Defense Innovation Board: Public Feedback
Dan Green

Opportunity

On Monday 27 March, President Trump announced the establishment of the Office of American Innovation (OAI).[1] This provides the Defense Innovation Board a perfect opportunity to influence, align and champion a "whole of government" approach to innovation that accommodates the revitalization, modernization, broadening and deepening of the "Defense Industrial Base". It is an opportunity to review and validate the uniqueness of DOD requirements and help articulate the markets, sectors and rates-of-adoption that must be achieved to revitalize both Defense and dual-use industries.

I offer the following as constructive commentary on the Defense Innovation Board report from the perspective of a government implementer and engineer. Innovation is a rubric, or grand theme, and it is important that we have some agreed upon Terms of Reference to allow us to communicate effectively. We need to discuss innovation in its proper context and define how we will measure progress in terms that can be applied to Defense modernization, readiness and capability.

Innovation: Terms of Reference

In the aggregate I recommend we consider the theme of Innovation along four, mutually supporting pillars: (1) Technological (2) Organizational (3) Operational (4) Financial. Depending on the context of the initiative and the perspective of the "innovator", one of the pillars will dominate, and the others then serve as supporting functions. If all four pillars are not considered, adoption and sustainment of the innovation will be difficult. In DOD it might be useful for us to think of Innovation in terms of campaigns with "supported" and "supporting" elements in the same way we approach other military objectives and COCOM interaction.

A fifth component of an innovation cycle is the immutable context of Time. Time serves to normalize different efforts and provides a degree of precision to discussions about innovation. It has been my experience that the absence of Time as the dominant key performance parameter is the root cause of fiscal and labor inefficiency for innovative and traditional DOD modernization efforts.[2] In effect, the Department of Defense and the Federal Government as a whole are "Competing Against Time"[3] with adversaries and peer competitors who have access to the same technological baseline as we do.

---

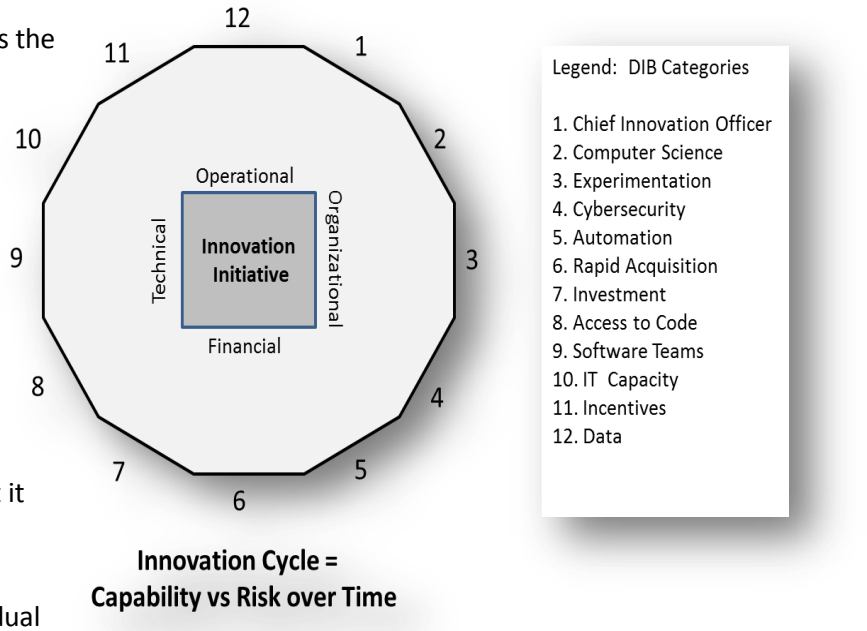
[1] https://www.whitehouse.gov/the-press-office/2017/03/27/presidential-memorandum-white-house-office-american-innovation

[2] Defense Acquisition (DODINST 5000.01/02) moved away from time-based modernization to performance-based modernization early in this century. In practice, rapid rate of technological change forced program managers to "freeze" requirements on older generation technological baselines in order to achieve procedural success. Our adversaries, and technology drivers themselves, do not conform to these artificial constraints.

