

The Washington Post

[Back to previous page](#)

U.S. spy network's successes, failures and objectives detailed in 'black budget' summary

By Barton Gellman and [Greg Miller](#), Published: August 29

U.S. spy agencies have built an intelligence-gathering colossus since the attacks of Sept. 11, 2001, but remain unable to provide critical information to the president on a range of national security threats, according to the government's top-secret budget.

The \$52.6 billion "black budget" for fiscal 2013, obtained by The Washington Post from former intelligence contractor [Edward Snowden](#), maps a bureaucratic and operational landscape that has never been subject to public scrutiny. Although the government has annually released its overall level of intelligence spending since 2007, it has not divulged how it uses the money or how it performs against the goals set by the president and Congress.

The 178-page budget summary for the National Intelligence Program details the successes, failures and objectives of the [16 spy agencies](#) that make up the U.S. intelligence community, which has 107,035 employees.

The summary describes cutting-edge technologies, agent recruiting and ongoing operations. The Post is withholding some information after consultation with U.S. officials who expressed concerns about the risk to intelligence sources and methods. Sensitive details are so pervasive in the documents that The Post is publishing only summary tables and charts online.

"The United States has made a considerable investment in the Intelligence Community since the terror attacks of 9/11, a time which includes wars in Iraq and Afghanistan, the Arab Spring, the proliferation of weapons of mass destruction technology, and asymmetric threats in such areas as cyber-warfare," Director of National Intelligence [James R. Clapper Jr. wrote in response to inquiries from The Post](#).

"Our budgets are classified as they could provide insight for foreign intelligence services to discern our top national priorities, capabilities and sources and methods that allow us to obtain information to counter threats," he said.

Among the notable revelations in the budget summary:

- Spending by the CIA has surged past that of every other spy agency, with \$14.7 billion in requested funding for 2013. The figure vastly exceeds outside estimates and is nearly 50 percent above that of the National Security Agency, which conducts eavesdropping operations and has long been considered the behemoth of the community.

- The CIA and the NSA have begun aggressive new efforts to hack into foreign computer networks to steal information or sabotage enemy systems, embracing what the budget refers to as “offensive cyber operations.”
- Long before Snowden’s leaks, the U.S. intelligence community worried about “anomalous behavior” by employees and contractors with access to classified material. The NSA planned to ward off a “potential insider compromise of sensitive information” by re-investigating at least 4,000 people this year who hold high-level security clearances.
- U.S. intelligence officials take an active interest in friends as well as foes. Pakistan is described in detail as an “intractable target,” and counterintelligence operations “are strategically focused against [the] priority targets of China, Russia, Iran, Cuba and Israel.” The latter is a U.S. ally but has a history of espionage attempts against the United States.
- In words, deeds and dollars, intelligence agencies remain fixed on terrorism as the gravest threat to national security, which is listed first among five “mission objectives.” Counterterrorism programs employ one in four members of the intelligence workforce and account for one-third of the intelligence program’s spending.
- The governments of Iran, China and Russia are difficult to penetrate, but North Korea’s may be the most opaque. There are five “critical” gaps in U.S. intelligence about Pyongyang’s nuclear and missile programs, and analysts know virtually nothing about the intentions of North Korean leader Kim Jong Un.

Formally known as the Congressional Budget Justification for the National Intelligence Program, the “top-secret” blueprint represents spending levels proposed to the House and Senate intelligence committees in February 2012. Congress may have made changes before the fiscal year began on Oct 1. Clapper is expected to release the actual total spending figure after the fiscal year ends on Sept. 30.

The document describes a constellation of spy agencies that track millions of surveillance targets and carry out operations that include hundreds of lethal strikes. They are organized around five priorities: combating terrorism, stopping the spread of nuclear and other unconventional weapons, warning U.S. leaders about critical events overseas, defending against foreign espionage, and conducting cyber-operations.

In [an introduction](#), Clapper said the threats facing the United States “virtually defy rank-ordering.” He warned of “hard choices” as the intelligence community — sometimes referred to as the “IC” — seeks to rein in spending after a decade of often double-digit budget increases.

The current budget proposal envisions that spending will remain roughly level through 2017 and amounts to a case against substantial cuts.

“Never before has the IC been called upon to master such complexity and so many issues in such a resource-constrained environment,” Clapper wrote.

An espionage empire

The summary provides a detailed look at how the U.S. intelligence community has been reconfigured by the massive infusion of resources that followed the 2001 attacks. The United States has spent more than \$500 billion on intelligence during that period, an outlay that U.S. officials say has succeeded in its main objective: preventing another catastrophic terrorist attack in the United States.

The result is an espionage empire with resources and a reach beyond those of any adversary, sustained even

now by spending that rivals or exceeds the levels at the height of the Cold War.

The current total budget request was [2.4 percent below that of fiscal 2012](#). In constant dollars, it was about twice the estimated size of the 2001 budget and 25 percent above that of 2006, five years into what was then known as the “global war on terror.”

Historical data on U.S. intelligence spending is largely nonexistent. Through extrapolation, experts have estimated that Cold War spending probably peaked in the late 1980s at an amount that would be the equivalent of \$71 billion today.

