Leadership Failures in the National Security Complex

Hal Berghel, *University of Nevada, Las Vegas*

Current NSA forecast: continued Snowden flurries with no end in sight. No one blames the hardworking NSA employees for the latest series of gaffes; it's the feckless leadership and the politics that got them there that are responsible for our current difficulties.

In his farewell address to the nation, President Eisenhower told Americans that the military–industrial complex offered enormous potential for abuse if not properly constrained. The problem has become much larger than he imagined. We now have a self-sustaining and self-regulating national military-industrial-surveillance-political-media-prison-energy-academic-religious-medical-legal-think-tank complex that is—taken together—too big to control. I'll return to this point at the end of this column.

When a country as technologically advanced as the United States becomes the object of global ridicule for its bungled attempt to cover up flagrant abuses of civil liberties—especially in cyberspace—something is very wrong. There's a reason why Vladimir Putin and Xi Jinping have remained silent about the spate of Snowden flurries—they're laughing too hard at our ineptitude.

I'm going to advance the thesis that the heart of the problem is a self-defeating leadership selection process. The intelligence community itself isn't the problem: it's the way we select the leadership that's the problem.

VAPIDITY CURVE

So who are these leaders? Where did they come from? Why are so many of them suboptimal decision makers? Why isn't the law of averages at work here? The answer to all these questions is that the leadership comes from a single source: the military. The selection pool isn't defined by any normal distribution of IQ or virtue. With a lack of clear-cut objectives, insensitivity to the ambient legal issues, a preoccupation with communication skills and subservience to authority, the selection process for the intelligence agencies produces a vapidity curve that favors the 5 percent of the candidates who hold 95 percent of the worst ideas. We're not talking about a cross-section of the military by any means, but rather the self-energizing, self-absorbed, and self-promoting part of the leadership that reveres the prestige and power of flag rank over accomplishments of enduring value. In the end, it isn't a matter of what rank they ultimately hold, but what they had to do to achieve it.

AN ALLEGORY OF THE HILL

See if you can detect a part of the following allegory that doesn't ring true.

General Eyes: "Colonel Smarts, command wants you and your men to take that hill, neutralize the enemy along the way, and plant a

Published by the IEEE Computer Society

big enough flag on the top so everyone on the island, especially the top brass, can see if from the fleet. The command is big on PR, Smarts, so we need to take advantage of this photo op. Make it happen."

Colonel Smarts: "General, I'm not seeing this. The enemy has been out of supplies for two months. He's low on everything: food, water, ammunition, you name it. Another couple of days, a week at the most, and he'll be begging to surrender just to get something to eat—without a shot fired! And by the way, General, no one fights uphill anymore; that's so Iwo Jima. Tell the General Staff that this operation just doesn't pass my smell test. We can have the photographers take a picture of my guys holding the flag over by the latrines, and Photoshop in the rest for the benefit of the media. The public will never know the difference, and no one will get hurt. "

General Eyes: "Good point, Smarts. I can see the error of their ways. Clearly, you have far more vision than the General Staff does. Why, I'll let my 3-star know you've rejected his plan. Let's give a name to your plan: "Operation Wait-and-See." I wouldn't be surprised if there's a commendation in this for you, Smarts. Tell your men to stand down while I straighten out the guys with scrambled eggs on their hats."

That's one story that you didn't see narrated on *The World at War*. The absurdity lies in the preposterous assumption that military planning is dynamic and BISF (Best Ideas Selected First). The ability to achieve a command rank in the military, and the ability to think through complex problems, are fundamentally different. The former is best suited to a team player who follows orders ("go along to get along" types) and can make quick decisions, while the latter prefers an individualist who questions everything, usually isn't all that compliant, and is exceedingly circumspect. Ask yourself how far stubborn determination, hasty decisions, and a myopic world view have got us in our foreign entanglements over the past 50 years. Bureaucracies tend to organize themselves around formal structures (like chains of command), not in terms of the capacity to make intelligent decisions.

