The Psychology of Espionage and Leaking in the Digital Age

Dr. Ursula M. Wilder

Introduction

In 2003, *Studies in Intelligence* published my classified article "Why Spy?: The Psychology of Espionage." A newly unclassified version of that article follows this one. "Why Spy" focused on the personalities, motives, behaviors, and experiences of people who commit espionage. The article also explored how unwitting colleagues might experience a spy's personality and behavior during day-to-day interactions in the workplace. Leaking was not addressed in 2003 because it was not at the time a leading threat. That has changed, and this essay addresses some of the reasons for the change.[a, 1] (See Textbox 1 on the next page for my working definitions of espionage, leaking, and spilling.)

Advances in technology—broadly speaking, the Internet, mobile platforms, social media, and computing power—are driving unparalleled, epoch-defining changes in the world. Communication technologies, in particular, have altered how people relate to each other individually, in social groups, in nations, and globally, and are expanding what people mean when they use the term "reality."[2]

The new technologies have, unsurprisingly, precipitated changes in the manifestations of spying from within the world of professional intelligence, where leaking now joins espionage as a major threat to national security. Other threats from insiders include sabotage and workplace violence.[3]

The model of espionage presented in the 2003 article describes three core elements that motivate a person toward espionage: personality pathology or vulnerabilities, a precipitating life crisis, and opportunity (finding a safe customer for the spy's espionage services). The critical role of personality vulnerabilities has not changed in today's spies, but, as we shall see, the Internet and associated technologies can amplify them. Similarly, the emergence of a life crisis remains an integral part of the decision to spy; in the digital age, technologies can exacerbate existing crises and also generate new ones.[b]

The greatest impact of the new technologies is in the third necessary element—ease of opportunity. During the past 15 years, a prospective spy's access to customers for espionage via the Internet has grown exponentially, and media platforms seeking leakers have proliferated. Today, many mainstream media outlets provide "leak bait" options on their websites that allow people to anonymously deliver information. Professional intelligence services hunting for prospective candidates for espionage now have Internet-enabled spotting, developing, and recruiting tools that work just as effectively for professional handlers seeking candidates to manipulate into espionage as they do for retailers seeking to target customers susceptible to advertising.[4]

For the remainder of this article, my primary focus will be on the role of the Internet (to include social media) in espionage and leaking. However, other aspects of technology, such as the physical engineering and operational design of devices and software, also play a potentially powerful role in priming vulnerable persons toward spying. Our devices of entry into the Internet "behave" as

a. Readers interested in gaining insights into the perceptions of serving officers on the WikiLeaks website, its sponsors and supporters, and related matters are encouraged to read the transcript of the Director of the CIA's presentation at the Center for Strategic and International Studies in Washington, DC, on 13 April 2017 entitled, "A Discussion on National Security with CIA Director Mike Pompeo"; available at https://www.csis.org/analysis/discussion-national-security-cia-director-mike-pompeo. In his opening remarks, DCIA Pompeo said intelligence officers are "not at liberty to stand up to . . . false narratives and explain our mission to the American people. But fortunately, I am."

b. This is not to say technology can only have negative effects on the vulnerable. At-risk people may find online interlocutors who alleviate loneliness and alienation in positive ways and who offer balanced views eluding people in crisis and point them toward options other than illegal or dangerous behavior.

if they have lives of their own; they can have strong "holding power" over the psyche of users (they are designed to have this power). People whose work, play, and relation-ships are mostly mediated through keyboards and devices and who experience their engagements in the cyber realm as more rewarding than anything else in their lives are, as we shall see, particularly vulnerable to the role the Internet and associated technologies can play in paving the way to spying.[5]

Despite the breathtaking size and pace of the social and psychological change we are witnessing in the digital realm, much remains the same in human nature. What we witness occurring in global culture because of technology is monumental and disruptive, but it is also coherent to us because we recognize our universal human needs, desires, and common pursuits playing out in the midst of the complexity and change. We can still rely on these universals as a solid basis for explanations for why people do what they do. Human fundamentals include complex positive qualities such as loyalty, dedication, good faith, authentic friendship and social bonds, need for real intimacy and trust, desire to belong in a community, curiosity, creativity, and common sense anchored in factual reality. They also include negative qualities such as treachery, greed, cruelty, malice, duplicity, readiness to dupe and manipulate others for personal gain or entertainment, and susceptibility to powerful psychological control techniques applied by experts. We should examine what is new but keep these fundamentals in mind as anchors to understanding contemporary humans and their behavior and choices.

Textbox 1: Definitions

The vocabulary surrounding matters of unauthorized disclosures is in flux. For readability and conciseness, in this article the behavior of individuals engaged in either espionage or leaking is referred to as "spying." I use this word on the premise that in both cases insider access to classified information is deliberately abused to make unauthorized disclosures, in secret or publicly.

Espionage. Spies engaged in espionage secretly deliver classified information to a party the spy understands is working directly against his or her own country. This typically involves an intermediary—a handler—who usually is a foreign intelligence service officer trained in managing agents safely and productively. The aim of a handler is to keep the spy undetected and the transfer of information ongoing and secret. For reasons of security and veracity, professional intelligence officers rarely handle anonymous sources for long periods.

Leaking. Spies who leak make classified information publicly available without authorization, usually through contacts with media outlets or via the Internet. Leakers may have regular, dedicated interlocutors such as journalists, who receive and disseminate the information. Unlike spies engaged in espionage, most leakers are (at present) not paid or otherwise rewarded materially for their actions. Nor do their interlocutors normally engage in the kind of long-term handling tradecraft used by professional intelligence services—although source protection and information authentication are core missions of journalists as well.

Spilling. The key concept in defining spilling is lack of intent. Spies engaged in espionage or leaking have specific goals in mind, whereas spilling is the inadvertent, unintended disclosure of information to uncleared environments, organizations, or people.[6]

The 2003 article made a distinction between self-serving and heroic spies; this article addresses the former. How professional intelligence officers address the subject is discussed in Note 7. The note also addresses a parallel distinction between leakers and whistleblowers. (See also Textbox 2 on facing page for discussion of ethical dimensions of the issue.)

❖ ❖ ❖

What Causes Someone to Spy or Leak?

The three essential factors predisposing individuals to espionage or leaking classified material—dysfunctions in the personality, states of crisis, and opportunity—operate symbiotically. Pathological personality features not balanced by healthy traits can result in conduct that precipitates life crises. These in turn, stress the already tenuous coping capacities of vulnerable personalities. Crises and vulnerability together intensify emotions, undermine already compromised judgment, and galvanize impulses to seize opportunities to obtain escape or relief through ill-judged negative conduct. People in this state are ready targets for manipulation and recruitment for espionage. They are also primed for behavior such as leaking, if they believe it will bring them respite and reward.

Personality

Psychologists consistently detect four personality characteristics when they study spies: psychopathy, narcissism, immaturity, and grandiosity (see page 21 of "Why Spy?" for detailed discussion of each). Some of these features are present in the personalities of a great many, if not most, people who will never engage in wrongdoing—the reader is likely

Textbox 2: Observations on the Ethics of Political Disclosure of Sensitive Information

Unauthorized disclosure of sensitive or proprietary information to the media for political purposes is an age-old feature of political life and will remain a permanent fixture of any democratic society with a free press. Those seeking political advantages through such disclosures generally partner with established media outlets, both to ensure an extensive audience and to gain legitimacy; they presume that audiences will assume the media partner has screened and verified the information before using it. Less well known is that professional members of the media usually seek comment from relevant members of the Intelligence Community before making public classified information they have acquired. Sometimes they will revise their drafts to mitigate credible risks described to them by the Intelligence Community or may even withhold a story when they are convinced that risks to national security, US citizens, or US allies or innocent persons are too high.

A 2013 case study on leaking published in the *Harvard Law Review* hypothesizes that periodic, tumult-inducing, unauthorized disclosures are not caused so much by institutional weak points or failures (such as feeble security measures, law enforcement investigations, and prosecutions of leakers) but by the considered choices of high-level officials who benefit from lax enforcement of legal prohibitions against unauthorized disclosures. The author further argues that, in subtle ways, lax enforcement benefits national security, government efficiency, and democratic transparency more than it harms them.[8]

The *Harvard Law Review* published a riposte to the essay asserting that the harm caused by "high level" leaking is very real, but, despite the self-evident harm, "the executive branch has been unable and unwilling to close the 'sluice gates' due to easily underestimated legal and technological constraints and also because of political constraints emerging from strong passions in American society that exert pressure on democratically elected leaders."[9]

In an article in *Foreign Policy,* William J. Burns (former deputy secretary of state) and Jared Cohen (president of Jigaw (previously Google Ideas) argue that "We should build a global consensus around both the need to protect the integrity of financial data and systems on which the global economy relies and the illegality of cyber-enabled commercial espionage, *making a clear distinction between traditional espionage and wholesale commercial theft*."[10] (Emphasis added.)

Apparently, in the international consensus these authors propose to build for the cyber age, an exception will remain between nations (in the tradition of a true gentlemen's agreement) that permits political and military espionage against each other to continue unabated, whereas technology-enabled commercial espionage and digital infrastructure destruction will be forbidden. Intelligence service officers will be pleased that their jobs remain secure, and at least somewhat respectable, according to the proposed rules for the brave new cyber world.

It is hard to predict where all of this is going to take us, nationally and globally; at present, we can only note that a sea change is occurring in the way all levels of society view technology and the access to information it enables. These are major areas of ongoing discussion and conflicts on both the formal governance level and on the "street" level. In regard to the psychology of espionage and leaking, persons considering spying will find ample justification and support to act on their impulses and desires in the evolving and contentious social dynamic in the public commons concerning the uses and control of technology and information.[11]

thinking of such people now. In the case of spies, however, personality vulnerabilities are relatively unmediated by other characteristics that might provide a counterbalance, as happens with healthy personalities.

A balanced personality might have a strong preference for logical reasoning and the detachment to counter the impulsivity and fantasies of immaturity; a healthy person might have empathy for others or respect for hard-earned expertise that compensates for a tendency toward the egoism and sense of entitlement characteristic of narcissists. Yet another individual might have acquired a capacity to anticipate long-term consequences or a set of acceptable rules for navigating the world that override psychopathic thrill-seeking and a predatory approach to exploiting the present moment.

Features of the Internet and associated technologies have the potential to undermine the counterbalancing traits of even healthy personalities and pose the risk of escalating pathological features. Often this occurs in anonymous encounters with facilitating individuals or groups who mutually reinforce and validate extreme or pathological viewpoints and embolden inappropriate behavior.

Online survey studies of the personality features of Internet trolls conducted by a group of Canadian scholars concluded that trolls are "prototypical everyday sadists."[12] The researchers explored the links between trolling and what psychologists call the "dark tetrad" of personality traits—narcissism, Machiavellianism, psychopathy, and sadism—and found that the tetrad was highest among survey respondents who said that trolling was their favorite online activity.[13] Illustrative of the attitudes the researchers were studying was inclusion in their Likert scale surveys of items such as *"The more beautiful and pure a thing is, the more satisfying it is to corrupt,"* and *"Hurting people is exciting."*[14]

The online jargon for producing and enjoying the distress of others is "lulz."[a] The phenomenon of cruelty for sport on the Internet now has its own etymology (with recognized usages such as "trolling" and "lulz"). Trolling is highly performative behavior: beyond seizing the attention and provoking the responses of the targeted persons, trolls also pursue psychological reward by gaining the attention of admiring audiences who share their taste for "lulz." Keeping bad company, online and anonymous, egged on by like-minded others looking for entertainment, can stimulate a vulnerable personality toward many harmful and destructive actions, including leaking and espionage.

For example, a person with psychopathic personality features might engage in espionage or leaking simply for the thrill of breaking rules and creating chaos; like trolls, psychopaths "do it for the lulz." For them, the Web is a playground and its darker elements a confirmation of their view of reality: exciting, Darwinian, and pitiless—a world populated by either predator or prey. When people such as these spy in an Intelligence Community context, their secret enjoyment of the contrast between the day-to-day, "real life" humdrum in their offices, surrounded by unwitting, duped colleagues, and their charismatic, online "spy" persona, uninhibited and free and complete with applauding admirers, provides ample reward for engaging in espionage or leaking. There is also plenty of material and people online to feed the vengeful, spiteful characteristics that are common to both psychopathy and narcissism.

People with narcissistic personality features can find ample fuel online for their grandiose fantasies and can experience on the Internet the expansive, protean sense of power and superiority that characterizes them, complete with clusters of fans and/or supporters spurring them on in espionage or leaking "for the greater good" or validating their desire to get revenge on organizations or authorities they believe insufficiently appreciated them or otherwise wronged them.

Immature personalities, defined by difficulties separating the fictions and dreams of their imaginations from hard, factual reality, find plenty of scope on the Internet for fantasy-driven activity—including espionage and leaking—that simply bypasses any consideration of consequence in real life ("IRL" in Web parlance). The immature personality is more easily seduced into action by the seeming unreality of behavior in the cyber realm, actions that can seem to disappear with the click of a mouse or the swipe of a fingertip.

An enduring paradox of the Internet is that while it is distinctly real (it exists in material reality), it is also distinctly different—and, to some,

a. The online Oxford Living Dictionary defines "Lulz" (also "luls") as "fun, laughter, or amusement, especially derived at another's expense" and describes it as "an early 21st century corruption of LOL or LOLZ ("Laugh Out Loud").

quite separate—from concrete reality. This is dangerous ground for those who do not readily distinguish between fact and fiction, between what resides in their imaginations, their desires and hopes, and what resides in concrete, material reality or IRL. In contrast, well-grounded people can find cyberspace exciting, even enchanting, and useful to sustaining a complex, full life—while remaining solidly anchored in the material world and retaining good judgment about the consequences of actions taken in either realm.

