

The AMERICAN INTEREST Publicity Copy

Spring (March/April) 2012, Vol. VII, No. 4

The following article, in whole or in part, may not be copied, downloaded, stored, further transmitted, transferred, distributed, altered or otherwise used, in any form or by any means, except:

- one stored electronic and one paper copy of any article solely for your personal, non-commercial use; or
- with prior written permission of The American Interest LLC.

To subscribe to our online version, visit www.The-American-Interest.com

To subscribe to our print version, call 1-800-767-5273 or mail the form below to:

The American Interest
P.O. Box 15115
North Hollywood, CA 91615



☐ BEST OFFER! Yes, send me two years (12 issues) of THE AMERICAN INTEREST for only \$69*. I'll save 23% off the cover price!

☐ Yes, send me one year (6 issues) for only \$39*. I'll save \$5.75 off the cover price.

Name

Address 1

Address 2

City

State

Zip

Country

E-mail

Credit Card

Exp.

Name on Card

Tel. No.

Signature

Date

*Please allow 4-6 weeks for delivery of first issue. Add \$14 per year for delivery to addresses in Canada and \$33 per year for delivery to addresses outside the U.S. and Canada.

- ☐ Payment enclosed
☐ Bill me later

A21PPC

CONTENTS

THE AMERICAN INTEREST • VOLUME VII, NUMBER 4, SPRING (MARCH/APRIL) 2012



THE NEXT AMERICAN REPUBLIC

- 5 **The Once and Future American Liberalism**
by Walter Russell Mead, with Gary Hart, James Q. Wilson & William A. Galston
The Blue Model is on the way out. What should come next?
- 22 **A Conversation with Peter Thiel**
Francis Fukuyama talks with the renowned entrepreneur.



WHO NEEDS DEMOCRACY?

- 32 **The Cultural Contradictions of Democracy**
by Vladislav Inozemtsev
The main threats to democracy lie within liberal societies themselves.
- 41 **Europe's Democracy Paradox**
by Ivan Krastev
Europe's crisis was set in motion by five revolutions in human affairs.



RUSSIA PROBLEMS

- 48 **Doing Well By Doing Right**
by David J. Kramer & Lilia Shevtsova
Some mythbusting about U.S. policy toward Russia.
- 54 **Putin, the Sequel**
by Thomas Graham
Putin's return means more of the dismal same for everyone.
- 58 **Eurasian Abrasions**
by Samuel Charap & Mikhail Troitskiy
Habits, not interests, are behind U.S.-Russian tensions in Central Asia.
- 63 **Who's a Russian?**
by Jeffrey Mankoff
It's not as straightforward a question as you might think.

HIGHER INTELLIGENCE

- 70 **Unfinished Business**
by Dennis C. Blair
Ten years after 9/11, intelligence reform is still a work in progress.



EXECUTIVE COMMITTEE

Francis Fukuyama, *chairman*
Charles Davidson, *publisher & CEO*
Walter Russell Mead, *editor-at-large*
& *director, The American Interest Online*
Eliot Cohen
Josef Joffe

Adam Garfinkle, *editor*
Daniel Kennelly, *senior managing editor*
Noelle Daly, *associate editor*
Lindsey Burrows, *assistant editor*
Damir Marusic, *associate publisher*
Andrew Iacobucci, *assistant to the publisher*
Erica Brown, Michelle High,
editorial consultants
Simon Monroe, R. Jay Magill, Jr., *illustrators*
cover design by Lindsey Burrows
cover photo of Peter Thiel
courtesy Robert Houser

EDITORIAL BOARD

Anne Applebaum, Peter Berger,
Zbigniew Brzezinski, Tyler Cowen,
Niall Ferguson, Robert H. Frank,
William A. Galston, Owen Harries,
G. John Ikenberry, Stephen D. Krasner,
Bernard-Henri Lévy, Sebastian
Mallaby, C. Raja Mohan, Ana Palacio,
Itamar Rabinovich, Ali Salem, Lilia
Shevtsova, Hiro Aida, Mario Vargas
Llosa, Wang Jisi, Ruth Wedgwood,
James Q. Wilson

