about our personalities. This is not to say attempts have not been made. In 2002, the Information Awareness Office was established by the Dcfense Advanced Researeh Projeets Agency (DARPA). As a branch of the Dcpartment of Defense, the office was intended to bring together several DARPA information teehnology projeets to create a mega databasc that would build "Total Information Awareness." Supporters of the office elaimed the system would help the United States combat asymmetric threats, especially from terrorists. Critics countered that the deployment of such teehnology eould potentially lead to an illegal mass surveillance system and political 'opposition researeh' databasc.

Public outcry against this database project was so strong that, in 2003, Congress halted funding for the initiative, though funding for other technologies researched by the Information Awareness Office remain in play. These types of battles over civil liberties restrictions will surely continue across the next 25 years, no doubt, but over time this type of project will surely be revisited. The task for intelligence professionals will be to eompete in this arena in a manner that ensures the protection of personal data from those who do not have a true national seeurity need for the information. The test for democratic institutions will be to calibrate a balance between security, civil liberties, and human rights that enjoys broadbased public support.

Advanees also will be made in the behavioral seiences that will greatly enhance the ability to do "stand off" evaluation of the pathology of individuals. Brainwashing and mind control have long been research topics for the CIA and foreign serviees alike. While these taetics appeared to have fallen out of favor in the late 1960s, therc apparently is renewed interest in them, here and abroad. This is clearly a troublesome development and should be a cause of concern. In the hands of unscrupulous individuals these techniques might be used to interview, interrogate, or evaluate targets, counterparts, and colleagues alike. Concerns aside, however, most nations, and certainly our adversaries, will be pressing the limits in this field, and it is hard to imagine that we would not keep pace, preserving our strategie edge.

One unanticipated aspeet of America's response to this rapidly changing landscape will be further consolidation and centralization of intelligence agencies. It is axiomatic that, to maximize our effectiveness, our intelligence resourees must be properly managed, organized, and led. There is awareness among intelligenee practitioners and eustomers alike that the existing bureaueratic system isn't working well enough, and that a serious adjustment needs to be made.

Reform and Prevention

As it stands, the American intelligence system is bloated with redundant layers of management – each programmed to protect its own turf. Regrettably, it will probably take another major intelligence failure or international catastrophe to force a full and serious evaluation of the organization of the Intelligence Community. Given recent history, we will probably not have to wait too long for this to happen.

Assuming a bipartisan evaluation can be done wisely, it is likely that in the end policymakers will return to what the original architects envisioned in 1947 when the CIA was established. If unencumbered by polities and bureaucratic history, it will be possible for policymakers to take a fresh look at how best to build an Intelligence Community and, in the process, rediscover the wisdom of the founders who emphasized a eentralized agency supported by a structure organized around three basic pillars of intelligence: eolleetion, analysis, and technology.

The Intelligence Reform and Terrorism Prevention Act of 2004, and a new executive order which marginally enhanced the Director of National Intelligenee's eontrol over the current 16 intelligence agencies, appear to be a small step in this direction. But a bolder more dramatic reorganization will be needed, hopefully well before 2033, ro centralize and streamline the Intelligence Community, sharpening

its effeetiveness and greatly reducing its size.

With such reform likely on the horizon, a powerful secretary of intelligence will be needed to provide leadership and authority of the new entity. He or she will have predominant eonttol over all aspeets of intelligence collection and analysis. This leadership role will be a challenging one, partieularly given historical resistance to putting the va tious intelligence agencies – the National Security Ageney (NSA), the Defense Intelligence Agency (DIA), the National Reconnaissanee Office (NRO), and the National Geospatial-Intelligence Agency (NGIA) – under civilian control.

The secretary of intelligence will likely have full authority over all covert action activities currently managed by CIA as well as the military's "ptepara-tion of battlefield" intelligence activities, which are deemed "quasi-eovert" action. An effective sectetary of intelligence will also bave budgetary and resource control over the FBI's intelligence division. Over the next 25 years, growing interest in spinning off this rcsponsibility and creating a domestic security service modeled on the British Security Service (MI5) may very well result in the creation of an American equivalent; especially should there be another devastating attack on the United States.