Psychopathy, narcissism, and immaturity all have in common the characteristic of grandiosity. A well-known adage of the digital age is: "On the Internet, everyone knows you are a dog."[a, 15] It could also be said that: "On the Internet everyone thinks you are a hero, or a villain." Our technology now makes it possible for a person to develop and express multiple selves in cyberspace.[16] This is a context of human interaction and action that can feed and reward grandiose self-perceptions.[17]

Furthermore, the Internet, and the technology and devices that give access to it, are ostensibly under the control of the anonymous user. If the anonymous user feels unrewarded, displeased, or psychologically threatened online, he or she can back out and re-enter in a different persona, not something that is possible—at least not to the same degree—IRL. A user can also set aside, discard, or destroy poorly functioning or frustrating devices, again, something difficult to do with people. Furthermore, both the Internet and the associated devices of entry into it appear to have "lives" of their own (they continue to act autonomously and separately from logged-off users), but the user has an illusion of control because he or she can turn the devices on or off, thus suspending their digital lives until the user chooses to re-engage on his or her own terms. Such seeming sovereignty over something as global and powerful as the Internet, the people one encounters there, and the "thinking and behaving" machines that mediate relationships can feed grandiosity, at least if the tendency toward grandiosity is uncoupled from the leveling and grounding of "real life."

A Precipitating Crisis

The second necessary element that paves the way for spying is the emergence of a personal crisis of such intense weight and urgency that the vulnerable person experiences a sense of immediate threat, loses perspective and judgment, and becomes fixated on finding a way to put an end to the situation. The state of crisis may or may not be visible to friends, family, and associates. (See "Why Spy?" "Precipitating Crises" on page 31.) Sources of psychological pressure obvious to observers might include a looming bankruptcy, imminent dismissal from work, or a divorce. Sources of psychological crises that are equally acute but invisible to others might include silently carried, lasting rage over perceived slights or injustices, an overwhelming desire for revenge, or other deep-seated feelings or beliefs that compel the vulnerable person to action.

Intelligence services have long exploited crisis states to recruit agents. As described in the 2003 article, unscrupulous services may deliberately create crises in the lives of targets to improve recruitment prospects, for example through escalating gambling debts or entangling the target in a risky sexual or romantic relationship with a partner controlled by the service. Such intelligence services may also find ways to precipitate similar crises in the lives of family members or other loved ones in order to control the prospective spy by offering espionage as a solution to the loved one's predicament. (See "Why Spy?" "Exploitation of the Vulnerable" on page 34.)

As we have seen, the cyber realm is a hazardous environment for those in crisis or easily led to crisis. Those with a propensity for problematic or pathological behavior—for example, uncontrollable gambling, computer gaming, spending, or sexual behavior—will find on the Internet remarkably easy ways to reach outlets for their addictions or compulsions. In cases such as these, the name "World Wide Web" is apt: psychologically vulnerable people, like insects in a spider's web, do get snared online. In addition, while they may believe they have found relatively safe outlets for their pathological or hazardous behavior, they are subjecting themselves to the possibility they will be tracked and risk suffering crises

a. This is an evolution of the now-classic adage "On the Internet, nobody knows you're a dog," the caption of a 1993 *New Yorker* cartoon by Peter Steiner featuring two dogs, one sitting on a chair working on a computer, making the above observation to the other dog, seated on the floor. The cartoon quickly became iconic and signaled the moment when global culture recognized the pervasive problems of identity on the Internet, where a user can never fully trust or know the true natures of unseen interlocutors.

of embarrassment or becoming the subjects of the attention of those eager to find and exploit vulnerable persons. Finally, the more a person's online life becomes the center of his or her consciousness and motivation, the more real-life, stabilizing commitments—to self-care, to others, to community—will weaken and attenuate. Work, relationships, health, financial status, and lifestyles suffer for people who have arrived at this point, causing the kinds of tangible, IRL crises that might bring a person with access to national security information to the attention of hostile intelligence services, and from there lead them into espionage.

More subtly, in a context in which seemingly complete anonymity enables the expression of all desires, no matter how deviant, dangerous, or harmful to others, no brakes on behavior exist other than those a person already possesses when entering cyberspace. For the group of people we are discussing—people with personality pathologies, in crisis—these brakes are often already weak and likely to grow weaker.

For those with moral qualms, Internet content can provide justification for behavior that leads to crises and to subsequent illegal choices. That justification can come from online dialogue with kindred spirits or with more focused interlocutors such as intelligence service officers, e.g., agent recruiters, pursuing their own goals through manipulating a person's crisis. Platforms seeking leakers may also manipulate a vulnerable person who is experiencing what he or she perceives as a crisis of conscience.

For others seeking justification, online material assists in rationalizing or trivializing acts such as espionage or leaking of national security information. This nullifying effect of the Internet, where qualms about espionage and leaking are neutralized by comparisons to a glut of "worse" behavior—is often underestimated. FBI Special Agent Robert Hanssen made this argument when he stated to an interviewer who was sharply challenging him to recognize the consequences of his espionage, "In the whole march of history, a little espionage doesn't amount to a hill of beans." (See "Why Spy?" "Robert Hanssen: Self-Designated Cold Warrior" on page 30 for a review of the case.) Today's spies need not turn to human history to find ways to minimize their behavior; they need only visit the Dark Web in the present moment and see what transpires there.[a]

In his book on Internet crime, former FBI futurist-in-residence, Interpol advisor, and police officer Marc Goodman devoted a section to the Dark Web entitled "Into the Abyss."[18] He used the metaphor of Dante's circles of hell to provide, in escalating order of gravity, a long list of illegal goods and services accessible to paying anonymous customers, ranging from pirated content to drugs, to legal documents (passports, citizenship papers, transcripts, professional licenses), trafficking in organs and humans, and murder-for-hire. He ended the list by describing a site that offered the opportunity to witness through live streaming the worst acts of child abuse—while interacting with other paying anonymous customers and the perpetrators. Goodman called this the very center of hell, and concluded that "the Internet provides a delivery system for pathological states of mind."

The Dark Web is also an education in nihilism. A prospective spy can find there sufficient reason to discard doubts and move forward into espionage or leaking. After such exposure, for those with compromised moral compasses, espionage seems trivial and leaking seems a lark. People with strong inherent moral compasses and an uncompromised capacity to stay grounded in concrete reality understand that behavior online has consequences in real life, such as the real plight of child and adult victims in Internet-mediated crimes.

Ease of Opportunity

The third necessary element in spying is connecting with a customer, patron, or platform interested in the information on offer. It is in this third element that the greatest changes have occurred since the publication of "Why Spy?" (See "Elements of Espionage" on page 20.) Those currently seeking to connect with customers or platforms for either espionage or leaking now have many

a. The Dark Web forms a small part of the Deep Web, which is the part of the Web not indexed by search engines. Because of free software, anonymity in the Dark Web is at present almost unbreakable, enabling hackers, terrorists, gangsters of every sort, pedophiles, and other criminals to transact their business there in safety, unless they become subject to their own "insider threat" (undercover police informants, for example). More positively, the Dark Web also provides a venue in which political dissidents and others with positive or non-criminal intent are able to communicate and collaborate in relative safety. (See Kristin Finklea, *Dark Web*, Congressional Research Service Report R44101, 10 March 2017.)

more possibilities and opportunities to explore via the Internet. Those considering leaking have a dizzying array of possible online venues to leak to as well as the promise of global dissemination of the information they provide. Many websites now include instructions for potential leakers, and these customers or patrons provide the option for anonymity, at least initially.[19] It should be noted that, in contrast to media, professional intelligence services do not generally handle anonymous agents for reasons of safety and veracity.

The Experience of Spying After Making the Connection and Commitment

Espionage

The information age has altered the environment for professional intelligence officers handling agents, not just in how they spot and recruit potential spies but also in managing agents engaged in espionage. Handlers work hard to stabilize their agents once they have started spying, because operational security and maintaining cover are paramount in sustaining the espionage, and unstable agents cannot attend to either. For example, a handler will work to prevent an agent from pursuing attention and affirmation by showboating online, will step in to head off or settle crises in the life of the agent (somewhat ironically, given the critical prerecruitment role of life crises in priming potential agents to consider espionage), and if the agent is motivated by the desire to earn a place in history, the handler will provide reassurances about the spy's impact and offer substitutes for the missed acclaim. Keeping a watchful eye on and reducing the destabilizing elements of the Internet in the agent's life is part of contemporary professional intelligence officer tradecraft.

Leaking

Such stabilization is generally not the case for leakers, many of whom seek immediate rewards and visible impact on a global scale, now achievable via the Internet. The attention of others is for many the main currency of reward online, and being noticed and famous is often the primary psychological reward pursued by leakers.[20] Psychologically gratifying attention can come in the form of either fame or infamy—even if the leaker's name is never revealed. In many cases leakers get a double dose of attention and reward: intense responses from admirers and opponents, who engage in vituperative conflicts with each other, adding lulz to the reward accruing to the leaker. As a result, encouraged and validated and absent the stabilizing presence of a professional handler, leakers will tend to intensify their activities, chasing more acclaim, excitement, a sense of power and efficacy—until they are unmasked.

❖ ❖ ❖

Remedies, Risk Management, and a Caution

My focus throughout this article has been on the human dimension of espionage and leaking, not on specific counterintelligence and security tools, programs, or techniques. The recommendations I made in 2003 remain as relevant today as they were then. (See "Remedies and Risk Management" on page 35.) Safeguarding entry points into Intelligence Community agencies through applicant screening remains a cornerstone of institutional risk mitigation against insider threats. We also still need programs designed to spot and address warning signs in employees' behavior or in their circumstances; we still must provide support to troubled employees to help them through their crises and return to productivity and a sense of belonging to the community at work.

These measures, necessary and still vital, are not, however, sufficient anymore. In "Why Spy?" I also suggested broad programs of education and community-building. In the digital era, these are now keystones to mitigating the risk of employees' becoming spies.

Actively Counter Loneliness and Safeguard and Build the Community

The psychological malady of the digital age—paradoxically, given its positive, extraordinary capacity to connect millions across the globe—is loneliness and its close cousin, alienation. These conditions do not apply pervasively, of course. For the majority of people, digital connectivity is just one more way to initiate, sustain, or complement healthy interpersonal relationships. As noted throughout this article, however, the Internet is a dangerous place for the vulnerable—

those who struggle with relationships IRL, and may be alienated from other aspects of real life, or those who find themselves temporarily alone and at loose ends.

In the face of the risks exacerbated or caused by loneliness and alienation, frequent organizationally sponsored events in workplaces—with people in physical attendance, not virtually present—have never been more critical to counterintelligence. When vulnerable employees are embedded in communities in which they feel they belong and are accepted, the risk of their acting on their vulnerabilities in times of personal crisis is mitigated. They will be less prone to seek connections and relief in the dangerous domains of the Internet or susceptible to relationships offered by those seeking to manipulate and exploit them.

Examples of significant traditions and community-building at CIA include annual events such as Family Day and Combined Federal Campaign (CFC) fundraising events before the winter holidays, during which offices and teams develop creative methods, including book sales and auctions, to raise funds—one particularly memorable fundraiser was the auctioning of a gingerbread replica of the model of Usama Bin Ladin's compound used in planning the SEAL operation against him in 2011. Also important is the commemoration of those lost in service held at CIA's Memorial Wall each May. Presentations by outside speakers in the Headquarters auditorium that are open to all employees and attended and moderated by senior leaders have also become highly popular opportunities for the workforce to gather and consider issues and ideas important to the mission and experiences of professional intelligence officers.

Volunteer employee groups should be actively supported, provided senior sponsors, and validated by the attention of senior leaders, and these groups should be encouraged to reach out to colleagues who seem to need help in connecting with community. In the digital era, such elements of community life in intelligence agencies have moved from being "nice to have" morale-builders to critical features of security and counterintelligence risk mitigation.

The Intelligence Community can also fight digital fire with fire by encouraging its online, secure, classified "village commons" to flourish and grow, including supporting those commons as venues for expressions of creativity, opinion, critique, and even dissent. We can count on the lack of anonymity in these online government-sponsored venues to avert the ills that plague the open Internet: trolling, harassment, bullying, hacking, and the like. At present our secure, classified online venues parallel the best of Internet values and provide a precious insider-threat risk-mitigating resource that must be protected despite potential disclosure risks.[21] Efforts to manage the risks that come from permitting open, online discourse should be devised in ways that protect the current vibrancy of this classified cyber community, because the vitality and the bonds created there will spill over into the Intelligence Community.

One of the hidden benefits of the prohibition of most portable personal devices in Intelligence Community buildings is connection; people are not locked into their screens in meetings and gatherings. This occasionally inconvenient (sometimes very inconvenient) but necessary security requirement may disappear at some point but at present we should celebrate our simple, yet profound, difference from the rest of the working world: we converse with each other, rather than with our screens, in the "open" moments before and after meetings, in the cafeteria, and in our hallways. We have opportunities to break away from the "holding power" of our devices and are therefore able to enjoy the best of both the digital world and the concrete, IRL, material world.