ADVERTISING & SYNDICATION

Damir Marusic
damir.marusic@the-american-interest.com
(202) 223-4408

website

www.the-american-interest.com

Subscriptions: Call (800) 362-8433 or visit www.the-american-interest.com. One year (6 issues): \$39 print; \$19 online; \$49 for both. Two years (12 issues): \$69 print; \$38 online; \$98 for both. Please add \$14 per year for print-subscription delivery to Canada and \$33 per year for delivery to addresses outside the United States and Canada. Postmaster and subscribers, send subscription orders and changes of address to: *The American Interest*, P.O. Box 15115, North Hollywood, CA 91615. *The American Interest* (ISSN 1556-5777) is published six times a year by The American Interest LLC. Printed by Fry Communications, Inc. Postage paid in Mechanicsburg, Pennsylvania. ©2010, The American Interest LLC. Application for mailing at periodical pricing is pending in Washington, DC and additional mailing offices. Editorial offices: 1730 Rhode Island Ave. NW, Suite 707, Washington, DC 20036. Tel.: (202) 223-4408. Fax: (202) 223-4489.

80

Intelligence as a Service Industry

by Thomas Fingar

Austerity and partisanship could derail U.S. intelligence reform.

85

The Anonymity Virus

by John McLaughlin

Forget Wikileaks. The real scandal is anonymous government leaking.

87

A Few Knowledgeable Men

by Mark Lowenthal

U.S. intelligence fetishizes data-manipulation over understanding.

90

Data Overload

by Jennifer Sims

The intelligence community is drowning in a deluge of data.

94

Information Triage

by Ron Capps

We'll never be able to weed out leakers like Bradley Manning, but some common sense steps can reduce our risks.

REVIEWS

97

The Revolution Will Not Be Tweeted

by James Kirchick

Debunking the transformational power of internet freedom.

102

Little Brother Is Watching

by J.P. O'Malley

A lot more than money is at stake in internet-driven marketing.

108

Apocalypse Still

by Crawford Gribben

Two new books on millenarian thinking hit (too) close to home.

114

The Great Sea

by John F. Guilmartin, Jr.

A capacious history of the Mediterranean.

120

A Night in Arzamas

by Jordan Smith

How Tolstoy's obsession with mortality became a teachable moment.

NOTES & LETTERS

124

The Euromess: A Letter from Madrid

by Ana Palacio

A former EU parliamentarian and Spanish Foreign Minister sums up Europe's woes.

How to understand intelligence reform in an age of austerity.

Intelligence as a Service Industry

Thomas Fingar

Ubiquitous fictional depictions of dashing spies with expensive high-tech “toys” may be entertaining, but they tend to distort public understanding and inflate both fears and expectations of the U.S. Intelligence Community (IC). This distortion of reality engenders a belief that the IC is dangerously omniscient and capable of knowing and doing just about anything it wishes. Misguided or misinformed journalists exacerbate public mistrust, revealing the IC’s technical capabilities and reviling examples of bureaucratic bloat, redundancy and its purported inability to “connect the dots.” Even in normal times such mischaracterizations are unhelpful, but in a period of budgetary stringency inflected by political demands for magic-bullet solutions they have the potential to trigger “reforms” that will do more harm than good.

We do need reform, and we need to accomplish it within an IC budget that should be reduced as part of the broader effort to realign Federal government expenditures and revenues.

Thomas Fingar is the Oksenberg-Rohlen Distinguished Fellow at Stanford University. From 2005 through 2008 he served concurrently as Deputy Director of National Intelligence for Analysis and Chairman of the National Intelligence Council.

Nor should those reductions be left to the IC itself. Many in the IC support reductions in total spending only if their own authorities can determine how best to achieve mandated reductions. But precisely because intelligence is a support function, policymakers are obliged to specify where they are willing to accept the increased risks inherent in making decisions with less information.

Making such choices will not be easy. One of the reasons the IC budget has grown so much in the past decade is that politicians and policymakers have been no more willing to make tough choices on intelligence expenditures than on most other matters. Their demonstrated lack of will, and a political atmosphere in which simple—and often simple-minded—solutions play so well with the public, create a real danger that budget cuts will bring mandates to “fix” intelligence in counterproductive ways.

Preventing the wrong kind of reform should begin with an exercise in *dotology*: the careful study of dots. We need to pay particular attention to the mutual connectedness of dots, their ideal number, their protection, reliability, intelligence and future.