[3] George Stalk Jr articulated this concept well in the book "Competing Against Time", first published in 1990.

Comparative Advantage goes to the early adopter and potential victory goes to those who create a culture of sustainable innovation adoption along the lines of the four pillars above.

To support a broader deeper dialog on Innovation I offer the following graphic utilizing the objectives from the Defense Innovation Board Report. Interestingly the Board came up with 12 categories of innovation. This lends itself to the metaphor of a clock which reinforces the notion that Time is on the critical path to innovation. The four pillars can be shown as "attributes" and are depicted inside the graphic to imply that the pillars belong in every conversation regardless of the initial thrust area. The clock metaphor also implies that no innovation category is inherently more important than the other, that it is a continuous process and that categories are part of a dynamic, interactive whole rather than individual stovepipes.



Innovation Cycle = Capability vs Risk over Time

Metrics

Once Innovation can be discussed in generally the same terms, it is most important that the DIB define metrics. Every project manager will attest to the fact that it is very easy to initiate a project and very hard to prove you have met expectations. Success metrics that show innovations contribution to improvement, not just change, can be developed to accommodate the priorities of the Administration, SECDEF and the implementers in the field. Like Innovation itself, specific success metric will be dynamic, however the categories of metrics (e.g., operational, financial, organizational, operational) help ensure specific metrics "roll-up" and are comparable between projects.

I recommend a Defense Innovation Board subcommittee be immediately established to adopt, refine or define a few foundational metrics categories either based on the pillars above or some other framework. This will allow the broad community of DOD related innovators to conceive and design their innovation proposals in ways that are testable. Without an agreement on metrics categories, units of measure, and timeframes, DOD will suffer through a great deal of innovation that is not feasible (e.g., noise) at the expense of focusing on those efforts which represent true modernization (e.g., signal). Metrics will help ensure the Signal to Noise Ratio is appropriate for the mission area, level of Risk, amount of time and the resources available.

Submitted: 29 Mar 2017 by Dan Green: US Navy

The Defense Entrepreneurs Forum (DEF) is an independent, 501(c)(3) registered, not-for-profit group of emerging defense and national security leaders (military, veteran, and civilian) who strive to solve national security problems from the bottom-up. Following the publication of the Defense Innovation Board (DIB) recommendations, the Defense Entrepreneurs Form gathered a cloud advisory unit to provide our view on how to move forward with the recommendations. This public comment submitted in advance of the DIB's April 4, 2017 meeting concerns the establishment of a Chief Innovation Officer (CINO) position in the Department of Defense (DOD).

Intro

We whole-heartedly support the DIB's recommendation to establish a Chief Innovation Officer within the DOD. The DOD is the world's biggest bureaucracy and bureaucracy is anathema to innovation. Innovation can exist within a bureaucracy but it cannot thrive without a champion to cultivate it. The right individual can fill that role and help the DOD retain its dominant global position through innovation.

Characteristics of the DOD Chief Innovation Officer

Assuming the CINO will possess neither a carrot (funding) nor a stick (authority) of any significance, they will be reliant on their powers of persuasion to inspire action toward innovation within the Department. For this reason, we recommend that the ability to influence others be one of the primary characteristics of the first DOD CINO. Second, we suggest that the first CINO be a DOD outsider who is willing to challenge the norms of the Department. Absent national defense bona fides, they should have a proven track record of innovation to establish credibility and be supported by a staff of DOD professionals who understand the dynamics of the Department. Third, they should be an integrator able to connect the innovators within and outside the Department as opposed to driving innovation themselves. Finally, the first CINO must have grit. They will face considerable resistance and disinterest. They must be able to persevere, and motivate others to do so, regardless of the obstacles and setbacks they encounter.

Role of the DOD Chief Innovation Officer

We see the role of the CINO as fourfold. The first responsibility of the CINO will be to foster a culture of innovation within the DOD. The Department's no-fail mission of defending the nation is contradictory to the trial-and-error method of innovative progress. However, few failures will truly jeopardize national defense. The CINO should identify the boundaries within which small, purposeful failures can be allowed and even encouraged. Those that venture into those areas in the name of innovation should not be penalized for their attempt.