A Caution: The Phenomenology of Surveillance[a]

Big data, allied with machine learning and cognitive computing, has ushered in an amazing panoply of digital surveillance methods purporting to evaluate, profile, and predict the behavior of people, based on the record of their activities online.[22] New technological tools collect and exploit the trail of information—sometimes labeled "digital exhaust"—that all people leave in IT systems as they go about their normal activities at work and in their personal lives. Big data and computing power together allow an individual's present behavior to be evaluated against his or her personal baseline of past behavior; changes and anomalies—for good or ill—can be flagged and analyzed. Proponents

a. Phenomenology is a specialized branch of philosophy and psychology that studies subjective experience. Here I address how people subjectively experience surveillance when they are aware of being subject to it and how people subjectively experience the process of surveilling others.

of such methods assert that they can be used to expose in intimate detail the psyche driving behavior, including assessing and predicting the current and potential risks individuals present to systems, to others, and to themselves.

For example, some elements of spoken and written language unrelated to the content or meaning being communicated—behaviors such as a person's habitual choice of words, repeated use of certain grammatical structures, tempo, and syntax—can shed light on a person's identity, background (regional and educational), state of mind, and emotions at the moment of communication. The "sentiments" expressed by others—such as colleagues, neighbors, friends, and even family members—about a particular person can be collected and assessed using the same methods corporations use to track public sentiments surrounding their brands.[23]

Currently employers, private corporations, politicians, and governments are applying these and other data analysis tools to assess, influence, and monitor persons and groups. The promise of such techniques to assist security and counterintelligence insider-threat programs is self-evident, but there are risks that must be taken into account in using them and costs to be tallied and weighed against promised benefits. (See Textbox 3, which addresses this point, on the following page.)

There exists a robust body of empirical research in the social and behavioral sciences tallying the potential negative effects on people and organizations of pervasive surveillance.[24] The current complex and heated cultural debate surrounding surveillance and privacy issues can be framed in many ways: political, legal, philosophical/ethical, and institutional risk management, as well as in terms of individual personality differences in support of and tolerance for surveillance.[25] For the purposes of this article, I focus on research that sheds light on how people experience surveillance psychologically and the potential consequences of those experiences on individual psyches and therefore on their attitudes and behavior.

What the research shows is that people dislike being surveilled.[26] Most, however, will tolerate some level of intrusion, if they believe it is necessary for institutional and social safety and to maintain order.[27] The surveillance, however, must be experienced as fair and transparent; the consensus from studies in management science in this area is that honest communication with employees—and citizens—about the specific nature of and need for surveillance is critical to gaining acceptance and compliance. Being able to judge for themselves if the level of surveillance is reasonable and knowing with some specificity about the methods used returns some of the personal autonomy that surveillance inevitably removes and recalibrates the relationship of trust and fair-dealing between the surveillors and the surveilled.

Government reports have reached the same conclusions. An atmosphere of constant observation that is perceived to be aimed at control rather than stopping wrongdoing breeds resentment and a tendency toward hidden protest; such surveillance at work undermines morale and productivity, increases stress, and undermines loyalty to the organization. Furthermore, blanket surveillance methods risk flattening a culture into blandness and dulling its creative edge. (See the "Appendix: Considerations on the State of Surveillance in Democratic Societies," beginning on page 11.)

Finally, it is important to be wary of the long-term, eroding effects of blanket, intrusive, or shadowy surveillance on the composition of teams or across an organization's workforce. Social and behavioral science research has demonstrated that there are individual differences in attitudes toward and tolerance of workplace surveillance. Technol-ogy-driven assessment and surveil-lance tools pervading a workplace are likely to repel highly autonomous, creative, questioning people who then self-select themselves out of the team or organization, leaving behind a concentrated group of people whose temperaments tend toward caution, order, and safety, and who are comfortable with established systems for security and institutional control. Over time, the "diversity of mind and temperament" necessary for an intellectually fresh, creative organization is damaged by systematic loss of certain types of productive, psychologically healthy people, irrespective of which type they happen to be.

Active Support for CI and Security Officers

In this dawning digital age, those responsible for protecting employees and information in the Intelligence Community have extraordinarily difficult jobs. Pre-Internet and pre-digital methods still apply somewhat, but new technology-driven risks prolifer-

Textbox 3: Weighing Costs and Benefits—Security at Fort Detrick in the Wake of the 2001 Anthrax Attacks

The week after the 9/11 terrorist attack, letters containing anthrax spores were mailed to several news media offices and to two US Senators over the course of several weeks, killing five people and infecting over a dozen more. After a long and complex investigation, the FBI homed in on microbiologist Bruce Ivens, a senior biodefense researcher at the US Army Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland. Ivens committed suicide in July 2008 while anticipating his imminent arrest. The investigation had revealed that Ivens had longstanding severe psychiatric conditions; several mental health professionals who had treated him over the years considered him highly dangerous to them, to himself, and others. At work he had shown behavior ranging from the eccentric to the bizarre.

After it was created in 2002, the Department of Homeland Security established the National Biodefense Analysis and Countermeasures Center (NBACC). The center soon developed a program—Personnel Reliability Program (PRP)—to identify specific psychological characteristics to be assessed in "more comprehensive" security evaluations of scientists and technicians and other "agents" working with the most dangerous biological materials. The PRP-recommended characteristics to be evaluated are: mental alertness, mental and emotional stability, trustworthiness, freedom from unstable medical conditions, dependability in accepting responsibilities, effective performance, flexibility in adjusting to change, good social adjustment, ability to exercise sound judgment [in emergencies], freedom from drug/alcohol abuse and dependence, compliance with requirements, and a positive attitude toward the Personnel Reliability Program (PRP).[28]

Setting aside for the sake of argument the infeasibility—on a technical assessment level—of psychologically screening personnel for these characteristics with any degree of scientific reliability and validity, taken together they depict a certain type of person: dependable, responsible, comfortable complying with authority and rules, conscientious, socially and emotionally stable, and predictable. If people could be hired and retained on the basis of these criteria, dangerous biological agents would certainly be in good hands. On the other hand, would a research program staffed solely with this type of person perform with insightful, prescient, inventive science? While the PRP's criteria might reduce the insider threat in USAMRIID labs, the ability of the resulting team to carry out its missions through innovative, cutting-edge science might also be compromised.

ate, adapt, or mutate before countermeasures can be fully conceived, tested, and applied. For leaders and officers serving in the domains of security and counterintelligence, the situation today is analogous to the challenges faced by military leaders and combat commanders at the dawn of mechanized warfare in the early 20th century. Horse cavalry eventually became armored cavalry, and "best practices" in the craft and art of tank warfare became normative, but the moments on the battlefields when military professionals relying on horses were first confronted with tanks must have been terrifying, as were those when infantrymen faced barrages of artillery and machine gun fire unimaginable previously.

We are confronting such a seismic moment now in the world of professional intelligence. In addition, security and counterintelligence officers have to manage, as never before, the core dilemma of balancing the need for technology augmented, state-of-the-art security methods against the importance of also protecting the scope of responsibility, access to information, capacity for informal open discussion with peers that broadens thinking and lends unexpected, fresh perspective to important questions, and the fundamental inquisitiveness, openness, and trust necessary to sustain a creative, engaged, and agile workforce. Counterintelligence and security officers wrestling with these always exigent, but now intensifying, dilemmas need our full support, not just in concrete resources, but in recognition of the enormity of what they face and the daily tough decisions they must make to safeguard their organizations, colleagues, and our common mission.

Conclusion

Today's intelligence officers know they are serving in tumultuous, exciting, astonishing, and dangerous times. In every generation, a few insiders have chosen the destructive path of betrayal and harmed themselves, their families, their nation, and many others who trusted in the United States to keep them safe. Three things keep loyal insiders going when news breaks of another case of espionage or leaking by one of our own: our personal commitment to our mission; our bonds of trust with our colleagues and teams; and the example of the generations of patriots who served before us, who also weathered betrayals by some of their own. So we keep faith, serve the Constitution with integrity and to the best of our abilities, and expect to pass the torch on to a new generation of officers who will do the same.

❖ ❖ ❖

Appendix: Considerations on the State of Surveillance in Democratic Societies

The discussion within democratic societies about the abundance of data, computing power, privacy and security (some frame this as a political conflict between civil rights and government surveillance) is ongoing. Below are some highlights for consideration.

George Orwell, 1984

Orwell's classic 1949 novel has enjoyed a resurgence in popularity because of renewed focus on privacy issues and fear of totalitarian government control enabled by technology.[29] The novel explores the psychology of surveillance from the perspective of the surveilled. Orwell counted on his readers' intuitive understanding of the motives of a protagonist who would risk everything to secure a bit of privacy in a world characterized by "Big Brother's" oversight of every aspect of life. The novel's enduring power results from the readers' empathy for the fictional Winston Smith's effort to resist, and his ultimate failure to attain even a small measure of autonomy, making it one of the great tragic novels in the Western canon.

INSA, 2017

In April 2017 the Intelligence and National Security Alliance (INSA) published a list of state-of-the-art surveillance tools available to organizations interested in mitigating insider risks, particularly in the national security context.[30] The document suggested mitigating insider threat through "leveraging innovative technology and data sources to monitor and evaluate individuals on a continuous basis" and noted that the listed computer-based tools could assist in "swift, continuous identification and assessment." It defined the technology-driven surveillance process as follows:

> *Effective monitoring tools . . . take advantage of technology to surpass standard [personnel] screening. . . . In particular, advanced text analytics and psycholinguistic tools that track an employee's communications across social media and other platforms to detect life stressors and analyze sentiment can help detect potential issues early. . . . Another critical element is improving the sharing of information within the organizations among managers, human resources, information technology (IT), security, and legal advisers regarding minor counterproductive work behaviors that may indicate an employee struggling and at heightened risks of committing a malicious act.*

The INSA document notes that this "continuous monitoring" approach to mitigating insider threat might have implications for "workplace morale," "civil liberties," and concludes that each organization must arrive at its own culture-driven decisions about the optimal balance of privacy and security in the organization:

> *In the end, this is a critical risk management exercise for senior leaders in all organizations as the destructive power of malicious insiders grows and the tools to monitor and mitigate become more sophisticated and intrusive.*

White House Review Group, 2013

Similarly, a 2013 report to the White House from the President's Review Group on Intelligence and Communications Technologies recommended the following:

> *All personnel with access to classified information should be included in a Personnel Continuous Monitoring Program (PCMP). The PCMP would access both internally available and commercially available information, such as credit scores, court judgments, traffic violations, and other arrests. (239)*

The authors added:

> *We recognize that such a program could be seen by some as an infringement of the privacy of federal employees and contractors. . . . But, employment in government jobs with access to special intelligence or special classified programs is not a right . . . we believe that those with the greatest amount of access to sensitive programs and information should be subject to Additional Monitoring . . . (240–41)*[31]

The House of Lords, 2009

In February 2009, the British Parliament received a document from a House of Lords committee titled *Surveillance: Citizens and State.*[32] It reported the results of a general review of methods and practices and included recommendations for future actions. It also described concerns that ubiquitous surveillance is changing the relationship between citizen and state.

The report quoted a professor of sociology and deputy director of Criminological Research at the University of Sheffield:

> *Mass surveillance promotes the view . . . that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted. (27)*

The report also described the distinct social gains—tangible and perceived—of broad surveillance programs, particularly in countering terrorism and crime, and it summarized empirical data suggesting that most citizens support the counterterrorism and crime-fighting functions of surveillance. The report quoted a senior constable and chair of The Association of Chief Police Officers CCTV Working Group, who said:

> *Several years ago London was suffering from a nail bombing campaign by an individual . . . targeting specific parts of London with his nail bombs and there were extremist groups claiming responsibility for the actions. That event was entirely supported by CCTV evidence in terms of actually detecting the crime. What value do you put on the price of that detection?(21)*

Emrys Westacott, 2010

Philosopher Emrys Westacott begins a 2010 article in *Philosophy Now* by asking if Adam and Eve would have eaten the forbidden apple had God installed CCTV cameras in Eden.[33] A more serious discussion follows this amusing opening in which Westacott explores the distinct pragmatic social benefits that derive from some forms of surveillance (for example, from traffic cameras) and also the harms that too much surveillance, or certain forms of surveillance, can cause by eroding bonds of trust within society, particularly between those who control the surveillance and those being surveilled. He asks, hypothetically, if you would you rather attend Scrutiny College, where examination rooms are equipped with several cameras and jammers prevent the use of private devices for cheating, or Probity College, where students are trusted to abide by an ethics code. The philosopher argues that blanket surveillance aimed at control undermines the ideal that persons in society will behave responsibly because they want to, out of love and respect for themselves and others. He concludes that too much monitoring destroys the free bonds between people in societies; it weakens the internal moral compasses of both the people and their society. He also concludes, however, that not enough surveillance of people's behavior results in a lawless state, as we have seen on the Dark Web.

❖ ❖ ❖

Notes and Sources:

1. ***Author Note***: When I was drafting my first article on the psychology of espionage 15 years ago, I relied on a long and established history of classified and unclassified scholarship on espionage that has accrued since the establishment of CIA's forebear, the OSS, in WWII. In contrast to the robust, longstanding literature that was then available to me, this essay on the psychology of digital-age spying must be more provisional. The current social and cultural contexts—in real life, online, domestically, and globally—are developing too rapidly to arrive at definitive conclusions about all of the elements at the core of the psyches and behavior of today's spies, particularly how they experience their espionage and leaking and the people, groups, and technologies assisting them in spying.

2. ***Cyber vs. Material Reality:*** Some argue that cyber reality is a part of material reality because it exists; however, the anchors of time, place, and physical contact are different in the digital and the concrete realms. For purposes of discussing how vulnerable people experience both cyber and concrete reality and navigate between the two psychologically, they are treated as distinct in this article, though there are some who would dispute this distinction and consider it as arbitrary as the mind/body division.