Connections: Fortunately, the U.S. IC is neither dangerous nor particularly incompetent, as these things go. But it is improvable. IC

professionals know their strengths and weaknesses and are willing (if not always eager) to embrace effective change. But they understand that fixing any specific shortcoming could create adverse consequences for other IC missions and responsibilities, because all the IC dots are connected to each other in one way or another. Those connections display certain inevitable tensions for the simple reason that the IC exists solely to support the missions and requirements of other U.S. government agencies whose purposes and interests are themselves in (we hope healthy) tension. The challenge, then, is to devise transformational reforms that accommodate competing demands; any proposed changes must avoid tradeoffs that improve performance or efficiency in some areas at the cost of degrading it in others. In other words, any proposed changes must factor in the impact on all the “dots” in the IC matrix.

How Many Dots? One obvious quick-fix reform that could be used to justify budget cuts would be to reduce the number of IC agencies. Why, many pundits scoff, do we need 16 intelligence agencies (17 if one counts the new National Intelligence Directorate)? Why not radically reduce the number, thus eliminating expensive duplicative effort and administrative overhead, at the same time simplifying the challenges of sharing and prioritizing information?

Reducing the number of agencies, especially going to the extreme of having just a single agency as some have proposed, would make the IC organizational chart neater and the IC more efficient in some bean-counting ways. But it probably would not deliver improved intelligence support to the IC’s diverse customers across the national security enterprise.

The structure of the IC is often depicted as a jerrybuilt house or Rube Goldberg machine. Such characterizations are only partially accurate. The current IC structure is admittedly the result of evolution, not intelligent design; if one likes an animal metaphor, IC structure looks more like a platypus than a gazelle. But there is logic to it nonetheless, which should not be surprising since evolution, after all, has a logic, too. That logic inheres in the fact that to be useful, intelligence support must be precisely tailored to meet the needs and timelines of specific customers. The Secretary of State requires very

different kinds of intelligence support than do those who design equipment and tactics for the Marine Corps, or those who track the financial transactions of terrorists and drug traffickers. Hence, different IC components focus on different issues and types of information, recruit and train people with different expertise and experience, and produce intelligence products with different emphases and perspectives. Deep understanding of the needs of particular customers and missions is essential for the “intelligence edge” demanded by national security decision-makers. One-size-fits-all intelligence is not very helpful to anyone; expecting the Secretary of Defense or the Attorney General to make use of intelligence collected and analyzed for the Secretary of the Treasury or Commander of U.S. Forces Korea is as impractical as it is undesirable.

Obviously, however, the current structure does generate predictable problems. Separate IC component cultures and competition among them foster rivalries that impede collaboration across organizational boundaries. And there is more duplication of effort than is necessary or desirable.

These simple observations carry an overarching implication for reform agendas: If organizational consolidations and other changes promote our intelligence edge as whole, they should be on the table; if they do not, the prospect of saving small chunks of money cannot justify the degradation of the range of capabilities that constitute that edge. As things stand now, only the Director of National Intelligence is positioned to make such judgments. The goal should be that all IC components function as parts of a single enterprise, but sustain the tailored provider-consumer intelligence relationships vital to keeping our edge.

In this regard, the establishment of the Director of National Intelligence is a necessary but insufficient step. Even if the incumbent DNI has the requisite authority and backing from the White House to effect desired changes—and this has not always been the case—determining precisely what those changes should be remains a formidable obstacle to effective change.

Protecting Dots: Unauthorized disclosure of sensitive information (leaks) is a perennial problem lately made many times worse by advances

in information technology that permit rapid downloading and dissemination of IC and other USG documents. In the aftermath of Wikileaks many have called for redressing a perceived imbalance between protecting and sharing information. In this climate, mandated changes could hinder the IC's ability to support its customers by producing work worthy of the money spent on intelligence collection and analysis.

Access to much of the information collected by the IC is limited because of the need to protect sources and methods. Disclosure of certain types of information would endanger the careers and even the lives of those who provide it. Revealing other types of information can jeopardize technical methods of collection and cut off access to critical sources. The need to protect sensitive information should be self-evident, but overclassification tempts those who handle sensitive information to bend the rules. Such behaviors, and other known manifestations of human fallibility, often trigger overcompensation in the form of even more stringent classification and handling requirements, leading to more bending of the rules, and so on *ad infinitum*.