The intelligence agencies' leadership selection process produces a vapidity curve favoring the 5 percent of the candidates who hold 95 percent of the worst ideas.

Why would that be? To understand, we'll start by asking what it takes to be a good military leader.

LEADERSHIP 101C

Effective cybersecurity leadership is hard to find because of finely interwoven technical, legal, and ethical dimensions involved. Government recruiting at top levels looks for individuals who don't wander from the political page, have only armoire skeletons that can be overlooked by a political base, and are familiar with operational strategies shaped by such things as burn rates, procurements, logistics, and asset management. These are just not the sort of skills required for world-class cyberleadership. Oversight of trucks, ships, aircraft, and captive recruits is different from oversight of code development, algorithms, and free thinkers.

So far, history seems to suggest that those prepared by education and training to oversee the physical and kinetic aren't well suited to oversee the virtual and digital. The latter is difficult to observe, harder to identify, and more difficult to quantify, and the outcomes at the macro level are less determinate. Cyberwarriors will find Sun Tzu's 13 principles and von Clausewitz's dialectical method a bit wanting at tactical levels. There are no straightforward reductive principles that allow you to move back and forth between the kinetic and cyber. Principles of mass, economy of force, battle geometry, and issues of warfare symmetry don't port over naturally to the digital realm.

George C. Marshall, the senior US military leader in World War II, listed the qualities of a successful military leader in a democracy: common sense, good student, physically strong, cheerful and optimistic, energetic, extremely loyal, determined, and possessing "flexibility of mind." What's more interesting is his list of undesirables: outliers, individualists, eccentrics, and dreamers—the qualities commonly found in creators, innovators, and designers.

An insightful look at military leadership can be found in Thomas Ricks' recent book, which describes studies of desirable leadership skills that followed the military debacles in Korea and Vietnam—studies that the military resists to this day.[1] Ricks points out that the military still emphasizes training over education, tactical over strategic thinking, and obedience over ethical philosophizing: "The Army's rejuvenation [has been] tactical, physical, and ethical but not particularly strategic or intellectual. … In its 21st-century wars the Army would come to realize it needed leaders comfortable with vague situations, alien cultures, inadequate information, and ill-defined goals" (*The Generals*, pp. 348–349). The Army tried to change the culture in the mid-1980s by creating a School of Advanced Military Studies (SAMS), but without much effect.

With few exceptions (Ricks specifically points to General David Petraeus), the upper echelons of the Army just can't seem to internalize the SAMS program. The legacy of our military (and civilian) leadership remains wars without exit strategies; under-appreciation of collateral damage; misunderstanding of underlying political realities; ignorance of world cultures and history; over-reliance on firepower, equipment, and technology; and the inability to think outside what Ricks calls the "standard operational repertoire." Incredible as it seems, our military and political leadership have managed the impossible: they've created a culture of preemptive wars and global nation building where more factions come out of the conflicts than went into them.

This isn't to say that very bright, open-minded individualists don't find their way into the officer cadre of the military—they are legion. But they won't be promoted to the most senior command ranks because of the military power structure's built-in bias toward tactics that were successful in prior wars and conform to the status quo. Ricks argues that the modern military remains in a "post-Vietnam" evolutionary period. Are these leadership characteristics well suited to cyberspace?

If the past 70 years of national security policy have shown us anything, it's that there's no room in intelligence and security leadership for demagogues and dilettantes.

WHAT MAKES A GOOD INTELLIGENCE AND SECURITY LEADER?