3. ***Evolving Insider Threat Model:*** In the past decade the model of "insider threat"—applicable to both private and public sectors—has evolved, and is commonly understood to include five types of threats from people inside organizations: spills, leaks, espionage, sabotage, and workplace violence. The focus of this essay is on those who leak and commit espionage. The five types of threats can overlap: leaking and espionage can include elements of sabotage and even workplace violence because the spy's underlying intent may be aggressive, aimed at harming an organization and sometimes targeting specific individuals for danger or distress. CIA officer William Kampiles, for example, said that one of his reasons for committing espionage was to get back at his supervisor who had not supported his desire to leave his entry-level job as a watch officer prematurely in order to gain entry into the operational domain. (See: "Why Spy?": "William Kampiles: Self-Styled Special Agent" on page 28.) FBI Special Agent Robert Hanssen was bitterly angry at and contemptuous of the FBI when he spied for the Russians. (See: "Why Spy?": "Robert Hanssen: Self-Designated Cold Warrior" on page 30.) Sometimes the danger and violence to others is secondary to the primary goals of the spy; danger to others might be an inevitable and predictable outcome of the espionage. In some cases the spy deliberately pursues harming others as a safeguard against being caught. Many Soviet citizens spying for the United States lost their lives when Aldrich Ames deliberately identified them to his Soviet handlers in order to prevent them from alerting their CIA handlers that there was a mole in CIA, which would have triggered an internal counterintelligence investigation, endangering Ames. By his own admission, Ames was purely driven by money, and he equated the risks he was taking for the Soviets to those Russian agents were taking when spying for the United States. In support of this article's theme of personality pathology and espionage, the author notes the psychopathic nature of Ames's rationalization of his ruthless elimination of those endangering him, and yet he remains alive, albeit in prison for life. In contrast, most of the agents he identified to the Soviets eventually were executed in Soviet prisons.

4. For examples of the application of such means in the corporate world, see Doug Laney, "Data as Corporate Asset: Private Sector Applications of Data Science" in *Studies in Intelligence* 61, No. 1 (March 2017).

5. ***Mind and Machines:*** For classics and contemporary overviews of the psychological effects of machines, devices, and technology on humans and culture, see: Louis Mumford, *Technics & Civilization* (Harcourt, Inc, 1934); Sherry Turkle, *The Second Self: Computers and the Human Spirit* (Simon & Shuster, 1984) and (MIT Press, 2005); Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (Touchstone, 1997); Sherry Turkle, *The Inner History of Devices* (MIT Press, 2008); James Gleick, *The Information* (Pantheon Books, 2005); Nicholas Carr, *The Shallows: What the Internet is Doing to Our Brains* (W.W. Norton, 2011); Kirsten Weir, "(Dis)Connected: Psychologists' Research Shows How Smartphones are Affecting Our Health and Well-Being, and Points the Way Toward Taking Back Control," *American Psychological Association Monitor* 48, No. 3 (March 2017): 42.

6. ***Spilling and J.K. Rowling.*** A spill may be caused by misjudgments or accidental inclusion of classified materials with documents authorized for release, or by skilled elicitors who induce people to say more than they should or intend. Sometimes spillers remain unaware of the spillage, whereas spies always know they are spying. In the digital age, spills may be caused by technical errors involving little human agency. A famous example of spilling is the revelation in July 2013 that Harry Potter author J.K. Rowling was also the author "Robert Galbraith," a pseudonym Rowling had used to publish an adult detective novel. Rowling's identity was spilled by one of Rowling's lawyers, who had inappropriately discussed the book with his wife's best friend and revealed the author's true name. The friend then tweeted about it to a columnist. Responding to the resulting firestorm of speculation, the lawyer's firm confirmed Rowling's authorship in a statement that included the following language, which illustrates the unwanted, unintentional element of spilling: "We, Russells Solicitors, apologise unreservedly for the disclosure caused by one of our partners, Chris Gossage, in revealing to his wife's best friend, Judith Callegari, during a private conversa-

tion that the true identity of Robert Galbraith was in fact J. K. Rowling. Whilst accepting his own culpability, the disclosure was made in confidence to someone he trusted implicitly." (See Jon Stock, "J.K. Rowling unmasked: the lawyer, the wife, her tweet —and a furious author, " *The Telegraph*, 21 July 2013. Also at www.telegraph.co.uk/culture/books/10192275.)

7. ***The Heroic vs. Self-serving Spy***: This article focuses on self-serving spies or those who have been manipulated or coerced. There is another type of person who commits espionage: the genuinely heroic spy. A critical element of a professional intelligence officer's expertise is the ability to accurately assess the true, underlying conscious or unconscious motives of sources. The evaluators begin by first registering, then looking beyond, the self-images of sources and testing the stated motives against the tangible and emotional benefits actually accruing to them. An officer's true assessment can be quite different from what the officer purveys to a source during handling interactions. Professional officers are trained to use observation, critical thinking, vetting techniques, comparisons with what is known from studies of past cases of espionage, and above all expert judgment to distinguish between sources who are genuinely heroic, and those who are not. Officers also submit their assessments to the scrutiny of their peers, particularly counterintelligence officers who independently evaluate sources and ensure that what is on record about a source's motives for espionage is unbiased and accurate and handling methods are appropriately matched to the source's true motives. While self-serving, manipulated, or coerced spies are the subject of this article, it is important to remember that heroic ones do exist and that their personalities, the crises that led them to spy, and the handling tradecraft appropriate for them are different from those of other types. There is also a distinction—psychological as well as legal—between whistleblowers, who use legal channels to address their ethical or other workplace concerns, and leakers, who bypass legal, authorized channels of redress. Readers who wish to explore the distinctions may be interested in the recently published, newspaper opinion piece written by a Washington, DC, lawyer who handles classified matters and represents whistleblowers in the national security field: Mark S. Zaid, "Reality Winner Isn't a Whistleblower—Or a Victim of Trump's War on Leaks," *Washington Post*, 8 June 2017. See also on this subject, US Department of Labor Occupational Safety and Health Administration, *The Whistleblower Protection Programs*, at https://www.whistleblowers.gov.

8. David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harv. L. Rev*. 127, No. 2 (20 December 2013).

9. Rahul Sagar, "Creaky Leviathan: A Comment on David Pozen's Leaky Leviathan," *Harv. L. Rev.* 127, No. 2 (20 December 2013).

10. William J. Burns and Jared Cohen, "The Rules of the Brave New Cyberworld," Foreign Policy.com (16 February 2017).

11. ***Disclosures in the Private Sector:*** The ethical, legal, and media dynamics surrounding the leaking of classified government information also apply to disclosures of private-sector sensitive or proprietary corporate information. These issues were the central themes, for example, of the film "The Insider," which was based on the true story of a former tobacco industry senior executive and scientist who worked with a reporter to disclose his former employer's effort to suppress information demonstrating that the company was aware of and manipulated the addictive components of cigarettes. The story was originally carried in *Vanity Fair.* (Marie Brenner, "Whistleblower: The Man Who Knew Too Much," May 1996). The article and movie also touched on questions about the scientist's mental stability, motives, and veracity.

12. ***Trolls and Trolling:*** The exact definitions of Internet "trolling" or "trolls" are evolving in tandem with changes in technology. Roughly speaking, there are two broad categories of trolls. Some primarily troll instrumentally and some primarily for fun or "for the lulz"—a variant of LOL, "laugh out loud," in Internet jargon. They differ psychologically in important ways. Those who engage in online manipulation, attack, and sabotage chiefly in pursuit of some other goal, most often financial profit (for example, those who are paid to disrupt commercial websites), may find only limited pleasure in the trolling itself. Their sense of reward (what psychologists call "emotional benefits") comes from achieving the primary goal, such as getting paid. The pleasure-seeking trolls do so for the inherent emotional reward (the "lulz") they generate in the behavior itself. The difference between the instrumental type and the lulz-seeking type is akin to the difference between a professional hit man, for whom killing is an emotionally neutral "professional" act that leads to a secondary reward, and a killer whose gratification resides in the act of killing itself, such as, for example, the sense of god-like power it brings or sadistic pleasure in the suffering of victims. Engaging in destruction for personal gain or for pleasure—an age-old practice among human beings—like so much else in real life has found new expression in cyberspace.

13. ***Readings on Trolls:*** E. E. Buckels, Paul D. Tranpnell, and Delroy L. Paulhus, "Trolls just want to have fun." *Personality and Individual Differences* 67 (2014):97–102. See also: N. Craker and E. March, "The Dark Side of Facebook: The Dark Tetrad, negative social potency, and trolling behaviors," *Personality and Individual Differences* 102 (2016): 79–84. For an early study of the decreased self-monitoring, decreased self-evaluation, and the disinhibiting and de-individuation effects of anonymity online, see: Sara Kiesler, Jane Siegel, Timothy.W. McGuire, "Social psychological aspects of computer-mediated communication,"

American Psychologist 39, No. 10 (October, 1984): 1123–34. For a somewhat different take on trolling that examines how it may not be wholly deviant behavior because it corresponds to and fits comfortably within the contemporary media landscape, readers are directed to Whitney Phillips,"Internet Troll Sub-Culture's Savage Spoofing of Mainstream Media," *Scientific American*, 15 May 2015. The article is excerpted from a book by the same author, *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture* (MIT Press, 2015).

14. This specific survey item from the research cited immediately above was reported by Chris Mooney in *Slate*, on 14 February 2014, in an article titled: "Internet Trolls Really Are Horrible People: Narcissistic, Machiavellian, psychopathic, and sadistic." See http://www.slate.com/articles/health_and_science/climate_desk/2014/02/internet_troll_personality_study_machiavellianism_narcissism_psychopathy.html.

15. ***Dogs on the Internet:*** In 2017, the *New York Daily News* published a cartoon by Bill Bramhall that played off of the 1993 *New Yorker* cartoon and resulting canine-at-a-keyboard meme. The new cartoon captured current alarms about surveillance, diminished or impossible online privacy, and the use of data analytics by private corporations and public agencies to profile, track, and target users who wish to remain incognito when they surf, work, or shop online. Bramhall's cartoon features a solitary dog at his computer confronting a full-screen pop-up advertisement showing a can of dogfood with the caption "You might like ALPO." A word bubble shows the dog thinking: "Whatever happened to 'On the Internet nobody knows you are a dog'?"

16. Turkle, *The Inner History of Devices* and *Identity on the Web*.

17. ***Internet Aliases:*** Anonymous online aliases, rhetoric and slogans often hint at the slyness of psychopathy, the egotism of narcissism, and the fantasies of immaturity. For example, some famous hacker handles are Scorpion, SOLO (which gestures to the allure of being a lone operator and also to the Star Wars character), MafiaBoy, Gigabyte, cOmrade, "why the lucky stiff" (sometimes abbreviated "_why"), Dread Pirate Roberts, Poison League, Commander X. According to the global computer magazine PCWorld, the British hacker SOLO left a message on a compromised machine that read: "*US foreign policy is akin to Government-sponsored terrorism these days . . . I am SOLO. I will continue to disrupt at the highest levels.*" (http://www.pcworld.com/article/2989146/security/infamy-and-alias-11-famous-hackers-and-their-online-handles.html#slide1). A famous online motto is this clever but also barbed inversion, from the hacking group Anonymous, of biblical stories of demonic possession and New Testament values: "*We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us.*"

18. ***The Onion Router:*** Tor ("The Onion Router") is the most popular gateway into the Dark Web. It is free software, enabling anonymous communication through encryption and multiple peer-to-peer Internet relay channels designed to hide users' IP addresses from those interested in tracking them. The result is an untraceable, secure platform that conceals users' location and usage. The concept of "onion routing" (the underlying metaphor is that pursuing an anonymous user through multiple relays is like peeling an onion, never arriving at the core) was developed in the mid-1990s by a mathematician allied with computer scientists at the US Naval Research Laboratory in order to protect US intelligence online communications.

19. ***Leak Bait:*** Sue Halpern, in her review of *Risk*, a documentary portrait of Julian Assange ("The Nihilism of Julian Assange," *The New York Review of Books*, 13 July 2017: 15), writes: "Almost every major newspaper, magazine, and website now has a way for leakers to upload secret information, most through an anonymous, online, open-sourced drop box called Secure Drop . . . *The New York Times*, *The Washington Post*, *The New Yorker*, *Forbes*, and *The Intercept*, to name just a few, all have a way for people to pass secrets along to journalists."

20. Keith Hampton, Lauren Sessions Goulet, Cameron Marlow, and Lee Rainie, "Why Most Facebook Users Get More Than They Give", PEW Internet and American Life Project, 3 February 2012, at http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give; Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other* (Basic Books, 2011).

21. ***Positive Internet Values:*** In an article in *The Wall Street Journal* titled "The Dark Side of the Digital Revolution" (19 April 2013), Google's executive chairman and former CEO Eric Schmidt and Google Ideas Director Jared Cohen described trying to explain the nature of the Internet to North Koreans during a visit to their country. They wrote: "We ended up trying to describe the Internet to North Koreans we met in terms of its values: free expression, freedom of assembly, critical thinking, and meritocracy." These values are evident in the secure digital commons shared by the Intelligence Community but absent the blight that anonymous negative actors bring to the World Wide Web.

22. ***Big Data:*** "Big data" is the term currently in common usage to refer to extremely large data sets that can be analyzed computationally to reveal patterns, trends, and associations, often relating to human behavior and interactions. While "big data" specifically refers to the data itself, the term is also used colloquially to allude to the many uses to which such data can be applied, such as profiling, tracking, predicting, and identifying individuals, and trends or patterns in both individual and group behavior.