All efforts to protect information, whether sensible or overzealous, complicate and can even thwart the purpose for which the information is collected: namely, to provide warning, reduce uncertainty and identify opportunities to protect or advance U.S. interests. Information that is collected but never delivered to those who need it negates the purpose and wastes the resources involved in collecting it in the first place. However, it is extremely difficult for collectors and stewards of information to know who in the IC, let alone in the national security enterprise as a whole, really "needs to know" any given piece or category of information. The default assumption has oscillated over time from access that is too strict to access that is too open; we have rarely got it just right both because there is an inherent tradeoff between using intelligence and protecting it, and because the technical circumstances of collection and dissemination keep changing.

Classification and other handling restrictions must exist to protect sources and methods, but that need differs from the requirements for

protecting the substantive content of intelligence reports. Some information is tightly held because revealing it automatically puts at risk the collection mechanism used to acquire it. In my experience, the percentage of intelligence in this category is extremely small. Most information can be discovered in multiple ways, many of them unclassified and available to anyone who takes the trouble to look for it. This makes it both possible and necessary to discriminate among the various parts of a report, perhaps providing greater protection to sourcing than to content. The challenge is to provide sufficiently stringent classification or handling restrictions to protect what most needs to be protected while at the same time making the report as useful as possible to analysts, decision-makers and operators.

Trust: Intelligence is a support function. Decision-makers rely on the IC to cope with uncertainty, and they value it enough to spend a great deal on it. The assumption is that more information and better analysis (not the same things, of course) will lead to better decisions and more effective policies. The IC is also the most disinterested source of input to national security decisions because it is barred by statute from advocating for or against particular decisions or policies. Its objectivity is arguably even more important to decision-makers than its access to classified information (much of which is collected specifically to address concerns of high government officials) because it gives the IC more and sometimes better insight into the problems being examined.

That said, reality is more complicated. Most decision-makers seem to employ a variant of Ronald Reagan's "trust but verify" approach to arms control arrangements, only applied to the IC. In other words, individual analysts and other professionals who interact with policy customers must earn the confidence and trust of those they support. Among other consequences, this often inclines policymakers to request as much "raw" intelligence as possible—enough to give them confidence that IC analysts have evidence to substantiate their judgments.

This understandable desire to verify IC analysis often plays out in the form of requests for additional information about sources and methods (otherwise known as "second

guessing”). That can sometimes be a problem, especially when intelligence support personnel recognize that the policymaker wants to use the information to press a case in a policy debate or diplomatic *démarche*. The competitive use of intelligence information in high policy circles is nothing new or rare, and it is often the source of politicized intelligence—a sin too often blamed on IC personnel themselves.

The best protection in cases like these is to refuse to disclose sourcing information to the officials who need to know the substance of what is reported. Collectors and security mavens rest easier when analysts in regular contact with their customers are trustworthy and transparent about other aspects of their analysis (how much information they have, from how many sources, how consistent it is, the assumptions used to close intelligence gaps, and so on). Then policymakers and other consumers will be confident that all available information has been analyzed in accordance with the highest standards of analytic tradecraft.

Trust and confidence are two-way streets. Analysts must also have confidence that those they support are willing to protect the information IC professionals share with them. If they lack such confidence, they will hold back in ways that distort understanding and erode trust in a particular analyst or in the IC as a whole. There is no simple formula for managing this tension, but both sides must be aware of it and seek balances that work for all concerned. Analysts can then convey substantive information and analytic judgments at levels of classification that make it easier for customers to use them (for instance, by making it possible for them to store analyses on their own computer networks and share it with subordinates and other decision-makers working on the same issues). With trust, customers can accept the word of analysts that judgments are supported by intelligence at higher or more restricted levels of classification than can be revealed in written or oral presentations. Without such trust, it is necessary to “show more of the homework” and thereby make it harder to share and in other ways utilize IC input.

The Future of Dots: One of the most frequent criticisms of the IC is that it devotes too much attention to current events and too little

to strategic analysis. It is certainly the case that the IC produces far more “current intelligence” than long-term assessments of how current developments and trends are likely to evolve, but that is what its customers demand most of the time. Most policymakers recognize, at least in theory, the importance of strategic analysis and know that better appreciation of long-term trends will increase the success of the policies they pursue during their terms of office. But most are slaves to their in-boxes, overwhelmed by immediate concerns, and unable to devote much time or effort to long-term planning. As one senior official memorably said to me when I brought him what I considered to be a particularly good analysis of trends through and beyond the next decade, “I’m sure it’s good, but I’m up to my ass in alligators and simply do not have time to worry about what is going to happen after my time in office.”