Second, the CINO should be responsible for advocating for and distributing resources for non-standard innovation activities (e.g. those outside of research and development

labs). For instance, the CINO could distribute funds or other resources to those that win an innovation competition or hackathon. An example of a non-funding resource is access to physical or virtual ‘maker spaces’ in which innovators can obtain the materials, equipment, and expertise they need to realize their ideas. Alternatively, the CINO should also seek to remove exiting barriers to innovation. Inspiring innovation within DOD is not a problem; enabling its advancement is an issue. A combination of both approaches will do the most to stimulate innovation within the Department.

Third, the CINO should seek to identify innovative individuals, and their supporters, within the Department and find ways to connect them through a network of innovators. The CINO cannot rely on duty or office titles to find innovators nor on the current military personnel system to highlight them. Fortunately, when provided the opportunity, many of these individuals self-identify. If the CINO builds a channel of communication and collaboration, they will come. There is no shortage of good ideas for identifying and solving existing problems, big or small, and there are many creative members of the DOD workforce with disruptive ideas for moving the DOD forward. Except for those few islands of innovation that do exist, many of these ideas are simply lost in the ocean of bureaucracy. There are few, if any, resources available to the would-be innovator to help them understand how to bring their idea to fruition with DOD.

Finally, the CINO must own the narrative surrounding innovation within the DOD. This first means defining innovation with the DOD and ensuring it encompasses forward progress in the non-technical areas of policy, organizational structures, processes, and personnel management. We recommend innovation be defined as "the application of creative and critical thought to effect significant positive change and enhance operational outcomes." Owning the narrative also means recognizing and lauding innovative efforts to both internal and external audiences.

Conclusion

The U.S. military will struggle to maintain its dominant position if it is unable to innovate. Fortunately, innovation and innovators already exist within the DOD. However, the bureaucratic nature of the Department restricts them to unconnected islands. The establishment of a Chief Innovation Officer within the Department is the first step toward bridging those islands and ensuring they can grow and flourish.

The Defense Entrepreneurs Forum (DEF) is an independent, 501(c)(3) registered, not-for-profit group of emerging defense and national security leaders (military, veteran, and civilian) who strive to solve national security problems from the bottom-up. Following the publication of the Defense Innovation Board (DIB) recommendations, the Defense Entrepreneurs Forum (DEF) gathered a cloud advisory unit to provide our view on how to move forward with the recommendations alongside suggested leads. This public comment submitted in advance of the DIB's 4 April 2017 meeting concerns the recruitment and talent management of computer scientists within the US military.

Unstick Cyber

To begin to address the role of computer scientists in the US military, it is important to acknowledge that the DoD often inappropriately conflates the cyber and computer science fields. If a computer science career track is to be properly implemented, it will be important to "unstick" cyber from computer science. Therefore the road to implementation should be paved with an appreciation that as computer scientist job titles may vary, so do their content areas. Computer scientists work on computing systems; computer networks; user interface design; data structures and analysis; algorithms and programming fundamentals; software engineering; and mobile, web, and communications development to name a few facets. Yet most public policy research has focused on cyber implementations in the military. Therefore we rely on the principles that are coming out of cyber-aligned research to project its relevance to a broader discussion on computer science.

Pockets of Excellence

Pockets of excellence do exist for DoD computer science, but the profession as a whole is limited in the US military. Important allies for DIB will understandably be found at United States Cyber Command and subordinate Cyber Mission Forces. Examples of service-specific leaders include the Army Cyber Command, Cyber Center of Excellence, and the Capabilities Integration Center. DIB can also look to the service academies in their leadership on computer science like the Naval Academy Center for Cyber Security Studies and the Army Cyber Institute at West Point. Not to be overlooked are computer science-oriented organizations like NSA, SPAWAR, DISA, DIUx, and Defense Digital Service which just launched Code.mil. Outside the US military, the Department of Homeland Security sponsors the US Cyber Challenge and the CyberCorps Scholarships for Service program which aim to expand the recruiting pipeline.