For an accessible, balanced book-length view of the benefits, limits, and downsides to society and to corporations of computing technology applied to data, see Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data* (First Mariner, 2014). For easy-to-read skeptical views, see: Tim Harford, "Big Data: Are We Making a Big Mistake?" *Financial Times*, 28 March 2014 at: https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0?mhq5j=e1 and "The Economist Explains: The Backlash Against Big Data" in *The Economist*, 21 April 2014, at https://www.economist.com/blogs/economist-explains/2014/04/economist-explains-10. At present, large-scale data analytics—their powers and capacities and their positive and negative effects on people and culture—are still very much in flux and subject to widespread opinion and debate.

23. ***Psycholinguistics:*** Corporations use big data to engage in so-called "sentiment analysis" to evaluate, based on data available on the Internet, the emotions around their brands. Sentiment analysis means computationally identifying and categorizing opinions expressed in pieces of text, and also now in voice communications, in order to determine whether writers' or speakers' attitudes toward a particular topic, product, or corporation (or brand) trend toward the positive, negative, or neutral. For a discussion of psycholinguistics (or forensic linguistics), including the history of their development and use, validity, reliability, and the stakes to individuals if computational tools applied to linguistics get it wrong in forensic contexts, see Jack Hitt, "Words on trial: Can linguistics solve crimes that stump the police?" in *The New Yorker*, 23 July 2012.

24. ***Readings on Organizational Risks of Surveillance:*** See for example: *Harvard Business Review* Staff, "With Big Data Comes Big Responsibility," *Harvard Business Review,* November 2014; Neil M. Richards, "The Dangers of Surveillance," *Harvard Business Review* 126, 20 May 20 2013; Kirstie Ball, "Workplace Surveillance: An Overview," *Labor History* 51, 1 April 2010; Watson N. Nathan, "The Private Workplace and the Proposed 'Notice of Electronic Monitoring Act': Is 'Notice' Enough?" *Federal Communication Law Journal* 54(1) (2001): 79–104, retrieved at http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1288&context=fclj; Graham Sewell and James R. Barker "Neither Good, Nor Bad, but Dangerous: Surveillance as an Ethical Paradox," *Ethics and Information Technology* 3 (3) (2001): 183–96.

25. ***Readings on Employee Attitudes Toward Surveillance:*** Those interested in individual differences in employee attitudes toward and tolerance of workplace surveillance are directed to: G. Stoney Alder, Marshall Schminke, Terry W. Noel, and Maribeth Kuenzi, "Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation," *Journal of Business Ethics* 80 (2007): 481–98; the *American Management Association/ePolicy Institute. Electronic Monitoring Surveillance Survey* (2007); Bernd Carsten Stahl, Mary Prior, Sara Wilford, Dervla Collins, "Electronic Monitoring in the Workplace: If People Don't Care, Then What is the Relevance?" in John Weckert (ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (Idea Group Publishing, 2005). This last reference explores not only how employees or other subjects react to being surveilled (they do not necessarily see it as problematic, within certain limits) but also how custodians and policy-creators of the surveillance methods react to their roles and the ethical dimensions of their functions. These researchers acknowledge real limitations to their empirical methods (small sample sizes and lack of generalizability) but their findings are still thought-provoking, given that they counter the general, decades-long consensus of scholars in multiple fields that people do not like being surveilled, even if they are willing to tolerate it in some circumstances and contexts.

26. ***Readings on Risks to Individuals of Surveillance:*** For a good academic book-length treatment of the range of issues involved in workplace surveillance, see John Weckert (ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (Idea Group Publishing, 2005) (one article in this book is cited immediately above). Core arguments for and against employee monitoring are examined in Kirsten Martin and R. Edward Freeman, "Some Problems with Employee Monitoring," *Journal of Business Ethics* 43 (2003): 353–61. For an article-length contemporary and a book-length classic exploration of the negative subjective experience of surveillance, see Michael P. Lynch, "Privacy and the Threat to the Self," *New York Times*, 22 June 2013, retrieved at https://opinionator.blogs.nytimes.com/2013/06/22/privacy-and-the-threat-to-the-self/; Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon Books, 1983).

27. The importance of context to acceptance of electronic monitoring is explored in: Lamar Pierce, Daniel C. Snow, Andrew McAfee, "Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity," MIT Sloan Research Paper No. 5029-13, October 2014, retrieved at: http://www.hbs.edu/faculty/Pages/item.aspx?num=51564.

28. Jessica Stern and Ronald Shouten, "Lessons from the anthrax letters" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threat* (Cornell University Press, 2016), 93–94.

29. George Orwell, *1984* (Harcourt, Brace & Co., 1949).

30. *Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation* (http://www.insaonline.org/i/d/a/b/MindofInsider_wp.aspx. See also INSA, *Leveraging Emerging Technologies in the Security Clearance Process*, March 2014

31. Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies,"* December 12, 2013. Available at https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world.

32. United Kingdom House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008–09, *Surveillance: Citizens and the State*, 27. Available at https://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf.

33. Emrys Westacott, "Does Surveillance Make Us Morally Better?" in *Philosophy Now* 79 (June/July, 2010). Available at https://philosophynow.org/search?q=westacott+surveillance.

❖ ❖ ❖

The Psychology of Espionage

Dr. Ursula M. Wilder

"In the whole march of history, a little espionage doesn't amount to a hill of beans."
— FBI spy Robert Hanssen

They [the KGB] *went around and they wrapped all the agents up. I was amazed. I was anxious and amazed and shocked and scared. And in the course of the following years, all of the agents I told them about were recalled, transferred, arrested, whatnot, and then later on some of them were shot. . . . The KGB later told me that they regretted acutely that they had been forced to take those steps* [thereby triggering a mole hunt at CIA]. *Had I known they were going to do that, I either would not have gone and sold them that information or I would have passed them out one by one.*

— CIA mole Aldrich "Rick" Ames[a]

There was just one part of me, a small part of me, I guess, that wanted something that was a bit abandoned, a bit uncontrolled, almost suicidal, maybe.

— Former CIA watch officer William Kampiles

❖ ❖ ❖

People who commit espionage sustain double lives. When a person passes classified information to an enemy, he or she initiates a clandestine second identity. From that time on, a separation must be maintained between the person's secret "spy" identity, with its clandestine activities, and the "non-spy" public self. The covert activities inescapably exert a powerful influence on the person's overt life. They necessitate ongoing efforts at concealment, compartmentation, and deception of those not witting of the espionage, which includes almost everyone in the spy's life. For some people, sustaining such a double identity is exciting and desirable; for others, it is draining and stressful. For a

a. "Why I Spied: Aldrich Ames," *New York Times* interview with Tim Weiner, 31 July 1994. A career CIA case officer, Ames was arrested in 1994 for spying over a nine-year period for the KGB and its successor, the Ministry of Security for the Russian Federation. Ames made a calculated decision to give the Russians the names of US penetrations in Russia who were in position to alert their American handlers—and therefore the FBI—that there was a mole in the CIA. All but one were executed. Weiner wrote, "He sold a Soviet Embassy official the names of two KGB officers secretly working for the FBI in Washington. The price: $50,000. The next month, he volunteered the names of every Soviet intelligence official and military officer he knew was working in the United States, along with whatever else he knew about CIA operations in Moscow . . . he received a wedding present from the KGB: $2 million." Ames is serving a life sentence without parole.

For some people, sustaining a double identity is exciting and desirable; for others, it is draining and stressful.

few heroic people, spying is a moral imperative that they would prefer to avoid but feel compelled to act on.

This article focuses on spies whose espionage appears to be primarily self-interested, rather than altruistic or self-sacrificing. Within this criminal or treasonous type, specific psychological factors commonly occur, providing a guide to understanding the motives, behavior, and experiences of this type of spy. The risk of espionage can be reduced through understanding these psychological patterns and tailoring countermeasures accordingly.

Elements of Espionage

Three essential elements set the conditions for a person's entry into espionage:

- dysfunctions in the personality
- a state of crisis
- ease of opportunity

The converse is true as well. Safeguards or strengths in these areas mitigate the risk of espionage.[a]

First, any consideration of motivation in espionage must closely examine personality pathology. Personality is the mix of traits, attitudes, and values that characterize a person. Spies frequently have pathological personality features that pave the way to espionage, such as thrill seeking, a sense of entitlement, or a desire for power and control. In addition, healthy countervailing traits—such as a calm temperament or strong sense of responsibility—may be either weak or entirely absent.

The second essential motivator is an experience of acute personal crisis resulting in intense distress. Though the spy may have regrets in hindsight, at the time he or she initiates the espionage, it appears a logical decision to solve a problem or the only option available to escape a desperate or painful situation.[b]

Third, ease of opportunity is a prerequisite for espionage. The potential spy must have access not only to classified information but also to an interested "customer." The manipulations of such customers, who are often professionally trained to present themselves to potential spies as rewarding and safe patrons, can be a major determinant in motivating a vulnerable person to take the step of committing espionage.

The elements of personality, crisis, and opportunity do not operate independently. Vulnerabilities in one area generate vulnerabilities in the others. A person with a problematic mix of personality features will tend to have more than the average number of life crises, including job terminations,

a. "Why People Spy," *Project Slammer Report*, December 1992; "Personality Characteristics of Convicted Espionage Offenders," *Slammer Psychology Team Technical Report*, May 1992; and "Managing At Risk Employees," *Project Slammer Report*, February 1993. Project Slammer is an Intelligence Community research effort, initiated in 1983, to understand espionage through in-depth interviews and psychological evaluations of incarcerated spies. More than 40 spies were interviewed.

b. In the wake of the Aldrich Ames case, the CIA surveyed 1,790 randomly selected employees to establish a baseline of employee attitudes and opinions regarding counterintelligence and security policies, procedures, requirements, and training. The results attest to employee awareness of the links between psychological factors and counterintelligence risks. Those surveyed identified emotional instability related to ambition, anger leading to a need for revenge, feelings of being unrecognized and unrewarded, and loneliness as the top vulnerabilities on the road to espionage. They ranked such problem behaviors as drug abuse and illicit sex as second, and various mental crises or stresses brought on by debt, work issues, or psychological factors such as depression as third.

Scope Note

A classified version of this article was published in *Studies in Intelligence* in December 2003. The concepts discussed in the 2003 article are unchanged in this revision, but the case study information contained in textboxes in the original article have been updated with unclassified or declassified material made available since 2003. This revision is intended to supplement the author's re-examination, 14 years later, of the psychological drivers of espionage and of intentional leaking of intelligence data. The latter is an issue the original article and this, now unclassified, article do not address because such leaking was not then the prominent problem it now is. The new article, "Why Spy? Why Leak?" begins on page 1.

Unless otherwise noted, quotations and information about the convicted spies used in this article are drawn from multiple sources, including law enforcement investigative documents, counterintelligence reports, court documents, and publicly available media accounts and books about US espionage and intelligence.

relationship or family problems, and financial troubles. Such personal crises will, in turn, further stress and magnify problematic traits and behaviors just when the person needs most to function with stability and maturity. Agents "spotting" a vulnerable person may insinuate themselves into the situation and find ways to exacerbate the personal crisis, "ripening" a targeted person's vulnerability to recruitment. Handlers will then continue to manipulate a recruited asset's vulnerabilities to maintain the person's long-term engagement in espionage.

The descriptive categories that follow are offered as a map of the psychological terrain of espionage. All maps oversimplify to a degree, and so does this one. No typology can encompass the full complexity of the psyche of any individual spy. Moreover, a proportion of people caught in criminally oriented or self-serving espionage will not fit the predicted patterns. Therefore, the typology must be applied with caution. Trained professionals can apply these concepts to mitigate risk in contexts such as applicant screenings and evaluations for clearances. Managers and other members of the Intelligence Community may use this information to sharpen their awareness of potentially risky behavior patterns. They should bear in mind, however, that these psychological patterns do not always lead to trouble—and that many troubled people do not exhibit these patterns.

Psychopathy

Money was a solution. Sorry about this, Hollywood. Sorry about this, Church. Sorry about this, everybody, but money solves everything. And it did. And why did it all fall apart? You wanna know? I'll tell you. Because the Soviets cut off the money supply and the old lady—I couldn't pay her off anymore—so she picked up the phone [tipping off the FBI]. *Otherwise I would not be sitting here. Money solves everything.*[a]

—Navy spy John Walker

If I really thought of the consequences all the time, I certainly wouldn't have been in the business. I'm sure that the people from Dow Chemicals in Delaware, I'm sure that they didn't think of the consequences of selling Napalm. If they did, they wouldn't be working at the factory. I doubt very much that they felt any more responsible for the ultimate use than I did for my equipment.

—Former CIA Communications Officer, illegal arms merchant, and access agent for the Cubans Frank Terpil[b]

No typology can encompass the full complexity of the psyche of any individual spy.

I don't believe that I was affecting the security of this country [the United States] *and the safety of its people. . . . I didn't give that stuff to the Soviets because I thought espionage is a dirty game. I mean, that's trivial.*

—CIA mole Rick Ames[c]

Psychopaths are predators, approaching life with remorselessness, manipulation, pursuit of risk and excitement, and sharp, short-term tactical abilities alongside poor long-term and strategic planning. They frequently leave people with a positive first impression. Over time and with extended exposure, the initial impression wears away as people become aware of, or are directly victimized by, the psychopath. Before they are unmasked, psychopaths can cause severe damage to individuals and institutions.