Spending in the most recent cycle surpassed that amount, based on the \$52.6 billion detailed in documents obtained by The Post plus a separate \$23 billion devoted to intelligence programs that more directly support the U.S. military.

Lee H. Hamilton, an Indiana Democrat who chaired the House Intelligence Committee and co-chaired the commission that investigated the Sept. 11 attacks, said that access to budget details will enable an informed public debate on intelligence spending for the first time, much as Snowden's disclosures of NSA surveillance programs brought attention to operations that had assembled data on nearly every U.S. citizen.

“Much of the work that the intelligence community does has a profound impact on the life of ordinary Americans, and they ought not to be excluded from the process,” Hamilton said.

“Nobody is arguing that we should be so transparent as to create dangers for the country,” he said. But, he added, “there is a mind-set in the national security community: ‘Leave it to us, we can handle it, the American people have to trust us.’ They carry it to quite an extraordinary length so that they have resisted over a period of decades transparency. . . . The burden of persuasion as to keeping something secret should be on the intelligence community, the burden should not be on the American public.”

Experts said that access to such details about U.S. spy programs is without precedent.

“It was a titanic struggle just to get the top-line budget number disclosed, and that has only been done consistently since 2007,” said [Steven Aftergood](#), an expert at the Federation of American Scientists, a Washington-based organization that provides analyses of national security issues. “But a real grasp of the structure and operations of the intelligence bureaucracy has been totally beyond public reach. This kind of material, even on a historical basis, has simply not been available.”

The only meaningful frame of reference came in 1994, when a congressional subcommittee inadvertently published a partial breakdown of the National Intelligence Program. At the time, the CIA accounted for just \$4.8 billion of a budget that totaled \$43.4 billion in 2012 dollars. The NSA and the National Reconnaissance Office, which operates satellites and other sensors, commanded far larger shares of U.S. intelligence budgets until years after the Cold War ended.

During the past decade, they have taken a back seat to the CIA.

The NSA was in line to receive \$10.5 billion in 2013, and the NRO was to get \$10.3 billion — both far below the CIA, whose share had surged to 28 percent of the total budget.

Overall, the U.S. government spends 10 times as much on the Defense Department as it does on spy agencies.

“Today’s world is as fluid and unstable as it has been in the past half century,” Clapper said in his statement to The Post. “Even with stepped up spending on the IC over the past decade, the United States currently spends less than one percent of GDP on the Intelligence Community.”

Dominant position

The CIA’s dominant position is likely to stun outside experts. It represents a remarkable recovery for an agency that seemed poised to lose power and prestige after acknowledging intelligence failures leading up to the 2001 attacks and the 2003 U.S.-led invasion of Iraq.

The surge in resources for the agency funded secret prisons, a controversial interrogation program, the deployment of lethal drones and a huge expansion of its counterterrorism center. The agency was transformed from a spy service struggling to emerge from the Cold War into a paramilitary force.

The CIA has devoted billions of dollars to recruiting and training a new generation of case officers, with the workforce growing from about 17,000 a decade ago to 21,575 this year.

The agency’s budget allocates \$2.3 billion for human intelligence operations and \$2.5 billion to cover the cost of supporting the security, logistics and other needs of those missions around the world. A relatively small amount of that total, \$68.6 million, was earmarked for creating and maintaining “cover,” the false identities employed by operatives overseas.

There is no specific entry for the CIA’s fleet of armed drones in the budget summary, but a broad line item hints at the dimensions of the agency’s expanded paramilitary role, providing more than \$2.6 billion for “covert action programs” that would include drone operations in Pakistan and Yemen, payments to militias in Afghanistan and Africa, and attempts to sabotage Iran’s nuclear program.

The black budget illuminates for the first time the intelligence burden of the wars in Afghanistan and Iraq. For 2013, U.S. spy agencies were projected to spend \$4.9 billion on “overseas contingency operations.” The CIA accounted for about half of that figure, a sum factored into its overall \$14.7 billion budget.

Those war expenditures are projected to shrink as the United States withdraws forces from Afghanistan. The budget also indicates that the intelligence community has cut the number of contractors it hires over the past five years by about 30 percent.

Critical gaps

Despite the vast outlays, the budget blueprint catalogues persistent and in some cases critical blind spots.

Throughout the document, U.S. spy agencies attempt to rate their efforts in tables akin to report cards, generally citing progress but often acknowledging that only a fraction of their questions could be answered — even on the community’s foremost priority, counterterrorism.

In 2011, the budget assessment says intelligence agencies made at least “moderate progress” on 38 of their 50 top counterterrorism gaps, the term used to describe blind spots. Several concern Lebanon’s Hezbollah movement, an enemy of Israel that has not attacked U.S. interests directly since the 1990s.

Other blank spots include questions about the security of Pakistan’s nuclear components when they are being transported, the capabilities of China’s next-generation fighter aircraft, and how Russia’s government leaders

are likely to respond to “potentially destabilizing events in Moscow, such as large protests and terrorist attacks.”