In other words, the demand for strategic analysis is small and, in my experience, gets smaller as an administration approaches the end of its four-year term. Relative disinterest in strategic analysis is paired with an insatiable appetite for current intelligence because no official wants to appear to be unaware of developments in his or her portfolio of responsibilities. Intelligence customers press their intel support teams for news that will enable them to stay on top of events and avoid embarrassment on the Hill or with the press.

Intelligence analysts should thus give customers not only what they want, but also what they need, in order to demonstrate utility and earn trust. Giving customers what they want means addressing subjects they ask about. It most emphatically does not mean cherry-picking intelligence or skewing judgments to please policy customers. Although instances of deliberate politicization are rare there is a tension between being responsive to customers and the imperative to tell them what they need to know, even if they don’t realize it. Some decades ago analysts were more confident than they are today to go beyond customer requests, and customers were more respectful and appreciative of IC personnel motives. We could use more of that today.

Dot Intelligence: Despite the limited market for strategic analysis, every analyst must think

strategically in order to properly interpret current developments. Good current intelligence must be assessed in the context of broader developments, secular trends, identification of key drivers and constraints and more. Otherwise the IC ends up producing information without insight or understanding about what the data mean. Many newly installed decision-makers tell their intelligence support team that they want only raw intelligence, not the judgments of analysts likely to be younger and less experienced than they are. “Just bring me the raw intelligence and I will figure it out myself” is a fairly typical attitude of those who have not previously been exposed to the huge volume of information collected by the IC, or who have not learned how to use its analytic resources. It does not take very long for most to discover that there are not enough hours in the day to be both policymaker and intelligence analyst.

The desire of policymakers to possess current information and raw intelligence puts a premium on speed, which, unfortunately, sometimes drives the IC to value velocity over veracity. It is relatively easy to identify developments and intelligence germane to the interests and instructions of a particular customer and to rush that information to the eager recipient. But doing so reduces current intelligence to little more than recapitulation of reported facts and denies the customer—and the national security enterprise as a whole—the benefits of assessment by experienced analysts and the ability to tap comparable and complementary expertise in other parts of the IC. This has many undesirable consequences.

One unfortunate consequence is that it exaggerates the importance of providing “warning” to decision makers. Warning is one of the IC’s most important functions, but when reduced to little more than the passing of undigested “news” to decision-makers without careful analysis of its validity, origins and implications, it compounds the “urgent in-box” problem and provides little help to customers who must decide what they need to do about the reported development. This drives the national security establishment toward *ad hoc* behavior, to which it is prone in any event.

A second undesirable consequence is that it causes some analysts, and some agencies

some of the time, to think that they have done their job when they have alerted decision-makers that something has happened or might happen. This allows them to claim to have “warned” officials if something untoward happens, but the result is so much “warning” that important signals are drowned out by noise.

A third consequence is the proliferation of redundant current intelligence reports containing little insight or added value. This exacerbates both the reality and the appearance of unnecessary duplication of effort across the IC.

Implications for Reform

This exercise in dotology should raise several cautionary flags to all who wrestle with the challenges of reducing expenditures and making the IC instruments of government more effective. The point, broadly construed, is that before politicians and policymakers start to tamper with the IC, they ought to have at least a rudimentary understanding of what it does and how it does it. Unfortunately, most don’t. The three key points to remember are:

- First, the intelligence budget should be cut, but policymakers—not IC professionals—must choose where they are willing to accept greater risks and operate with less information.
- Second, allowing the IC, under the direction of the Director of National Intelligence, to determine how best to adjust to new priorities and reduced budgets is generally preferable to externally mandated prescriptions for reform that inevitably will not fully appreciate the collateral consequences of the changes.
- Third, there are no magic-bullet solutions to the problems of the national security enterprise or the IC. Any narrowly focused or single-issue reform is certain to disappoint and very likely to make matters worse.

This is not a counsel to abandon hope, all ye who enter. It is merely to remind would-be reformers of an old truth: It’s one thing to destroy the outhouse, another to install plumbing. 🚽