Management abilities are important, but technical expertise is a sine qua non. It's essential that a leader have the capacity, if not the actual experience, to master the technical requirements of subordinates. Understanding and open-mindedness are also required. The ability to second guess yourself is critical because it's essential to assume that in cyberspace the enemy is smarter than you are. A corollary to that principle is the willingness to delegate to others strategic decision making just as our General Eyes did above. Great security and intelligence leaders aren't authoritarian executives. They're more like orchestra directors who have the chops to duplicate their subordinates' unique capabilities and strengths if and when needed while simultaneously focusing on the bigger picture. These skills, it seems to me, are best developed bottom-up, not top-down. Chains of command are anathema to such leaders.

Such leaders recognize that contrarianism is a prerequisite for creativity. The siblings of contrarianism are abstract thinking, imagination, and innovation, and the cousins are self-doubt, second guessing, deference, and dependence on others for critical decisions. Irreverence and insolence share considerable DNA. Deference, homage, fealty, loyalty, and the like are not prerequisites. For simple, straightforward tasks, a military-control mindset might be fine. But for more complicated situations this isn't the gene pool you want to draw from. Gung ho mindsets won't work—today's conflict environment is too fragile and complex.

There are also cybersubtleties/nuances that typical military leaders would likely overlook—for example, why large groups of people would work diligently to develop world-class software (think Linux) so that they can give it away. But unless a leader has internalized that phenomenon, it'll be impossible to understand how the Internet works and the motivations of the major players (think: Anonymous). We can't rely on contractors to provide such understanding. In intelligence, privacy, and security matters, people's interests are best served by people who can think outside the Beltway.

ABSENCE-OF-THOUGHT LEADERS

Let's return to variations on our original questions. Why is the US incapable of integrating IT protection, military communications, criminal investigation, and this war on terrorism of ours into a constitutionally friendly framework? Why do we have Army privates rummaging through State Department secret archives and low-level employees of government contractors walking out with the NSA's favorite PowerPoint slides? Why was the public in the dark about the government's dragnet digital surveillance? Why does the government overclassify information, and overprosecute leakers and whistle-blowers who disclose it? What would the NSA be doing with a State Department Rolodex with contact information of world leaders?[2] Why is a former NSA director overheard slamming the Obama administration on a train?[3] Just look who's running these government agencies: political retreads and military double-dippers who have built their latter career around mastery of the iron triangle. It's a paradigmatic worst of all worlds—the combination of skill inversion and double-dipping combined with a healthy dose of cognitive dissonance running amok within a military–ndustrial complex fueled by deficit spending.

Examples abound of the consequences of a failed leadership selection strategy. For example, we have past NSA Director Michael Hayden explaining how the NSA uses a Fourth Amendment that's different from the one in the Constitution—one without the requirement of probable cause (https://www.youtube.com/watch?v=cGhcECnWRGM). And Hayden's explanation that Senator Feinstein lets her emotions interfere with her appreciation of torture.[4] And let's not forget Director of National Intelligence James Clapper's explanation that he didn't actually lie to Congress, he just offered the "least untruthful answer" he could think of (www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-082.pdf). For another perspective on the "fog of misunderstanding," see former NSA Director Keith Alexander's surveillance-bathtub metaphor (http://voiceofrussia.com/news/2013_10_27/NSA-Chief-Keith-Alexander-in-interview-to-Youtube-comparing-surveillance-to-taking-a-bath-0012) and his proposal that the NSA can improve security by firing 90 percent of its system administrators (https://www.schneier.com/blog/archives/2013/08/nsa_increasing.html). Let's not overlook tapping the phone lines of friendly governments. It doesn't get much better than this. To the rest of the world, this reality TV is better than *Pawn Stars*.

Although largely ignored by the mainstream media, former President Truman realized by the early 1960s that the National Security Act he signed in 1947 was bearing toxic fruit (www.maebrussell.com/Prouty/Harry%20Truman%27s%20CIA%20article.html).[5] By then he was aware of Project Shamrock, Operation Northwoods, Operation Bumpy Road (Bay of Pigs), Operation PBSUCCESS (CIA-sponsored coup d'état in Guatemala), Operation Mongoose (plots to kill Fidel Castro), and so on, and saw that the military–industrial complex apostolates were out of control. He recognized then, as we do now, that a moral compass doesn't read true when caught in the magnetic field of hegemony and unilateralism.