Where DIB Can Influence the Short Term

- **Sponsor a Capture the Flag Exercise** -- Not just studying the principles of computer science, but actually enacting hands-on research, test, and development is a key element of recruiting and maintaining talent within the DoD. Potential testbeds for the DoD to explore are shortening software

development release times and giving teams the ability to craft their own software tools and deploy those tools to operational systems within the appropriate sandbox. Role models here are found in events like DI2E Plugfest, CyberDome, Network Integration Exercises, Army Warfighting Assessments, and Enterprise Challenges as prime outlets for demonstration of talent and the art of the possible. (Lead: Defense Digital Service)

- **Lend Star Power to Promote a Culture of Valor** -- It is important to tie computer science into military concept development and public affairs so there is larger understanding of where computer scientists in uniform play a role. Though the public at large is familiar with military veterans as heroes who do valorous work "over there", there is room to expand upon the warriors dedicated to computer science topics where it is just as easy to be valorous from the homeland. In order to disrupt the foggy impressions of what computer scientists do in the military, the DIB could play a more visible role in encouraging a broader civilian and military understanding of the centrality of computer science to today's warfighting missions. (Lead: DIB Members)

Where DIB Can Influence the Mid Term

- **Run A/B Tests to Improve Recruitment of Minority Candidates** -- In order to rely upon the fullest pool of talent available, the DoD will have to push extra hard to bring in participation from communities that are underrepresented in computer science professions. Carnegie Mellon, Harvey Mudd College and Stanford have all been standouts in turning around statistics on women in computer science, therefore A/B tests could be run mimicking their recruitment and talent management strategies to help uncover what the appropriate application to the military may be. (Lead: OSD P&R—Policy; Service Talent Management Task Forces—Implementation)

- **Ensure Cadre in Information Security is Proportional to Commercial Sector Best Practices** -- Intrusions into US networks have been costly and the DoD Defense Science Board warns of a future "death by 1,000 hacks."[1] In order to appropriately safeguard US computer science-based systems it will be imperative to ensure information security professionals develop alongside the larger computer science track in the US military. One examination found that as a percentage of the workforce, US military information security professionals lagged behind commercial sector practices, when it can be inferred that US military networks require even more information security professionals than the commercial sector.[2] (Lead: Defense Digital Services)

[1] http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf
[2] http://www.rand.org/pubs/research_reports/RR847.html

Where DIB Can Influence the Long Term

- **Explore a Block Structure That Allows the Ability to Specialize** -- Individuals aligned with computer science in their DoD service are computer scientists by education or interest, not by title, trade or profession. The absence of computer science as a core function of the DoD leaves computer scientists in the military without the ability to specialize. As a present day officer recommends in an Air & Space Power Journal article, "Having individuals remain current in a certain number of functional and technology classes would allow easy assembly of the right team for specific missions."[3] There is also proof that ongoing investment in training aids recruiting[4] and specificity in qualifications will help the services make requests for computer science talent by knowing the blocks of specialization that are accredited and at the ready for certain mission sets. (Lead: OSD P&R—Policy; Service Talent Management Task Forces—Implementation)

- **Allow Crossover in Rank** -- Though there is a perceived struggle to compete with the commercial sector for talent, there is evidence that a strong core of computer scientists already exists in the military who are not serving in computer science-based positions. The DIB should look to Reserve components as considerable untapped potential, particularly among the Cyber Protection Teams being established across the Army and Air National Guard. Establishing a way to allow crossover in rank for personnel trained in computer science in their civilian career would go a long way in meeting the initial establishment and basing of a DoD computer science career track. The added benefit of a crossover track is the effectiveness found in roping in talent that is already in the military and aligned with military culture and values. (Lead: OSD P&R—Policy; Service Talent Management Task Forces—Implementation)

DEF agrees with DIB's recommendation and commends the above pathways to leverage DIB strength to prepare the DoD for a future of warfare that is guaranteed to be increasingly software-centric. As the New York Times put forward in their 2020 Report—an examination of the future of their profession—their strategy for resiliency included being the news outlet with the most coders on staff. As DIB has emphasized, so too should the DoD make computer scientists a distinguishing feature of its preparations for 2020 and beyond. In conclusion, DEF looks forward to shaping a service culture where the percentage of computer scientists among DoD ranks is a point of pride and strength, rather than a hidden figure.