Psychopaths cannot consistently follow laws, rules, and customs and do not understand the social necessity of doing so. They have limited capacity to experience the feelings of guilt, shame, and remorse that are the building blocks of mature

a. See case study on page 24.

b. *Frank Terpil: Confessions of a Dangerous Man*, documentary directed by Anthony Thomas, 1981, WGBH (Boston). Terpil's comment related to his selling weapons, explosives, torture instruments, poisons, and classified information to such customers as African dictator Idi Amin, Libya, and assorted terrorists. Terpil was a CIA communications officer who resigned under duress in 1972. Arrested in New York in 1979 for illegal arms dealing, he fled the United States while free on bail. He was tried in absentia and sentenced to over 60 years in prison for illegal arms dealing. As a fugitive, he began working with Cuban intelligence as an access agent, targeting former CIA colleagues. He died in Havana in March 2016.

c. In the 1994 *New York Times* interview from which this quote is drawn, reporter Weiner described Ames as follows: "Since the 53-year-old Ames was arrested, his hair and skin have grayed perceptibly. On the surface, he is smooth, beguiling, sometimes charming. He fumbles for words only when he considers the nature of his treason and then that calm exterior cracks. His interior? There is an emptiness where pain or rage or shame should be."

Case Studies in Investigating Espionage: Use and Limitations

Experts in the Intelligence Community and outside scholars rely on case studies for insights into the motives and behavior of those who spy. Case studies look backward and highlight warning signs that in hindsight become obvious. Because it can be easy to discount the factors that obscured such signs, case study methods run the risk of hindsight and confirmation bias, focusing solely on the spy and insufficiently on the context. Often spies go undetected by exploiting or manipulating routine organizational processes and accepted customs or practices, first to "survive" in the system despite problems in personality and job performance, and later to cover their espionage. Sometimes larger organizational variables erode or undermine counterintelligence and security practices to such a degree that these variables are arguably equally instrumental in espionage. The term "systemic failure" is often used in official reports after major catastrophes to account for such variables. It is important, therefore, not to assume that the problem of espionage resides solely in the nature of the individual spy; problems in the context within which the spy operates can be equally serious.[a]

Alert readers will point out that experts in espionage only have arrested spies to study and that there may be some who have "gotten away with it." These spies would by definition not be included in our study sample, and therefore our model only describes those who get caught. Ironically, many caught spies eventually tell investigators they were certain they had the skills to avoid capture, unlike their less skilled counterparts. Nicholson, for example, said this about his fellow case officer Ames, whose arrest prompted Nicholson to start his own espionage and "do better" at not getting caught. FBI special agent Hanseen served in counterintelligence and was convinced he could outperform the spies he was tasked to study and catch.

It is extremely difficult to predict complex, relatively rare human behavior such as espionage because of the problem of false positives: many people demonstrate the common warning signs that can lead to the the decision to spy but most will never engage in espionage. It is equally difficult for an organization to detect, measure, and therefore account for the reasons behind good-news "success" stories, for example, when a budding insider threat is recognized early and effectively addressed before causing great harm.

The small number of arrested spies means there is insufficient statistical power to conduct meaningful empirical analyses to predict who in an organization will become a spy. For example, the press dubbed 1985 the "Year of the Spy" because of a string of high-profile cases: eight Intelligence Community insiders were arrested that year on charges of espionage. In fact, the previous year the FBI had apprehended a much larger number: 12.[b] Even in these two consecutive "banner years" for espionage arrests, the total number of spies (20 individuals) was vanishingly small compared to the millions in the US government with top secret accesses who did not commit espionage. The low base rate for espionage cases has not changed since the mid-80s. The *2015 Annual Report of Security Clearances Determinations* by the Office of the Director of National Intelligence reports that 1,220,678 top secret security clearances were active in 2015, and arrests for espionage in 2015 were in no way comparable to the "high" of 20 cases in 1984 and 1985.

In sum, as a result of these limitations, the Intelligence Community turns to in-depth psychological assessments to better understand the psychology of espionage.[c] The long-term consensus among Community counterintelligence professionals (psychologists, law enforcement and investigative professionals, and analysts) is that the key individual variables motivating espionage described in this article—personality, crisis, and opportunity—are supported through the accumulation of case studies of arrested spies since formal psychological and investigative studies began during and after WWII.

---

a. A good example of a study that addresses the relationship of organizational processes to an insider crime is Amy B. Zegart's case study of the Army psychiatrist, Maj. Nidal Malik Hasan, who killed 14 soldiers and wounded 43 in a military deployment center at Ft. Hood, TX. See "The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Cornell University Press, 2017), 42–74. The book contains numerous other useful case studies.

b. https://www.fbi.gov/history/famous-cases/year-of-the-spy-1985.

c. Alexander L. George and Andrew Bennet, *Case Studies and Theory Development in the Social Sciences*, 4th ed. (MIT Press, 2005).

conscience and moral functioning. They are facile liars. In fact, many psychopaths take inordinate pleasure in lying because perpetrating an effective "con" gives them a sense of power and control over the person lied to, an emotional charge sometimes termed "duping delight."[a] Their glee in manipulating others may be so acute that it overrides judgment and good sense, causing them to take foolish risks simply for the pleasure of temporarily conning others.

Psychopaths are interpersonally exploitative. The condition is not infrequently associated with acute cruelty and the enjoyment of inflicting pain on others. Harming or alarming others is, to psychopaths, its own reward. They pursue these pleasures with relish irrespective of the risks involved or the limited potential for gain.

Navy spy John Walker illustrates the manipulative, exploitative, predatory characteristics of psychopaths. (See case study on next page.) Faced with retirement, he aggressively recruited family members to preserve his access to classified materials. Walker also exhibited a psychopath's excessive need for excitement and characteristic pursuit of thrills and adventure. This need for stimulation can express itself in multiple ways and in many contexts, such as in gleefully breaking rules and disregarding social conventions, deliberately provoking authority, harming others or their property, using drugs illegally, and engaging in hazardous physical activities such as excessive speeding or extremely dangerous sports.

In the workplace, psychopaths are noteworthy for their central roles in frequent, enduring, and bitter conflicts.

Finally, psychopaths rarely learn from mistakes and have difficulty seeing beyond the present. Consequently, they have deficient long-term planning, and their judgment is weak. In contrast to their problems in strategic planning, psychopaths can be supremely skilled tacticians and exceptionally quick on their feet. Absent the usual prohibition against violating rules or social customs, psychopaths are tactically unbound and remarkably uninhibited.

Snakes in Suits

In the workplace, psychopaths are noteworthy for their central roles in frequent, enduring, and bitter conflicts. Psychopaths exert themselves to charm select superiors, whereas their immediate peers experience their abuse and quickly come to view them with mistrust. Peers see them as possessors of a guilt-free lack of integrity, as remorseless pursuers of their own agendas, and as ruthless eliminators of threatening critics or obstacles—even legitimate competitors. Subordinates of psychopaths most often fear them. A great deal of resolve and courage are required to publicly take on psychopaths because of their ruthlessness, manipulative acumen, and the thrill and excitement they experience from generating stress and conflict.

Those in the bureaucracy responsible for oversight or disciplinary functions—such as security or finance officers—will frequently be the first targets of psychopathic manipulations. These institutional watchdogs or disciplinarians are often in positions to collect hard data against the psychopath, such as fraudulent accountings or inaccurate time-and-attendance records. Therefore, they present an especially acute threat to a psychopath's freedom to maneuver undetected within a bureaucracy. They often are subjected to vicious attacks instigated by the psychopath, which may take personal rather than professional form. These preemptive strikes serve to obstruct or obscure legitimate efforts to bring to light concerns about the psychopath's integrity and behavior. In addition, if a psychopath's immediate supervisor, peers, or subordinates try to feed their concerns upward to management, they often find that the psychopath has been there before them and had prepared key managers to expect such criticism. The warnings, therefore, fall on deaf ears or result in blowback to the messengers.

Because psychopaths thrive in an atmosphere of turbulence and instability, corporate cultures that tolerate risk taking and controversial or even abusive behaviors will provide congenial ground for them. Organizations in which the usual institutional systems of control or supervision are

a. The psychological literature on psychopathy and its cousin, antisocial personality, is voluminous. Classics include: Hervey Cleckley, *Mask of Sanity: An Attempt to Reinterpret the So-Called Psychopathic Personality* (Originally published in 1941, it is now in a fifth edition with a slightly different subtitle, "An Attempt to Clarify Some Issues . . ."); Robert Hare, *Without Conscience: The Disturbing World of the Psychopaths Among Us* (Guilford Press, 1993); Paul Babiak and Robert Hare, *Snakes in Suits: When Psychopaths Go to Work* (HarperBusiness, 2007); M.J. Vitacco, "Psychopathy," *The British Journal of Psychiatry* 191 (2007): 357; R. Hare and C. S. Neumann, "Psychopathy as a Clinical and Empirical Construct," *Annual Review of Clinical Psychology* 4 (2008): 217–46.

The John Walker Spy Ring: Keeping it in the Family

John A. Walker joined the Navy in 1955. He developed into an experienced and competent communications specialist, received numerous awards and promotions, and retired as a chief warrant officer after 20 years in the service. At the time of his retirement, he had been spying for the Soviet Union for a decade. Before leaving the Navy, Walker recruited three subagents with active clearances to ensure that his espionage could continue and that he would retain personal control over the feed mechanisms to his handlers.

Walker recruited his friend Jerry Whitworth, a Naval communications specialist who, like Walker, had a "top secret crypto" clearance. Walker and Whitworth agreed to a "50/50 split" of the proceeds, with Walker functioning as the middleman. After retirement. Walker also recruited his brother, Arthur, a retired Navy lieutenant commander, who was working for a defense contractor. He also signed up his 20-year-old son, Michael, who had enlisted in the Navy. Walker used greed to induce his brother and son to spy, though during post-arrest debriefings Michael said his primary motive had been a desire to be like his father.

Walker's daughter enlisted in the Army in 1978. He offered her "a great deal of money" if she would seek a position in Army communications, giving her $100 and promising that this was only the beginning should she cooperate. She steadfastly refused, but he continued to contact her periodically to ask if she had given it further thought. After his daughter left the Army, Walker appeared at her residence accompanied by Whitworth and Whitworth's wife and again tried to recruit her, telling her that his "man in Europe" was willing to provide her with special equipment to spy but was worried that she was getting "too old" to reenlist. She rebuffed him again, but Walker later sent her $500, characterizing the money as an advance from his "man in Europe."

Walker and his subagents were arrested in 1985 after his ex-wife called the FBI after he had stopped support payments to her. She was stunned when her tip-off also resulted in the arrest of her son and said afterward that she would never have called the FBI had she known that Walker had recruited their son. Walker's daughter called the FBI separately in an attempt to regain custody of her only child, which she had surrendered during divorce proceedings from her husband, who had threatened to reveal her father's espionage to the FBI if she fought for custody.

During the debriefings after his arrest, Walker characterized his spying as an exciting game and adventure that was also "quite profitable." Asked if, in hindsight, he would have done things differently, he joked that he should have killed his alcoholic ex-wife, and he maintained that he was caught only because he lost his capacity to pay for "the drunk's" silence. Walker's exploitative and callous attitude and inability to appreciate his role in damaging the lives of others are characteristic of psychopaths.

Walker died in prison in August 2014. His son was paroled in 2000 after serving 15 years of a 25 year sentence.

weak—such as those with inadequate personnel measurement and tracking systems or with vulnerable information systems— will be particularly unprotected against psychopathic manipulations.

The Intelligence Community has both more protection from and more vulnerability to deliberate manipulation by insiders. The institutional safeguards are greater than in most workplaces because of rigorous medical and security screenings of applicants, regular security reviews of the workforce, and programs for medical and lifestyle support for troubled employees. These unique institutional controls are essential because the Intelligence Community's compartmentation of information, secrecy regarding programs and activities, and constant mobility of personnel make it relatively easy for unscrupulous employees to maneuver undetected and to manipulate the system. In the national security environment, such behaviors have the potential to do especially grave harm.

Narcissism

I have had much opportunity to reflect on what happened . . . Greed did not motivate me. It never did. If it had, I would have taken the actions I did far sooner. There were many chances to pursue greed through sustained contacts with Russians and others in [various locations] *. . . but I didn't. This is not meant to be an excuse, just a reflection. Patriotism, Loyalty, Honor—all these had once been of paramount importance to me. They all took a back seat when*

my true loves were threatened— my children and my future.

—CIA spy Jim Nicholson[a]

Yes, and there were Kapos, too, during the concentration camps.

—Navy civilian analyst Jay Pollard[b]

Convinced of their own inherent superiority, narcissists blame others for their problems or for negative things that happen to them.

Narcissistic personalities are characterized by exaggerated self-love and self-centeredness. Alongside an all-encompassing grandiosity runs a subtle but equally pervasive insecurity, into which narcissists have limited insight. Their internal world typically is built around fantasies about their remarkable personal abilities, charisma, beauty, and prospects. They are compelled to exhibit their presumed stellar attributes and constantly seek affirmation from others. Though their imaginings distort common sense or everyday reality, narcissists nevertheless believe in the accuracy of their daydreams and act accordingly. Others, therefore, often experience them as lacking common sense and twisting reality. When facts or other people contradict or interfere with their fantasies, narcissists become combative and vengeful. Their defensive hostility to criticism— even mild feedback—is often well out of proportion to whatever provocation sparked it.

Narcissists possess a careless disregard for personal integrity and can be very unscrupulous and manipulative in pursuing their own ends. They are, on the whole, indifferent to the needs of others, who in turn see them as having flawed social consciences. Narcissists feel entitled to special— even extraordinary— favors and status that they do not believe they have to reciprocate. They heedlessly exploit others emotionally and financially, or in other ways that suit their ends. They are deeply antagonistic to sharing decisionmaking with others, irrespective of the legitimacy of the claims of others for some degree of control. Convinced of their own inherent superiority, they blame others for their problems or for negative things that happen to them, including social rejection. Because they do not consider themselves at fault for any troubles or setbacks, narcissists feel at liberty to take whatever steps they deem necessary to redress wrongs or regain a sense of mastery and superiority.

