Produced by:

Government Business Council

Sponsored by:

mastercard

Disruption Pays Off

Why One Agency Chose Smart Disruption And Never Looked Back

In a recent demonstration attended by three of the nation's top intelligence officials, an unnamed CIA analyst logged into a computer, downloaded a DevOps workspace application from the cloud marketplace, and proceeded to populate the environment with real data — all within the span of a few minutes.[1] For those in attendance, the implications were astonishing: what one year ago would have taken 'nine to twelve months' to purchase, procure, test, and integrate had just been executed from start-to-finish in the time it takes to brew a pot of coffee.

How did the nation's premier intelligence agency do it? The answer lies in smart disruption.

At a time when federal agencies face looming budget cuts[2], workforce reductions[3], and escalating pressure[4] by lawmakers to meet public demands, the CIA's technological leap forward is a vivid illustration of one agency bucking the status quo and rising to the challenge. While many in government continue to mark progress with incremental gains, the CIA (and Intelligence Community-at-large) are changing the playbook one bold investment at a time, providing other agencies a prime lesson in disruption payoff. The story hints at a larger shift happening across the federal government, one made possible by new technology but propelled by mission demands.

Disruption In The Cloud

Four years ago, the CIA's leadership faced a dilemma. The federal government had announced its intention to pursue a cloud-first policy, and the CIA's license as an

independent agency and the sensitive nature of its mission could have easily afforded them time and financial leeway to prop up a multibillion-dollar cloud infrastructure of their own.[5] But, against all expectations, they went a different path.

"What we were really looking at was time to mission and innovation," according to one former intelligence official. "The goal was, 'can we act like a large enterprise in the corporate world and buy the thing that we don't have, can we catch up to the commercial cycle?' Anybody can build a data center, but could we purchase something more?"

In a radical departure from its risk-averse nature, the CIA instead signed a 10-year, $600 million dollar contract with commercial outsider Amazon Web

Services (AWS) to develop a secure, private, on-campus cloud platform capable of relaying some of the most classified information on the planet.[6]

The decision predictably ruffled some in the IC who were accustomed to owning and maintaining all assets of the intelligence process. Doug Wolfe, who served as Chief Information Officer at the time of the signing, said it was important not to dismiss these concerns out of pocket, but rather treat them with continuing earnestness: "Some of the typical government challenges about how you contract and pay for this thing, how do you deal with security, what data can go where and why… these are the kinds of questions that we continuously have to answer."[7]

Wolfe's team worked to address the concerns of 'server-huggers', pointing out that consolidating agency data under a single infrastructure actually posed less risk than storing data on multiple older data centers. Jason Hess, Chief of Cloud Security at the National Geospatial-Intelligence Agency (NGA), says the CIA's decision mirrored his own agency's motivation to migrate to the cloud: "We're investing less in commodity and more in prosecuting the business of intelligence. We're able to focus on the meat and potatoes of intelligence and not spinning disks." That, he says, has led to more "consistent security across the board."[8]

There's no doubt Wolfe and other CIA leaders saw the risk in bringing in an outside partner to safeguard top-secret intelligence. But as a *Defense One* article described in great detail, penetrating the AWS network successfully amounts to a nearly impossible task. "It took a lot of wrangling, but it was easy to see the vision if you laid it all out," says one former intelligence official. "We decided we needed to buy innovation."[9]

Fast forward a few years, and it's easy to see how the purchase has paid off. Building on the success of the Commercial Cloud Services (C2S) platform, earlier last year AWS launched its commercial cloud marketplace for the IC, a virtual hub dedicated to providing spy agencies with the latest commercial solutions and innovative products. The IC Marketplace, as it is most commonly known, allows IC members to download and evaluate security-vetted software, tools, and applications as their work demands. What's especially innovative is its try-before-you-buy capability, enabling analysts to quickly install applications in minutes, play them against different datasets, and only then determine if they're worthy of purchasing for more extended use.

> "You hear so many people on the fence about cloud, and then to see the CIA gobble it up and do something so highly disruptive…it's kind of cool."
>
> **John Pirc, former CIA Cybersecurity Analyst**

According to CIA Chief Information Officer John Edwards, that kind of freedom is unprecedented: "Once you have that [application], it works with my mission data, and it solves a problem. I can lease that for as long as I want, and use for as little or as long as I want to. I can buy exactly what I need, for exactly as long as I need it."