If the past 70 years of national security policy have shown us anything, it's that there's no room in intelligence and security leadership for demagogues and dilettantes. Military officers in particular are trained to fight wars, not interpret the Constitution, establish sound policy, and wax eloquent on the future of cyberspace. Failure to take note of this fact is costing us dearly in both the protection of civil liberties and global prestige. Due to exceedingly poor leadership, our intelligence agencies have wasted hundreds of billions of dollars on a brutish surveillance panopticon, whereas more talented and refined intellects could have invented and deployed constitutionally compatible alternatives at a fraction of the cost.

In fact, this is exactly what happened when NSA Director Hayden replaced the million-dollar ThinThread project that worked and was faithful to the Constitution with the billion-dollar Trailblazer Project that didn't work and lacked privacy protections for US citizens. Trailblazer was the legacy of the same general who denied that probable cause had any relevance to the Fourth Amendment, and that Senator Feinstein shouldn't have stuck her toe in the sand over enhanced interrogation techniques that fall short of organ failure and death.

I agree completely with the recent Presidential Review Committee's recommendation that at this point the director of the NSA should be a civilian who is approved by the Senate and that DIRNSA shouldn't head US Cyber Command.[6] While not silver bullets, these changes would be an important first step toward sensible leadership and intelligent oversight. All three were rejected by President Obama. ■

References

1. T.E. Ricks, *The Generals: American Military Command from World War II to Today*, Penguin, 2012.
2. J. Ball, "NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts," *The Guardian*, 23 Oct. 2013; www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.
3. T. McCarthy, "Former Spy Chief Overheard Giving Off-the-Record Interview from Acela Train," *The Guardian*, 24 Oct. 2013; www.theguardian.com/world/2013/oct/24/former-spy-chief-overheard-acela-twitter.
4. E. Delmore, "Hayden: Feinstein too 'Emotional' over Torture Report," MSNBC.com, 6 Apr. 2014; www.msnbc.com/all/hayden-feinstein-too-emotional-over-report.
5. R. MacGovern, "Truman's True Warning on the CIA," Consortiumnews.com, 22 Dec. 2013; http://consortiumnews.com/2013/12/22/trumans-true-warning-on-the-cia.
6. *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, report, 12 Dec. 2013; www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Hal Berghel, *Out of Band column editor, is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.*

Incorporating domain-specific concepts and high-quality development experience into MDE technologies can significantly improve developer productivity and system quality. This tactic has led to work, starting in the late 1990s, on MDE language workbenches that enable the development of tool-supported DSMLs. A DSML bridges the problem space in which domain experts work and the implementation (or programming) space. Domains in which DSMLs have been developed and used include automotive, avionics, and cyber-physical systems.

John Hutchinson and his colleagues provided some indication that DSMLs can pave the way for wider industrial adoption of MDE.[3] Research on systematic DSML development has produced a technology base robust enough to support the integration of DSML development processes into large-scale industrial system development environments. Current DSML workbenches support the development of DSMLs to create models that play pivotal roles in different development phases. Workbenches such as Microsoft's DSL tools, MetaCase's MetaEdit+, JetBrains' MPS, the Eclipse Modeling Framework (EMF), and the Generic Modeling Environment (GME) support the specification of the abstract syntax, concrete syntax, and static and dynamic semantics of a DSML. These workbenches address DSML developers' needs in a variety of application domains.

Today's complex, software-intensive systems development often involves the use of multiple DSMLs to capture different system aspects. In addition, models of system aspects are seldom manipulated independently of one another. Systems engineers are thus faced with the difficult task of relating information presented in different models. For example, a systems engineer might need to analyze a system property that requires information scattered in models expressed using different DSMLs. Current DSML development workbenches provide good support for developing independent DSMLs, but little or no support for integrated use of multiple DSMLs. The lack of support for explicitly relating concepts expressed in different DSMLs makes it very difficult for developers to reason about information spread across different models.