A chart outlining efforts to address key questions on biological and chemical weapons is particularly bleak. U.S. agencies set annual goals for at least five categories of intelligence collection related to these weapons. In 2011, the agencies made headway on just two gaps; a year earlier, the mark was zero.

The documents describe expanded efforts to “collect on Russian chemical warfare countermeasures” and assess the security of biological and chemical laboratories in Pakistan.

A table of “critical” gaps listed five for North Korea, more than for any other country that has pursued or is pursuing a nuclear bomb.

The intelligence community seems particularly daunted by the emergence of “homegrown” terrorists who plan attacks in the United States without direct support or instruction from abroad, a threat realized this year, after the budget was submitted, in [twin bombings at the Boston Marathon](#).

The National Counterterrorism Center has convened dozens of analysts from other agencies in attempts to identify “indicators” that could help law enforcement officials understand the path from religious extremism to violence. The FBI was in line for funding to increase the number of agents who surreptitiously track activity on jihadist Web sites.

But a year before the bombings in Boston, the search for meaningful insight into the stages of radicalization was described as one of the “more challenging intelligence gaps.”

High-tech surveillance

The documents make clear that U.S. spy agencies’ long-standing reliance on technology remains intact. If anything, their dependence on high-tech surveillance systems to fill gaps in human intelligence has intensified.

A section on North Korea indicates that the United States has all but surrounded the nuclear-armed country with surveillance platforms. Distant ground sensors monitor seismic activity and scan the country for signs that might point to construction of new nuclear sites. U.S. agencies seek to capture photos, air samples and infrared imagery “around the clock.”

In Iran, new surveillance techniques and technologies have enabled analysts to identify suspected nuclear sites that had not been detected in satellite images, according to the document.

In Syria, NSA listening posts were able to monitor unencrypted communications among senior military officials at the outset of the civil war there, a vulnerability that President Bashar al-Assad’s forces apparently later recognized. One of the NRO’s functions is to extract data from sensors placed on the ground near suspected illicit weapons sites in Syria and other countries.

Across this catalogue of technical prowess, one category is depicted as particularly indispensable: signals intelligence, or SIGINT.

The NSA’s ability to monitor e-mails, phone calls and Internet traffic has come under new scrutiny in recent months as a result of disclosures by Snowden, who [worked as a contract computer specialist for the agency](#) before stockpiling secret documents and then fleeing, first to Hong Kong and then Moscow.

The NSA was projected to spend \$48.6 million on research projects to assist in “coping with information overload,” an occupational hazard as the volumes of intake have increased sharply from fiber-optic cables and Silicon Valley Internet providers.

The agency's ability to monitor the communications of al-Qaeda operatives is described in the documents as “often the best and only means to compromise seemingly intractable targets.”

Signals intercepts also have been used to direct the flight paths of drones, gather clues to the composition of North Korea's leadership and evaluate the response plans of Russia's government in the event of a terrorist attack in Moscow.

The resources devoted to signals intercepts are extraordinary.

Nearly 35,000 employees are listed under a category called the Consolidated Cryptologic Program, which includes the NSA as well as the surveillance and code-breaking components of the Air Force, Army, Navy and Marines.

The NSA is planning high-risk covert missions, a lesser-known part of its work, to plant what it calls “tailored radio frequency solutions” — close-in sensors to intercept communications that do not pass through global networks.

Even the CIA devotes \$1.7 billion, or nearly 12 percent of its budget, to technical collection efforts, including a joint program with the NSA called “CLANSIG,” a covert program to intercept radio and telephone communications from hostile territory.

The agency also is pursuing tracking systems “that minimize or eliminate the need for physical access and enable deep concealment operations against hard targets.”

The CIA has deployed new biometric sensors to confirm the identities and locations of al-Qaeda operatives. The system has been used in the CIA's drone campaign.

Spending on satellite systems and almost every other category of collection is projected to shrink or remain stagnant in coming years, as Washington grapples with budget cuts across the government. But the 2013 intelligence budget called for increased investment in SIGINT.

Counterintelligence

The budget includes a lengthy section on funding for counterintelligence programs designed to protect against the danger posed by foreign intelligence services as well as betrayals from within the U.S. spy ranks.

The document describes programs to “mitigate insider threats by trusted insiders who seek to exploit their authorized access to sensitive information to harm U.S. interests.”

The agencies had budgeted for a major counterintelligence initiative in fiscal 2012, but most of those resources were diverted to an all-hands emergency response to successive floods of classified data released by the anti-secrecy group WikiLeaks.

For this year, the budget promised a renewed “focus . . . on safeguarding classified networks” and a strict “review of high-risk, high-gain applicants and contractors” — the young, nontraditional computer coders with

the skills the NSA needed.

Among them was Snowden, then a 29-year-old contract computer specialist whom the NSA trained to circumvent computer network security. He was copying thousands of highly classified documents at an NSA facility in Hawaii, and preparing to leak them, as the agency embarked on the new security sweep.

“NSA will initiate a minimum of 4,000 periodic reinvestigations of potential insider compromise of sensitive information,” according to the budget, scanning its systems for “anomalies and alerts.”

Julie Tate contributed to this report.

© The Washington Post Company