And if it doesn't meet the specific mission need? "If it doesn't," says Edwards, "[then] we blow up that instance and download something else." With 100 applications currently available and a reported 70 more in the pipeline, IC analysts have plenty of opportunities to 'sandbox' their new tools.

That capability also means agencies can evade the software licensing hurdles which Government Accountability Office (GAO) estimates is responsible for billions of dollars in overspending by the federal government each year.[10,11] And because AWS fully owns and operates the cloud's hardware, the CIA no longer has to pay for maintenance or upkeep; rather, just for what they actually use.

However, money is just one factor. For those involved in national security, mission takes precedence, and delivering expedient results can often mean the difference between life and death. John Pirc, a former cybersecurity analyst at CIA, puts it in stark terms:

"profits aren't lost when you make mistakes in the intelligence community — people die when you make mistakes."

To that end, the CIA's partnership with AWS dramatically changed its mission capabilities. By way of the IC Marketplace, mission units can now bypass nearly all of the hurdles that plagued classic system acquisitions of the past. "It used to take the CIA 180 days to provision a single server," says Edwards. "Through virtualization, we got that down to 60 days and thought, 'we're doing pretty good.' Now through AWS and C2S, we're down to minutes. That's amazing."

On top of this, every improvement Amazon makes to its public cloud marketplace can now be easily replicated and introduced to the classified C2S, ensuring it stays up-to-date and protected from the latest threats. CIA has high confidence in the security of its cloud for other reasons: for one, the C2S cloud is never connected to the Internet, sharply reducing the penetration vector from online threats. Second, AWS has worked with CIA to provide extra security overlays, segmenting the cloud across "three geographically dispersed zones of availability." Finally, the CIA ensures all solutions in the marketplace are properly vetted to meet FedRAMP requirements and other national security baselines.[12]

"I'm never going to say anything you do in the cyber world is totally invincible, but this is pretty close," Edwards says. "We took a hardened cloud on the outside, [and] dropped it behind our guards, gates and guns. I would argue [...] this is the most secure thing out there. It's a game-changer for us, I don't think anything out there is any more protected."

As they say, the proof is in the pudding. Cloud adoption among agencies has increased 200% year over year, the IC has upped its computing power by 1400% since 2015, and a new DevOps factory in C2S now enjoys the assistance of over 4,000 full-time developers.[13]

With An Eye Toward The Future

"You hear so many people on the fence about cloud, and then to see the CIA gobble it up and do something so highly disruptive, it's kind of cool," says Pirc. "To me, this removes the clouded judgment that cloud isn't secure. Their moving forward with this should send a message to the rest of the industry that cloud is something you shouldn't be afraid of."

As more agencies find emerging technology capable of satisfying baseline security requirements, previously secondary considerations like performance, agility, and scalability will gain greater appeal to those interested in disrupting the status quo. The DoD's creation of the Defense Innovation Unit (DIUx) in Silicon Valley is the most recent example of this development, its stated mission being "to accelerate the development, procurement and integration of commercially-derived disruptive capabilities."[14] Likewise, the NSA's Commercial Solutions for Classified (CSfC) program has radically accelerated the security assurance pipeline for agencies to access and deploy the latest in commercial technology.[15]

As a result of these initiatives, a significant performance gap could open up over time between agencies that commit to disruptive innovation and those that don't, but are rather content to remain at the shallow end of the pool. However, those who find safety in the status quo arguably put themselves at greater risk by imagining a future that still plays by current conventions.

And this is decidedly *not* the future that's in store. Consider a few of the innovations just around the corner:

- **Artificial intelligence (AI):** Late last year, the White House announced its commitment to promoting artificial intelligence research, with key investments in machine learning, automation, and big data analytics.[16] Experts anticipate AI could save government $41 billion annually and free up 1.2 billion hours of labor, enabling personnel to pursue more intellectually stimulating tasks.[17]

- **Improved digitization:** Advancements in natural language processing (NLP) and optical character recognition now make it possible to process massive amounts of data in record time. Spearheaded by their internal innovation accelerator Ignite, the Department of Health and Human Services (HHS) successfully piloted an

NLP categorizer to dramatically reduce the 1,000 hours traditionally required to process and classify public comments on regulations.[18] The agency credits the pilot with saving millions of dollars and improving employee satisfaction.