[3] http://www.au.af.mil/au/afri/aspj/airchronicles/apj/2011/2011-2/2011_2_04_franz.pdf
[4] https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161011_Reeder_CyberSecurityNinjas_Web.pdf

Rebuild Our Defenses for the Information Age

Trump's infrastructure upgrades could start at the Pentagon, which still uses 8-inch floppy disks

By Mackenzie Eaglen

The Wall St. Journal

March 21, 2017

President Trump has pledged to rebuild both America's military and its infrastructure—priorities that are more intertwined than they might appear. In the 21st century, "infrastructure" means more than roads, bridges and airports. Just as American life increasingly relies upon the virtual infrastructure of internet and satellite connectivity, so does the Pentagon.

The Global Positioning System is a prime example. The same GPS signal that helps you navigate around a traffic jam or lets your kids play Pokémon Go also guides the Air Force's smart weapons and enables American commanders to direct ground forces in battle. But much of this widely used technological infrastructure is out of date, unreliable or easily tampered with.

The Defense Department still uses 8-inch floppy disks and computers from the 1970s to coordinate nuclear forces, according to a report (http://www.gao.gov/assets/680/677436.pdf) last year from the Government Accountability Office. Many of the Pentagon's communications systems are so vulnerable to sabotage that the Army and Navy regularly practice fighting without them. Satellites can be shot down by missiles or have their sensors dazzled by lasers. Their ground links can be jammed or hacked.

Dale Hayden, a senior researcher at the Air Force's Air University, told an audience of aerospace experts earlier this month that proliferation of antisatellite technology has put America's communications networks at risk. "In a conflict, it will be impossible to defend all of the space assets in totality," he said. "Losses must be expected."

It has never been easier for America's adversaries—principally Russia and China, but also independent non-state actors—to degrade the U.S. military's ability to fight and communicate. Senior military officials have expressed grave doubts about the security of the Pentagon's information systems and America's ability to protect the wider commercial virtual infrastructure.

The U.S. Navy, under its mission to keep the global commons free, prevents tampering with undersea cables. But accidents—and worse—do happen. Last year a ship's anchor severed a cable in the English Channel, slowing internet service on the island of Jersey. In 2013 the Egyptian coast guard arrested three scuba divers trying to cut a cable carrying a third of the internet traffic between Europe and Egypt. "When communications networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt," warned a senior staffer to Federal Reserve Chairman Ben Bernanke in 2009. Trillions of dollars in daily trading depends on GPS, which is kept free by the Air Force.

There are now an estimated (http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated) 17.6 billion devices around the world connected to the internet, including more than six billion smartphones. The tech industry expects those numbers to double by 2020. That growth is dependent, however, on secure and reliable access to intercontinental undersea fiber-optic cables, which carry 99% of global internet traffic, and a range of satellite services.

The U.S. military is working on ways of making them more resilient. For instance, the Tactical Undersea Network Architectures program promises rapidly deployable, lightweight fiber-optic backup cables, and autonomous undersea vehicles (http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG808.pdf) could soon be used to monitor and repair cables. In space, the military is leading the way with advanced repair satellites as well as new (http://www.losangeles.af.mil/About-Us/Fact-Sheets/Article/343728/gps-iii) and experimental (http://aviationweek.com/awindefense/afrl-test-more-resilient-gps-technologies) GPS satellites, which will enhance both military and civilian signals.