Last, and in a broader sense, we should anticipate in the coming years that intelligenee liaison relationships between allies and friendly intelligence services will be enhanced, and that new multilateral intelligenee groups will be developed to face down global ehallenges, much like a beefed-up version of *Interpol*, the 186-member nation police ageney that currently coordinates eross-botder law enforcement investigations. These alliances may not be as solid or long-lasting as in the past, and strategic allies may change issue to issue, tather than from eountry to country. The Europeans clearly are moving in this direction and the United States will not be far behind in structuring robust multilateral intelligence relationships of its own, with the EU and other allies.

Black Swans

It is critical to factor into onr over-the-horizon planning the international variables that are likely to kick in duting the coming years. It is necessary that we align our intelligence resources with an informed strategic view of the future. Where possible, as in the cases of China and Russia, we should set our collection priorities aecordingly. Foreeasting is a risky and unpopular business in the Intelligence Community, but it must be done in order ro be well-positioned for change. Over the years, the community has become increasingly tactical in its planning activities and now focuses almost exclusively on current issues: today's inbox. In fairness, many intelligence professionals also recognize the uneven past performance in fote-seeing seismic changes on the world scene and the practical shortcomings of "conventional wisdom." In the 1990s, no one was focusing sharply enough on a catastrophie terrorist attack on American soil, nor on the prospect of wars in Itaq and Afgbanistan, or more recently on a resurgent nationalistic Russia.

Recognizing the potential for what the scholar and writet Nassim Taleb coined a "blaek swan" – an event that comes out of nowhere and tilts the world order – the need for creative but reality-based assessments in the intelligence world is great. For example, preventing a significant weapon of mass destruction attack in the United States from sovereign or non-sovereign forces should be a top intelligence priority for years to come. We must consider the difficult questions: was the 9/11 attack the high point in Al Qaeda's capabilities? Will such challenges peter out as other terrorist threats have in the past, in Latin America and Europe in the 1960s and '70s? Or will Al Qaeda regroup, inspire new rectuits, and pull off a dramatic, catastrophic, and/or sustained attack in the United States?

No matter what scenario unfolds, the American Intelligence Community must remain appropriately focused on this issue if there is to be any hope of preventing the next 9/11. It's clear that Russia, China, and Islamic tetrorism will remain eritically important threats throughout the next quarter century. But how these challenges to our national security will play out depends greatly on our policies in dealing with the future. The Obama administration has an opportunity to enact additional policies that address these known threats. It will also have the opportunity to lay the cornetstone for the future of intelligence, while building the structute and priorities that sutround it. This is not to say that the Intelligenee Community should be focused solely on Russia, China, and Islamic terrorism. The community, as well as the new Obama administration, needs to also consider the possibility of a nuelear Pakistan ruled by anti-Western extremists, unresolved issues between Israel and its neighbors, an empowered and nuclear Iran, as well as North Korea's military intentions and proliferation gamesmanship.

Where else might a black swan appear that tilts strategic thinking during the coming years? A reasonable suggestion might be in the economic arena. While we are busy measuring the politieal landseape of today

to forecast tomorrow, we need also to invest in intelligence collection and analysis to evaluate worldwide economic threats and financial developments. This arena has historically been an underinvested component of the intelligence world. If the last few years have taught us anything, the global economy is much more complex and vulnerable than generally perceived, with a capacity to rock institutions and individuals alike. The interlocking pieces are so complicated that it is extremely difficult to forecast even short-term economic trends. There is a growing awareness of this problem in the Intelligence Community and it is very likely that more time and effort will have to be devoted to it. This substantial effort will require the hiring of university MBAs, finanee, and economics majors who understand the many intricacies of global markets. It likewise will necessitate the recruitment of foreign agents imbedded in the international economie world. It will take years to hone this capability.

The coming decades will bring other unanticipated surprises to which policymakers and members of the Intelligence Community will have to respond and adapt. The possibility of a black swan event can never be discarded, and the Intelligence Community must boost its efforts to think creatively about future threats, including those which could dramatically impact American and global economies. How we structure our effort, allocate resources, and apply technological breakthroughs should be the basis for serious bipartisan discourse in Congress, the executive branch, and among the American public at large.

Jack Devine a career clandestine services officer of the Central Intelligence Agency, headed the agency's Afghan Task Force from 1985–1987, and served as the CIA's acting deputy director of operations. He is currently president of The Arkin Group, a New York-based intelligence consulting firm. He is a longtime member of AFIO.
This article is reprinted by permission of the author and the World Policy Journal where it first appeared in Fall 2008. It is available online at *http://www.mitpressjournals.org/doi/pdf/10.1162/wopj.2008.25.3.1*