Supporting coordinated use of DSMLs leads to what we call the globalization of modeling languages.

GLOBALIZED DSML CHALLENGE: LOOKING AHEAD

Past research on modeling languages focused on their use to bridge wide problem-implementation gaps. A new generation of software-intensive systems—such as smart health, smart grid, building energy management, and intelligent transportation systems—presents new opportunities for leveraging modeling languages. The development of these complex systems requires expertise in a variety of domains. Consequently, different stakeholder types (such as scientists, engineers, and end users) must coordinate on various aspects of the system across multiple development phases. DSMLs can support the work of domain experts focusing on a specific system aspect, but they can also provide the means for coordinating work across teams specializing in different aspects and development phases.

Supporting coordinated use of DSMLs leads to what we call the globalization of modeling languages, that is, the use of multiple modeling languages to support coordinated development of diverse system aspects. This is analogous to globalization: relationships are established between sovereign countries to regulate interactions (such as travel- and commerce-related interactions) while preserving each country's independent existence. The term "DSML globalization" describes the desired goal that independently developed DSMLs will meet specific domain experts' needs and should have an associated framework that regulates the interactions needed to support collaboration and work coordination across different system domains.

Globalized DSMLs aim to support the following critical aspects of developing complex systems: communication across teams working on different aspects, coordination of work across the teams, and control of the teams to ensure product quality. The objective is to offer support for communicating relevant information, coordinating development activities and associated technologies within and across teams, and imposing control over development artifacts produced by multiple teams.

Coordination and related separation of concerns issues have been software engineering's focus since early work on modularized software. David Parnas' use of the term "work product" to denote a module that can be the source of independent development is also a focus of team demarcation across design and implementation tasks. Modularity in modern software-intensive systems development leads to well-known coordination problems, such as problems associated with coordinating work over temporal, geographic, or sociocultural distance.[4] This has also led to the recognition that sociotechnical coordination, including coordination of the stakeholders and the technologies they use to perform their development work, is a major systems development challenge.[5]

DSMLs support sociotechnical coordination by providing the means for stakeholders to bridge the gap between how they perceive a problem and its solution on the one side, and the programming technologies used to implement that solution on the other. When they're supported by mechanisms for specifying and managing their interactions, DSMLs also support coordination of work across multiple teams. In particular, proper support for coordinated use of DSMLs leads to language-based support for social translucence, where the relationships between DSMLs are used to extract the information needed to make a development team aware of relevant work performed by teams working on other aspects. Such awareness minimizes the counterproductivity that results from social isolation when work is distributed across different teams.

ON MODELING LANGUAGE GLOBALIZATION

To support globalization, relationships among multiple heterogeneous modeling languages must be established to determine how different system aspects influence one another. We identify three possible relationships that modeling languages might use to support interactions across different system aspects: interoperability, collaboration, and composition.

Interoperable modeling languages provide support for information exchange across their models. Interoperable DSMLs can be developed in a relatively independent manner, but relationships defined across the different DSMLs allow information expressed in one model to be related to information contained in models expressed in different DSMLs. These DSML relationships facilitate the development of integrated modeling tool chains in which information from a model built for a specific purpose (such as a SysML model, which specifies the system architecture) is used to annotate a model that serves a different purpose (such as a generalized stochastic Petri net used for performance analysis). Interoperable DSMLs have the lowest coupling of the three relationships we identified; the focus is on supporting coordinated use of modeling tools, as opposed to tightly coupling model development.