Still, America is falling behind in its mission to keep the world's virtual infrastructure secure. In part that's because the Pentagon's own IT is in such dismal shape. Contractors buy computer parts on EBay (http://quotes.wsj.com/EBAY) for missile-defense systems, and the Navy pays Microsoft (http://quotes.wsj.com/MSFT) to support obsolete operating systems. Ancient hardware and software not only leave weapons vulnerable, they also hamper the efficiency of back-end business systems.

Earlier this month, I spent 10 hours trying to reset a password on an Army computer system so I could file financial disclosure forms. More than two million people work for the Defense Department. If only a fraction of them has had a similar experience, think of the time that the Pentagon's antiquated IT wastes. In the end, that increases the vulnerability of the front-line American soldier.

Investments in virtual infrastructure—to protect network connectivity and upgrade military information systems—could have economy-wide benefits. Recall that President Reagan's defense buildup in the 1980s not only restored America's military superiority, but helped juice recovery from the 1981 recession. It also pushed the American electronics, aerospace and communications industries toward international dominance.

A reprise of targeted investment in advanced IT—hardware and software—is overdue. Getting it right could mean more secure networks, more high-paying jobs and more technological breakthroughs in areas that will rule the commercial and military future.

Ms. Eaglen is a resident fellow at the American Enterprise Institute and a former House, Senate and Pentagon staffer.

https://www.wsj.com/articles/rebuild-our-defenses-for-the-information-age-1490138210
https://www.wsj.com/articles/rebuild-our-defenses-for-the-information-age-1490138210

To: Defense Innovation Board
From: Erin M Simpson, PhD
Re: Data recommendation
Date: 30 March 2017

Over the last ten years, I have had the opportunity to observe the collection and use of data in a wide variety of context across the Defense Department. As a counter-insurgency advisor in Afghanistan I worked with Marines to develop novel indicators of stability –and watched them ship hard drives full of data home to Camp Lejeune only to be erased. I later supported a number of big data programs at DARPA – some of which also provided operational support in Afghanistan. At one point, I believe we had the most extensive and best curated integrated data repository for the theater. It was scraped and collected by hand from dozens of different repositories at multiple levels of classification. I have no idea where it is now. And finally, in working on a 18 month project focused on urban operating environments and "megacities" my Caerus team talked to TSOCs, civil affairs teams, the Army corps of engineers, and a variety of others looking for the proverbial data pot of gold to support improved IPOE of these environments. Everyone was sure that someone else had it – but no one did.

These are but a few of the data collection and analysis efforts I have observed or participated in. And they serve as both a point of departure and a cautionary tale for future data integration efforts. What follows are some additional observations and initial recommendations as the Board moves forward with this idea.

1) There are a number of specific DoD efforts that would benefit from improved integration and access to data. Many of these are outside the traditional threat intelligence analyses conducted by intel staffs and therefore rely to greater extent on unclassified or open-source political and economic data (sometimes referred to as "white" or "green" data, vice enemy "red"). There are also opportunities to improve our understanding of our own (blue) activities in terms of operations and procurement. Some examples:

- -IPOE (unclassified white/green data)
- -"atmospherics" and other elements of influence analysis (unclassified white data mixed with red targets)
- -campaign analysis and operations research (classified blue data)
- -cost analysis (classified blue or proprietary data)
- -ISR optimization (classified blue)

But the data requirements and classification levels can vary widely. Choices will need to be made early on about what types of analysis/efforts are to be supported by an integrated data repository and which level of classification is best suited to those ends. The technical decisions must be mission driven with a clear understanding of who the "customer" is for this effort.

There are clear tradeoffs:

- -aggregating everything into a TS/SCI cloud environment is tempting as it allows all the data to be stored and analyzed in one place. But it is nearly impossible to move data to lower levels (even if they originated at those levels). And most of the DoD enterprise does not have JWICS access or TS/SCI clearances. This approach would be very limiting once you wanted to share products with regular units and offices operating at the Secret level on SIPR.
- -Moving everything to classified networks also limits the utility of many open-source programming packages like python and R (among others) as not all the component libraries are approved for use on SIPR and JWICS. Working on those networks also requires technical staff with those clearances, which are already in short supply.
- -An unclassified system would allow for the most flexibility with regard to software and commercial cloud solutions, but would by definition lack certain kinds of operational data (to say nothing of SIGINT or other SCI materials).

