Security Capabilities Network
a project of the
National Strategy Information Center

Is the Classified Information Paradigm Beyond Repair? What Would It Take to Fix It?

James B. Bruce

The problem. The U.S. government is demonstrably unable to protect the classified information on which much of national security is based. In the Manning and Snowden era when possibly two million classified documents are made public and the press is awarded prizes for publishing much of the stolen material, it is fair to ask whether the government is capable of protecting the information required for effective intelligence, military, and diplomatic results. As internet-age leakers are outpacing spies as insider threats, it would appear that the paradigm to protect classified information is fundamentally broken, and it is time to consider what it might take to fix it. Or if the paradigm is truly beyond repair, what should replace it?

The paradigm. As a framework that shapes our mindset and practices for acting,[1] the combination of the structure, culture, rules, and technologies that afford protection to the nation's secrets can be said to constitute the classified information protection paradigm. The argument made here is that this secrecy paradigm now requires the kind of scrutiny that will lead to a determination about whether it is so broken that it must be replaced. As Thomas Kuhn has noted, "Probably the single most prevalent claim advanced by the proponents of a new paradigm is that they can solve the problems that have led the old one to a crisis. When it can legitimately be made, this claim is often the most effective one possible."[2] At this point, considerable work needs to be done before we can meet Kuhn's paradigm replacement threshold.

While the threats to secrecy are better understood inside government than outside it, their broad dimensions are well known. The main threats consist of foreign espionage and leaked, i.e., unauthorized, disclosures of classified information, along with authorized foreign intelligence sharing, the demarche process, and the massive declassification program.[3] Although espionage has held the top spot for damage in the past, the scale of the recent Internet disclosures probably match if not surpass the total classified hemorrhage of every U.S. spy and leaker since World War II. The key elements of the classified information protection paradigm include at least these:

- How a secrecy determination (yes or no) is made for specific information, and what level of protection is needed (lowest-to-highest classification) to keep it secure.
- The safeguards to afford protection at the desired level, such as physical, electronic, communications, and operational security, and counterintelligence; and
- Capabilities for secure dissemination, storage, and retrieval of classified information.

[1] Roy Godson and Richard H. Shultz, *Adapting America's Security Paradigm* (Washington, DC: National Strategy Information Center, 2011), p. 222; definition elaborated there.

[2] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: Univ. of Chicago Press, 3rd ed., 1996), p. 153.

[3] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C.: U.S. Government Printing Office, 2005), pp. 380–384.

The questions. These elements present a mix of strengths and vulnerabilities. The vulnerabilities are principally of two types: Human and digital. The defining question here is whether these two major vulnerabilities have so overpowered the strengths of these key elements that the secrecy classification paradigm is beyond repair. Is it? And how would we know? This is the first of three big questions this topic challenges us to answer. The second question is if the paradigm is not terminally broken, what would it take to restore it to good working order? And third, if it is indeed beyond repair, what kind of secrecy paradigm should supersede it?

Diagnosis. Determining whether the infirmities of the security classification patient are terminal is no easy task. A useful metric is assessing how much U.S. government national security performance is impaired by its inability to protect secrets. Answers are neither easy nor readily available and competent observers will differ. Here are five hypotheses:

1. In *intelligence*, effective performance is appreciably impaired in collection against the hardest targets. Analysis is thus poorer for the denial of valuable information. And both policy and military customers suffer impaired decision advantage for the lack of needed intelligence resulting from significant disclosures of sensitive sources and methods.
2. The *military* effects are less well understood, but unauthorized disclosures in publications like *No Easy Day* illustrate how some special operations options can be taken off the table. Protecting conventional as well as offensive cyber operations suggests a separate discussion.
3. Impairments in *diplomacy* are a key theme in the Manning-WikiLeaks disclosures as diplomatic confidences are publicized, as earlier compromises to the Russians, Cubans, and Chinese have enfeebled U.S. diplomatic effectiveness in some key areas.
4. A 2014 snapshot cannot capture the rate of descent, but the trend lines in classified compromises are getting worse, not better. We cannot yet predict exactly how much worse.
5. We are not even close to having a solid or comprehensive understanding of the scope and scale of the problem. If the true dimensions of the impairments were well understood, the problem would almost certainly look worse than it now appears.

Treatment options. If the maladies now crippling extant security protections are treatable, then the present classification paradigm may be salvageable. But to succeed, treatment must be urgent and based on accurate diagnosis, and that assumes that the problems are well enough understood and curable as well. And even then, success is not assured. We need a solid understanding of the human and digital vulnerabilities assessed against the present paradigm's capacity to recover before we can reliably assess treatment options and apply them.

But failure, too, is also possible, and perhaps even likely. The consequences of failure would mean a government hobbled, maybe even crippled, in key instruments of power—intelligence, military, and diplomacy—that shape its ability to provide security to the nation.

Agenda: Beyond handwringing. Well before we reach this crisis point, we would be well advised to give this vexing issue the priority attention it deserves. A catastrophic paradigm failure in secrecy protection will likely be more gradual than abrupt. But by the time we identify it as such, it will be too late for needed fixes. The immediate issue is whether we can up our game in time to take meaningful correctives, while still hoping to keep disclosure risks to national security at non-catastrophic levels. But if we learn that the present secrecy paradigm cannot be salvaged, we won't regret early investment in what a new one should look like.