Narcissistic self-absorption should not be confused with an inability to grasp the perspective of others. Their hunger for affirmation produces acute awareness of the reactions they are provoking from the people around them. This deep hunger for affirmation also makes them vulnerable to manipulation, particularly by people whose admiration or approval they desire. Narcissists are particularly sensitive to authorities or to otherwise socially prominent or powerful people. Conversely, they can be inordinately indifferent to or contemptuous of the feelings or needs of people whom they believe to be insignificant or social inferiors.

Narcissists in the Workplace

Narcissists are often magnetic because their supreme self-confidence wedded to their urgent drive to impress enables them to project the appearance of talent and charm effectively. Over time, the charisma wears thin as it becomes evident that this appearance is not built on substance, but rather on fantasies and fabrications. Furthermore, narcissists' pervasive tendency to see others as inferior causes them to be needlessly sarcastic, belittling, or supercilious.

a. Harold James Nicholson, in a letter written from prison addressed to a senior Intelligence Community official. A career CIA case officer, Nicholson was arrested in 1996 for spying for the Russians, to whom he had volunteered in 1994 when he was completing a tour of duty as the second-in-command of a post in Asia. In addition to passing a wide range of intelligence documents, Nicholson compromised the identities of numerous CIA colleagues working under cover, including the identities of many newly hired students destined for their first posts. (He had been one of their trainers as a senior faculty member at a CIA training center.) He pleaded guilty and was sentenced to 23 years and 7 months imprisonment. While serving his sentence, he induced his youngest son, Nathan, then 22, to contact and collect over $47,000 from Russian officials, which the elder Nicholson called a "pension." FBI agents were tracking Nathan and arrested him in 2008; his father then pleaded guilty to charges of conspiracy to act as an agent of a foreign government and conspiracy to commit money laundering. Eight years were added to his sentence, which he is now serving in a federal "supermax" penitentiary. His son cooperated with the investigation and was sentenced to five years probation (see "Twice Convicted ex-CIA spy gets 8 more years," *USA Today,* 18 January 2011).

b. This comment reflects Pollard's indictment of Jewish-American officials, including a federal judge, involved in his prosecution, trial, and life sentence for spying for Israel. In "60 Minutes: The Pollards," an interview with Mike Wallace, CBS, 20 November 1988. (See case study on page 26.)

Jonathan Jay Pollard: Self-Appointed Hero

Jonathan Pollard, a civilian analyst with the Navy, spied for Israel from June 1984 until his arrest on 21 November 1985. Pollard was highly responsive to Israeli tasking and compromised numerous intelligence documents from CIA, NSA, DIA, and the US military. He has consistently characterized his espionage as the duty of a loyal Israeli soldier and claimed he was a martyr, comparing his life of incarceration to that of an Israeli pilot abandoned after being shot down in enemy territory.

Pollard's pre-espionage history showed a pattern of self-aggrandizement and lapses in judgment. As an undergraduate at Stanford University, he bragged to fellow students that he was a Mossad agent, claiming that Israel was paying his tuition and that he had fought and been wounded in the 1973 Yom Kippur War. In one memorable episode, he brandished a pistol in front of startled fellow students, loudly proclaiming that he needed to carry it for protection because of his intelligence activities. A former college roommate described Pollard as having a penchant for "dirty jokes" and being so immersed in fantasy war games on campus that he was nicknamed "Colonel" (of the Mossad).[a]

Pollard's conduct and attitude problems continued after he secured an analytic job with the Navy. One Monday, he arrived disheveled and unshaven for an interview for a new position, claiming that the Irish Republican Army had kidnapped his then-fiancée and he had spent the weekend securing her release. This incident went unreported, although he did not get the job.[b] In a 1980 effort to join the Navy's HUMINT intelligence element, Pollard made fictitious claims to have completed an M.A., to be proficient in Afrikaans, and to have applied for a commission in the naval reserve. Even more far-fetched, he told his immediate supervisor that he had valuable South African contacts because his father had been a CIA chief of station in South Africa. (Pollard's father was a microbiologist on the faculty of Notre Dame University.) Based on these fabrications. Pollard secured the assignment. Once on the job, his falsehoods became apparent and his erratic behavior raised further alarms. He showed up at meetings against orders, claiming he was entitled to attend, and he disclosed classified information without authorization to a South African defense attaché, perhaps in an attempt to sustain his lies about his valuable liaison contacts.

In a letter from jail in 1989 designed to raise political support for an Israeli-fostered campaign to gain his release from his life sentence, Pollard wrote, "I do not believe that the Draconian sentence meted out to me was in any way commensurate with the crime I committed. As I have tried to point out on innumerable occasions, I was neither accused of nor charged with having intended to harm this country, as I could have been under the provisions of the espionage statute. In other words, I did not spy 'against' the United States. Nowhere in my indictment . . . was I ever described as a 'traitor,' which is hardly a surprise given the fact that the operation with which I was associated actually served to strengthen America's long-term security interests in the Middle East." Pollard's lack of insight into his failures in judgment and ethics and his recasting of events to conform to his grandiose fantasies and self-image are consistent with narcissistic personalities.[c]

---

a. Wolf Blitzer, *Territory of Lies: The Rise, Fall and Betrayal of Jonathan Jay Pollard* (Harper Paperbacks, 1990), 36.

b. Seymour M. Hersh, "The Traitor," *New Yorker*, 18 January 1999: 27.

c. In a 15 May 1998 interview with the Associated Press, Pollard expressed regret. "There is nothing good that came as a result of my actions," he conceded "I tried to serve two countries at the same time. . . . That does not work. . . . People could identify with my predicament . . . because they knew they could be in my place through love of state. . . . There can be no justification for violating the trust given an intelligence officer. I made a mistake." In November 2015 Pollard was released on parole after serving 30 years of his life sentence.

People around narcissists may note stark contrasts in their conduct toward different classes of people, depending on their social rank and usefulness. Furthermore, the hostile and vindictive attacks narcissists mete out when others challenge their grandiosity tend to provoke angry responses in return. The result is that narcissists frequently find themselves the recipients of antagonistic feelings at distinct odds with their view of themselves as infinitely superior and admirable. They have limited insight into their role in these dynamics and tend to blame others for their own lack of social success, in the workplace as elsewhere. Their managers will frequently have to intervene in the interpersonal conflicts they habitually generate.

In addition, narcissists often show a pattern of violating organizational rules and disregarding institutional or managerial authority. They trivialize inconvenient regulations or hold themselves superior and exempt from policies, directives, and laws. They

feel entitled to favorable workplace treatment— whether this comes in the form of forgiveness for transgressions, early or frequent promotions, attractive work assignments, or other advantages such as having their requests expedited by support staff. They are acutely sensitive to the advancement of others and become suspicious and angry if they find themselves being left behind. They perceive workplace competitors who get ahead of them as "stealing" advantages or rewards that are rightfully their own. Finally, narcissists will lie, fabricate information or events, willfully exaggerate accomplishments, and often believe their own fabrications, all in the interest of appearing successful or important.

Many of these characteristics, properly contained, can be very useful in certain types of work requiring flexibility, charisma, and persuasion—for example, in sales, politics, and case officer work. It can be very difficult for managers to know where to draw the line between a tolerable or useful level of narcissism—what psychologists call healthy narcissism—and more dangerous self-absorption and self-aggrandizement. One way to make this determination is to look for positive, counterbalancing features in the personality—such as tolerance of competition and a realistic self-perception—that control and channel the narcissism into productive pursuits.

Immaturity

My thinking before I joined the CIA was, I think, noble and patriotic and all this, help the United States or whatever. And even when this happened, I didn't feel anti-American or anti-CIA. It never came to me that this was a—a real damaging thing that I had done. I thought that more good really could come out of it. That's the reason that I returned to the CIA, contacting them and obviously, you know, the whole thing was backwards and I'm not sure if—even if—I'll ever really know how it happened. It's—when I think back about it—it—it almost seems impossible that it could have happened but it did and I hope maybe it, you know, clears up.

—Former CIA watch officer William Kampiles[a]

No one is born a spy. Spies are made. Some are volunteers, many are coerced, but all begin somewhere on the other side from where they inevitably end up. . . . My age at the time of entry into the world of espionage was nineteen. I was one of the youngest spies ever in the history of the United States. . . . This story is not only one of manipulation. Like all spy stories, it is also one of betrayal. . . . I betrayed and was betrayed. Today, years after my release, years after my kidnapping and trial, I am confronted by this reality on a near daily basis.

—Enlisted Air Force linguist Jeffrey Carney[b]

It can be very difficult for managers to know where to draw the line between a tolerable or useful level of narcissism and more dangerous self-absorption and self-aggrandizement.

Observers frequently compare immature adults to adolescents. Attitudes and behaviors that are expected and even endearing in normal adolescents or children, however, are unsettling, disruptive, and potentially hazardous in adults.

The most salient characteristic of immaturity is the ascendancy of fantasy over reality. Immature adults spend an inordinate amount of time daydreaming, deliberately calling to mind ideas that stimulate pleasant or exciting emotions. In contrast to mature adults, immature adults do not readily distinguish their private world from objective external reality and, in fact, may expect reality to conform to their self-serving and stimulating fantasies. Their fantasies about their special powers, talents, status, prospects, and future actions can be so seductive that they become resentful of conflicting real-world truth.

All three types of personalities described in this article are distinguished by active fantasy lives, but the fantasies tend to differ in both

a. See case study on page 28.

b. These quotations are from the opening chapter of Jeffery M. Carney's self-published memoir (*Against All Enemies: An American's Cold War Journey* [CreateSpace, 2013], 11–12). Carney was a mole for the East Germans while he was a US Air Force linguist. After he was exfiltrated to East Germany, he developed detailed targeting files on Americans for them. (See case study on page 32.) The kidnapping Carney refers to in this quote is his arrest after German reunification in 1990, when a tip from his former East German handler led officers from the US Air Force Office of Special Investigations to seize him in Germany and return him to the United States for trial. (See case study on page 32.)

William Kampiles: Self-Styled Special Agent

In March 1978, after resigning under duress from his position as a watch officer in the CIA Operations Center, William Kampiles passed to the Soviet Union a top secret KH-11 satellite technical manual. He received $3,000 for this document that contained detailed information on a major US intelligence collection system.

Kampiles had joined the CIA in 1977 at age 22. He was offered a watch officer position when his application for Directorate of Operations (DO) case officer training was rejected. He arrived at work with distorted notions of his abilities and prospects and quickly became disgruntled. Uninterested and contemptuous of his assigned duties, he clashed with his supervisor, and his persistent efforts to transfer to the DO led to a formal notice that he was required to serve in his present position for two years, which only deepened his disgruntlement.

Through personal contacts, Kampiles managed to secure an interview with the DO Career Training Staff. His interviewer described him as immature and lacking self-discipline and judgment. Highlights of their discussion include Kampiles revealing that he had only accepted the watch officer position as a way to secure entry into the DO and that he would resign from the CIA if he were not accepted. He attributed his difficulties in the Operations Center to his reputation as a playboy, and when his interviewer asked if this reputation was deserved, he boasted of his successes with women. Questioned about what he had liked best about a past menial job, he quipped that it was the expense account.

Kampiles smuggled a KH-11 manual out of the Operations Center to try to get his CIA supervisor in trouble when it was found to be missing. He also vaguely envisaged that he could turn around his upcoming termination by using the document to initiate a free-lance, James Bond-style operation, thus persuading the CIA that he was indeed case officer material and could be deployed as a double agent against Moscow. Four months after his resignation, he volunteered the document to the Soviets in Athens, Greece, where he was visiting relatives. Upon his return to the United States, he got in touch with a former CIA colleague and revealed his contact with the Soviets. The colleague asked him to describe his activities in a letter. Kampiles wrote about his "accidental" meeting with a Soviet in Athens and noted that other meetings followed, but he did not directly admit to passing documents. "What I have talked about thus far has been generalized," he explained. "I did this because to be entirely specific it would take the length of a short book to narrate this entire story. If you think there might be agency [i.e., CIA] interest, I might be willing to discuss this experience in full detail."

The letter led to an FBI investigation and Kampiles's arrest for espionage, for which he was sentenced to 40 years in prison. Reflecting on his motives and state of mind at the time that he took the KH-11 manual and later when he passed it to the Soviets, Kampiles told his FBI interrogators, "I think you know, boiling it down, I think it was monetary and the glamour and the excitement, that this sort of thing might bring on . . . the danger . . . the intrigue, all that together." Kampiles's immersion in a fantasy world, his belief that both reality and other people would play along, the profound failures in perception and judgment caused by his fantasies, and his initial shock upon his arrest and eventual remorse at the harm he caused are all consistent with immaturity.

content and degree. Psychopaths tend to fantasize mostly about power, pain, and control, while narcissists focus on their personal superiority and the hostility provoked by those who do not notice it and their plans to get revenge for perceived slights and insults. The fantasy lives of immature persons are frequently much less well defined; they can be likened to the dreamlike blend of perceptions, thoughts, imagination, and facts characteristic of psychologically healthy children. Because the reasoning, judgment, and self-control of immature adults are underdeveloped, such individuals are less tied to factual reality than their mature peers and more dependent on fantasy to cope with events and to maintain stability.

Consequently, immature adults generally expect others to embrace what to them is the self-evident legitimacy of their personal ideas and longings. They often cannot understand why others do not share their perspective and fail to see that reality itself works against the validity of their fantasies. They frequently will act on their fantasies with little anticipation of consequences that to most people would be completely predictable. They are often genuinely shocked when reality intrudes on their plans and interferes with anticipated outcomes.