2) Raw data isn't always that helpful. Data arrive with differing levels of specificity: individual, country, annual, daily. Sensor data is often has a specific lat-long, but post-processing is often necessary to turn point data in to tracks or turn data on individuals into network analysis. Unit level reporting from the field can be terribly unstructured (but still very meaningful). Whatever repository is eventually established, resources should allocate to data cleaning, processing, and other ETL efforts to usefully serve up data products for non-technical users.

2a) Units returning from theater often have incredibly valuable information on their individual (classified) laptops. This is not always structured "data" per se, but can still be invaluable. Some of this is uploaded to the great sharepoint in the sky, but not everything. And the most useful things – detailed local information – is omitted, e.g, the number of nights the district governor slept in the district center, price of goods in the market, how long it takes (and how much it costs) for a truck to get to the provincial capitol. Those laptops are often wiped when units return to home stations, leading to significant losses in data and knowledge. A convenient, secure protocol to capture that data in theater for subsequent use would be invaluable. But that data in its raw form (spreadsheets, powerpoints, pdfs) may not be very useful for machine learning applications. Additional cleaning and processing will likely be necessary.

2b) Most data within the USG is organized by country or individual. There is no Lagos desk or Taipei team. NGA serves up some geolocated data, but it is not a full picture and the software architecture leaves a lot to be desired. For data integration efforts like those under discussion here to be successful, there needs to be more attention to hyper-local data that can be aggregated into a bigger picture. In particular, for units and commands focusing on "megacities" or other sub-national

areas of interest, data tagged to the country level are analytically unhelpful (especially if the area crosses international borders). Resources should be allocated to collecting, storing, and processing local, ground-level data - especially at the unclassified level. This is likely to come from open-source data whether scraped form online sources or purchased in bulk.

3) Of the many machine learning techniques available to analysts, most can be understood in terms of pattern analysis and anomaly detection. For either to work, there must be a "baseline" of what is normal for a given place or group. Leveraging baseline data requires passive and persistent collection of some sort. If that sounds expensive, that's because it is! It's also not how most of our intelligence collection is designed. More typically, we have a list of priorities (typically, known threats) and assign assets and collection against those. But if something happens in a place you weren't previously worried about, you won't have much data. Which means there is no baseline. And you can't backcast the data – you can only collect it going forward. A system that systematically collected various unclassified, geolocated data would be enormously helpful on this front, whether from unclassified news reports, purchased data, social media or other feeds. If this data were then served up to agencies and commands, it could provide valuable tipping and cuing of emerging crises and provide context once the red balloon goes up.

3a) Similarly, there is a need for parsing and processing the huge volume of written reports. Natural language processing and event detection/extraction techniques can greatly improve the usefulness of this massive backcatalog of textual information.

4) Intel shops primarily focus on "red" threat intelligence, focusing on bad guys and target packages. For all the purported gains in bottom-up intelligence and appreciation of "white" or "green" data, most staffs have returned to their more traditional role of providing threat analysis. Intelligence is a customer driven business: interesting questions generate interesting answers. If commanders are not asking for rich, detailed, and dynamic IPOE assessments or influence analyses, intel shops are unlikely to develop them. As such, these teams are unlikely to use or contribute to this repository unless pressed by their commanders. The success of this effort will depend on more than efforts by analytical teams; operators and combat arms commanders will need to be educated to demand more and better data from their staffs.

4a) One place where gains could be made is in developing the notion of "intel support to plans." Huge gains have been made over the last 15 years with regard to "ops-intel fusion" as a variety of units have engaged in deliberate and dynamic targeting, elevating the role of intelligence across units and commands. With lighter footprints around the world – and increasingly complex battlespaces – our military planning process should be supported with richer data and analysis.

5) At risk of improperly using a company or product name, I ask of you: please get us Google for SIPR.