Collaboration relationships among modeling languages provide support for coupled model development. DSMLs in such a relationship are referred to as collaborative modeling languages. The model development expressed in a collaborative modeling language can directly influence the form and the correction of models created using other collaborative modeling languages. For example, developers can use consistency relationships defined across DSMLs to ensure consistency among the different models they create. Model-authoring tools for collaborative DSMLs are thus coupled. Collaborative DSMLs can support a priori as well as a posteriori global analysis of properties.

Interoperable and collaborative DSMLs support DSML interactions without deriving new forms of information from that which is spread across different models. However, some situations call for creating new forms by combining information scattered in other models—for example, to support system documentation generation and test cases, or to provide support for simulating global system behavior. Model composition (such as weaving and merging) is thus the third form of interaction facilitated by explicit definitions of relationships across elements in different DSMLs.

These ideas can be applied at various phases of the development life-cycle, ranging from early analysis to system runtime. Models can also be used to coordinate work done by different components, subsystems, or services. The use of DSMLs to coordinate work can potentially have a beneficial impact on the running systems' management. Different model kinds are currently used as runtime abstraction layers to support reasoning about the system or even adapting it.[6] These model-based runtime environments can leverage explicitly defined relationships across DSMLs to coordinate the manipulation of models at runtime.

Challenging issues will need to be addressed to realize the above forms of language integration. Relationships among the languages will need to be defined explicitly in a form that corresponding tools can use to realize the desired interactions. Requirements for tool manipulation are thus another topic that will be a focus for future work in the area of DSML globalization. ■

Acknowledgments

This work is supported by the GEMOC initiative (http://gemoc.org), an open, international initiative that brings together a community to develop software language engineering breakthroughs supporting DSML globalization.

References

1. D.C. Schmidt, "Guest Editor's Introduction: Model-Driven Engineering," *Computer*, vol. 39, no. 2, 2006, pp. 25–31.
2. R. France and B. Rumpe, "Model-Driven Development of Complex Software: A Research Roadmap,"

Future of Software Eng., IEEE CS, 2007, pp. 37–54.
3. J. Whittle, J. Hutchinson, and M. Rouncefield, "The State of Practice in Model-Driven Engineering," *IEEE Software*, vol. 31, no. 3, 2014, pp. 79–85.
4. J.D. Herbsleb and R.E. Grinter, "Architectures, Coordination, and Distance: Conway's Law and Beyond," *IEEE Software*, vol. 16, no. 5, 1999, pp. 63–70.
5. J.D. Herbsleb, "Global Software Engineering: The Future of Socio-Technical Coordination," *Future of Software Eng.*, IEEE CS, 2007, pp. 188–198.
6. G. Blair, N. Bencomo, and R.B. France, "Models@ run.time," *Computer*, vol. 42, no. 10, 2009, pp. 22–27.

Benoit Combemale *is an associate professor at the University of Rennes, France, and a research scientist at Inria. His research interests include model-driven software engineering, software language engineering, domain-specific languages, and validation and verification. Contact him at benoit.combemale@inria.fr.*

Julien DeAntoni *is an associate professor in the Department of Computer Science at the University of Nice Sophia-Antipolis, France. His research focuses on the connection between model-driven engineering and concurrency theory by using the notion of logical time. Contact him at julien.deantoni@inria.fr.*

Benoit Baudry *is a research scientist at Inria. His research interests include metamodeling and model-based software analysis and testing. Contact him at benoit.baudry@inria.fr.*

Robert B. France *is a professor in the Department of Computer Science at Colorado State University. His research focuses on model-driven development, models at runtime, software product lines, domain-specific languages, and formal methods. Contact him at france@cs.colostate.edu.*

Jean-Marc Jézéquel *is a professor at the University of Rennes and director of IRISA. His research focuses on the theory and practice of model-driven engineering. Contact him at jezequel@irisa.fr.*

Jeff Gray *is a professor in the Department of Computer Science at the University of Alabama. His research focuses on model transformation, domain-specific languages, and computer science education. Contact him at gray@cs.ua.edu.*