- **Mass mobility:** Mobile devices aren't exactly new to government, but recent breakthroughs in mobile finance management and user authentication offer disruptive capabilities not seen before. The next line of agency-issued handheld devices will allow personnel to digitally review and purchase goods on the move, file and upload expense reports, and approve purchase orders anytime, anywhere.[19]

These are just a few of the disruptive technologies that agencies could have in their arsenal going forward. As the CIA's own venture demonstrates, fortune favors the bold — and those agencies willing to take bold measures can set themselves up for success down the line. With reports of robotic wingmen[20], self-driving cars[21], and biologically inspired gecko-nanosuits[22] also on the horizon, this is government like we've never seen it before: disruptive, bold, and fearlessly devoted to mission.

Sources

[1] "How the CIA's cloud puts fresh tech at analysts' fingertips." *Nextgov:* December 14, 2016. http://www.nextgov.com/cloud-computing/2016/12/how-cias-cloud-puts-fresh-tech-analysts-fingertips/133897/

[2] "What Trump cut in his agency budgets." *The Washington Post*: May 23, 2017. https://www.washingtonpost.com/graphics/politics/trump-presidential-budget-2018-proposal/

[3] "Trump ends federal hiring freeze, but workforce cuts loom." *Government Executive*: April 11, 2017. http://www.govexec.com/management/2017/04/trump-ends-federal-hiring-freeze-workforce-cuts-loom/136942/

[4] "The high cost of Congressional demands for agency documents." *Government Executive*: April 14, 2016. http://www.govexec.com/oversight/2016/04/high-cost-congressional-demands-agency-documents/127498/

[5] "Federal Cloud Computing Strategy." White House: February 8, 2011. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

[6] "The details about the CIA's deal with Amazon." *The Atlantic*: July 17, 2014. https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/

[7] "CIA creates a cloud: An interview with CIA's Chief Information Officer, Doug Wolfe, on cloud computing at the agency." CIA: 2014. https://www.cia.gov/news-information/featured-story-archive/2014-featured-story-archive/cia-creates-a-cloud.html

[8] "What do US intelligence agencies and Netflix have in common? Both are Amazon cloud customers." *Nextgov*: June 26, 2015. http://www.nextgov.com/cloud-computing/2015/06/what-do-us-intelligence-agencies-and-netflix-have-common-both-are-amazon-cloud-customers/116440/

[9] "How to break into the CIA's cloud on Amazon." *Defense One*: July 7, 2015. http://www.defenseone.com/technology/2015/07/how-break-cias-cloud-amazon/117175/

[10] "Federal Software Licenses: Better management needed to achieve significant savings government-wide." GAO: May 2014. http://www.gao.gov/assets/670/663560.pdf

[11] "Agencies waste hundreds of millions on software." *Nextgov*: May 23, 2014. http://www.nextgov.com/cio-briefing/2014/05/agencies-waste-hundreds-millions-software/85144/

[12] http://www.fedramp.gov

[13] "CIA's cloud is 'pretty close' to invincible, CIO says." *Nextgov*: June 14, 2017. http://www.nextgov.com/cloud-computing/2017/06/cias-cloud-pretty-close-invincible-cio-says/138679/

[14] https://www.diux.mil/docs/work-with-us/DIUx-Commercial-Solutions-Opening-White-Paper.pdf

[15] https://www.nsa.gov/resources/everyone/csfc/

[16] "The National Artificial Intelligence Research and Development Strategic Plan." NSTC: October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf

[17] "AI could save government $41 billion, report says." *StateScoop*: May 11, 2017. http://statescoop.com/ai-could-save-government-41-billion-report-says

[18] "Increasing efficiency in rule making with natural language processing." HHS.gov. https://www.hhs.gov/idealab/projects-item/increasing-efficiency-in-rule-making-with-natural-language-processing/

[19] "Mobile Services Roadmap (MSCT Strategic Approach)." Mobile Services Category Team: September 23, 2016. https://assets.documentcloud.org/documents/3221622/MSCT-Strategic-Roadmap-DRAFT-STRATEGY-for-PUBLIC.pdf

[20] "The Pentagon is building robotic wingmen to fly alongside fighter planes." *The Washington Post*: June 14, 2017. https://www.washingtonpost.com/news/innovations/wp/2017/06/14/the-pentagon-is-building-robotic-wingmen-to-fly-alongside-fighter-planes/

[21] "Self-driving cars gain powerful ally: The government." The New York Times: September 19, 2016. https://www.nytimes.com/2016/09/20/technology/self-driving-cars-guidelines.html?mcubz=2

[22] "Z-man." Defense Advanced Research Projects Agency. http://www.darpa.mil/program/z-man