Furthermore, immature people are persistently egocentric, they see themselves as the epicenter of any crowd or event. They believe others are paying close attention to them personally in most contexts, and as a result they are acutely self-aware. When it becomes clear that they are not the center of attention and that

others might, in fact, be indifferent to them, they often react negatively and take steps to bring attention to themselves.

Immature people have difficulty moderating their feelings. Rather than appropriately disciplining and channeling feelings, they are subject to them. As a result, they are given to dramatic displays of emotion when stressed or excited, and while these displays may be congruent to whatever stimulated the feelings—for example, they will become very angry at perceived injustices or delight in successes—observers will sense that the emotions lack proper proportion and moderation.

A significant consequence of poor emotional control is impulsivity. Immature people have difficulty restraining their immediate wishes in the interest of anticipating long-term consequences. When prompted by sudden feelings or urgent desires, they take precipitous action. They tend to have limited attention spans and need to be emotionally engaged with a task or a person to retain focus. They can be quite fickle and easily distracted.

Finally, like psychopaths and narcissists, immature adults have defective consciences, but they are capable of feeling real guilt and often have well-developed moral codes. Their egocentricism and impulsivity limit their capacity for foresight, but in hindsight they often deeply regret their impetuous actions. Though they may want to behave ethically and feel guilt and shame when they behave badly or hurt other people, their capacity to apply their moral understanding and desires consistently to control their behavior is compromised.

Like psychopaths and narcissists, immature persons have defective consciences, but they are capable of feeling real guilt and often have well-developed moral codes.

An occasional feature of immaturity is dependency, which is highly relevant to espionage because dependency makes a person particularly susceptible to manipulation and control. (See Sharon Scranage case study on page 34.) Dependent people experience relationships to be so crucial to their well-being that they will do almost anything to sustain them. Dependent people may function quite adequately and seem well adjusted as long as they are not required to be on their own and are able to rely on a relationship as a psychological crutch. If the relationship is threatened, or there is even the possibility of separation, they become anxious and less able to cope. Their hunger to both please and cling to the person or people on whom they are dependent necessarily affects their judgment, and they will willingly compromise their own and others' well-being—including their personal ethics— to sustain the relationship on which they depend.

Children at Play

In the workplace, immature people are often spontaneous and imaginative and can be quite appealing. In optimal conditions, they can be productive and inventive people who are eager to form attachments with others and to please and impress them.

When such employees are stressed, however, these characteristics can take distinctly negative turns. Spontaneity can translate into erratic and impulsive behavior, and active imaginations can cause problems with decisionmaking and judgment. If stress is not reduced, immature workers rapidly lose their ability to cope and can become inordinately needy and demanding. Coworkers who discern these patterns become alarmed, and immature people are often considered by others to be somewhat unbalanced and a risk for hazardous behavior and bad judgment.

In general, immature persons are naive about normal expectations regarding adult workplace attitudes and conduct. They are too susceptible to environmental distractions and internal pressures to be consistent performers. They do not readily distinguish between personal and professional spheres. They are easily bored with routine and heedlessly seek stimulation from people and things around them. They can be either too dependent on, or reactive against, control mechanisms. They tend to be very demanding of positive attention from authorities, while at the same time overly hostile or sensitive to negative feedback. Their seeking after attention or stimulation often becomes a drain on supervisors, who must engage in constant oversight, and can deplete peers, who get pressed into fixing problems caused by their immature colleague's inattention and poor judgment.

Robert Hanssen: Self-Designated Cold Warrior

Former FBI Special Agent Robert Hanssen spied for the Russians for a total of nine years over a 21-year period, beginning in 1979 and ending with his arrest in 2001. Because of his position in the FBI Foreign Counterintelligence Unit and his use of computer technologies, Hanssen was able to pass extensive and highly damaging information.

After his arrest, Hanssen reported that as a junior special agent working in the FBI's New York office, he was inspired to commit espionage by reading operational files of past and then current Russian agents. While fascinated by the clandestine and secret world described in the files, he was also struck by what he estimated to be amateurish tradecraft and was curious to see if he could do better. He initiated his espionage by leaving a letter signed with a code name for a Russian case officer whose tradecraft he admired. In this, as in all communications with his handlers, Hanssen insisted on remaining unidentified.

His anonymous letters to his handlers provide a window into his psyche. The tone varies from arrogant lecturing to pleading for understanding and communication. He often addressed his handlers with a mixture of superciliousness and admonition, as in the following excerpt from an 8 June 2000 letter in which he describes how they should view the United States: "The US can be errantly [sic] likened to a powerfully built but retarded child, potentially dangerous, but young, immature, and easily manipulated. But don't be fooled by that appearance. It is also one which can turn ingenius [sic] quickly, like an idiot savant, once convinced of a goal."

Hanssen was motivated to spy by a mixture of greed, need for excitement, desire to test himself, and craving to feel like a "hero" by becoming involved in something significant. To external appearances, there were many signs of stability in his lifestyle. The Hanssen family was religiously devout with extensive ties in their faith community. Hanssen appeared to be a responsible primary breadwinner. He was a moderately successful FBI special agent who, while not necessarily fitting the typical mold, had secured a niche job that suited his talents. Despite these external signs of stability, however, Hanssen possessed salient secret vulnerabilities. His desire to serve as a hero led him to initiate a mentoring relationship with a prostitute he imagined he could rescue from her lifestyle by showing her a better way to live. He abruptly cut off this relationship when she proved unable to live up to his expectations. He installed a live-feed camera in his bedroom and surreptitiously captured his sexual activity with his wife for a male friend, even discussing with this friend ahead of time what he would like to watch. He also passed to him nude pictures of his wife and posted pornographic stories on the web featuring him and his wife, all without her knowledge.

At work, Hanssen was considered odd and carried several pejorative nicknames. He was disciplined for angrily grabbing a female colleague. He exploited a breach in the computer firewall to break into his supervisor's computer, claiming he did it to show FBI security the vulnerability of sensitive computer systems. When he was reprimanded as a young special agent for throwing classified information in the trash rather than shredding it, he responded that he knew what was really classified and what was not. The failures in empathy and in respect for others, the self-absorption, and the poor judgment evident in these behaviors suggest a mixed personality disorder.

Mixed Personality Disorder

> *I feel I had a small role in bringing down the USSR. . . . I wanted to be able to contribute in some way to that. . . . So I launched my own war.*
>
> —FBI mole Robert Hanssen

While the traits and behaviors of many spies match the features specific to psychopathy, narcissism, or immaturity and dependency, in some cases the personalities do not readily fit any one of these types. What may be most notable in such cases is a lack of positive personality features to counterbalance negative ones. In addition, some spies show a mix of characteristics from all three dominant types. Some may also show other psychopathologies such as paranoid or compulsive symptoms. A case in point is former FBI Special Agent Robert Hanssen, who spied for the Russians over the course of 21 years. A psychological evaluation conducted as part of the damage assessment concluded that his personality contains a mix of psychopathic, narcissistic, and dependent features.

Healthy Personalities

In healthy personalities, positive characteristics counterbalance negative ones. Positive features might include the ability to accept criticism; to feel remorse and make reparations for mistakes; to show genuine empathy for at least some people. Healthy personalities also exhibit reasonable stability of mood over time and

in different contexts; experience, express, and contain a wide range of emotions; show tactical adaptability alongside good long-range planning and self-discipline; and demonstrate ethical behavior across various situations.

In contrast to exhibiting a mix of positive features to temper problem characteristics, pathological personalities tend to be structured around a few dominant, relatively uninhibited characteristics. The complexity of healthy personalities enables them to deploy an array of coping strategies depending on the nature of the challenges they have to address. In contrast, pathological personalities possess a limited range of coping techniques. People with personality pathology tend to adhere stubbornly to a few approaches to problem solving and have difficulty adjusting, changing, and growing despite repeated evidence that their strategies for dealing with life are not working adequately.

Precipitating Crises

I'm growing extremely tired of American society, American modern day values, American class consciousness, American TV, American law, American consumerism, American hypocrisy.

—CIA spy Jim Nicholson[a]

What I was thinking? How was I thinking? It was a very busy and stressful period both professionally and personally and it was like a leap in the dark.

a. Nicholson, personal journal entry, 15 July 1985.

While problematic personality features are essential, they are not sufficient to provoke espionage. The majority of people who have some, or even many, of the personality features described above will never engage in criminal conduct.

—CIA mole Rick Ames[b]

I think I was pissed off in the fact that all my expectations on what the job would be like were falling short and I guess I was perhaps bitter about the situation as it was and that may have been part of the motive but I'm not sure because when I look back it's not really all that clear.

—Former CIA watch officer William Kampiles

While problematic personality features are essential, they are not sufficient to provoke espionage. The majority of people who have some, or even many, of the personality features described above will never engage in criminal conduct. Espionage must be triggered by a crisis and the person's assessment that illicit criminal conduct offers the solution to or an escape from the crisis. The precipitating crisis may be self-evident to observers—for example, the breakup of a marriage, the loss of a job, or bankruptcy. But it can also be private and invisible. Such psychological crises as feeling intensely frustrated and humiliated at being consistently outperformed at work by peers can be just as acute and painful as externally evident problems.

CIA officer Jim Nicholson's sense of deep personal humiliation at not having savings in the bank and his frustration at not being able to provide his children with a more affluent and sophisticated lifestyle are examples of how a psychological crisis can lead to espionage. To all external appearances, this GS-15 case officer was progressing well in his career and, while not in a superior financial position, was living a solidly middle-class lifestyle. This view did not match his internal sentiments of frustration and failure, which led him to volunteer to spy for the Russians. He was prompted by the arrest of fellow case officer Rick Ames and his observation that Ames had experienced a long and financially lucrative run of espionage for the same customer. Nicholson believed his tradecraft was better than Ames's and that he would not be caught.

Navy spy Jonathan Pollard also went through a psychological crisis just prior to his espionage—he later described it as a spiritual crisis. In contrast to Nicholson, however. Pollard was experiencing work and financial problems alongside his psychological crisis. In debriefings after his arrest, Pollard said he had resolved to spy for Israel in a state of deep anger and frustration after the US Marine Corps barracks in Beirut was bombed in 1983. He claimed that he "walked out of the memorial service [for the Marines] committed to doing something that would guarantee Israel's security even though it might involve a degree of potential

b. "Ames on the Inside," CNN Interview with Wolf Blitzer and Bob Franken, 27 December 1994.

Jeffrey Carney: The Spy Codenamed "The Kid"

Jeffrey Carney enlisted in the US Air Force on his 17th birthday in 1980 and was granted a top secret clearance a year later. He began spying for East Germany's Ministry of State Security (MfS) in 1983 while working as a linguist at Marienfelde Base in West Berlin. He continued spying at his next post in Texas, from which he abruptly deserted in 1985. The MfS exfiltrated and resettled him in Berlin, where he helped them target Americans. When the Iron Curtain fell, his handlers abandoned him and tipped off US authorities; he was arrested in 1991.

Carney's initial motivation for his walk-in was a sense of betrayal by family, friends, and supervisors. His family background was painful and unstable, including severe physical and emotional abuse and neglect and the frequent disappearance of his father. Carney described himself as having been a lonely child, an "underdog" who felt inferior and had a burning desire to prove his worth. He dropped out of high school to help support his mother financially, including paying for her divorce from his father. When he visited home in 1983 on leave, he was shocked to find his father living there. After an acrimonious visit, he returned to Germany, nursing feelings of bitterness and inadequacy. He was also coming to terms with his homosexuality, which at the time put his military career at risk. In addition, Carney was deeply dissatisfied with the Air Force. Despite salient intellectual gifts, he was unable to sustain an unblemished work record, had been decertified as a language instructor, and had trouble regaining his credentials. He was outraged by his decertification, which he blamed on his supervisors' ill will, and felt humiliated and embarrassed.

On the night of his impulsive attempt to defect to East Germany, all of the acquaintances and friends he approached rejected his overtures to go out. He went alone to some bars, had several drinks, and contemplated suicide. At one bar, he happened to read an article about a Taiwanese pilot who defected to mainland China, was feted as a hero, honored with a parade, and given money. "I'll show them, I'll show them all," was Carney's reaction. Acting on this thought, he took a cab to Checkpoint Charlie, walked across, and presented himself to the East Germans as a defector. They quickly convinced him to go back to his post at Marienfelde as a spy.

After his routine reassignment in 1984 to a domestic post, Carney became preoccupied with the announcement that all employees with access to sensitive compartmented information (SCI) would be polygraphed. He was also furious with Air Force doctors, who refused to operate on what he believed was a hernia. When he threatened to go to the inspector general with his complaint, he was referred for a psychological evaluation and became concerned that drugs would be used to make him say things beyond his control, exposing both his espionage and his homosexuality. He deserted and flew to Mexico City, presenting himself unannounced to the East Germans. Upon his resettlement in East Berlin, the MfS tasked him with transcribing intercepted conversations of US military and embassy personnel, from which he discerned their responsibilities, attitudes, relationships, and personalities. If he felt that particular individuals were vulnerable, he wrote an assessment describing their situation and suggesting the best recruitment approach. Carney claimed that the MfS apparently prized his work.

After his arrest,[a] Carney readily confessed to his espionage and said that it helped him regain a sense of personal pride and purpose. "Each time I took information out," he asserted, "I felt like I was slapping my supervisors in the face." He also expressed bitterness that the US government had violated his German rights by forcibly taking him away from his home, his personal belongings, and his common-law spouse. Carney's impulsive decision to defect in a time of despair, along with the psychological stability and sense of achievement and purpose that he temporarily gained once engaged in espionage, demonstrate the role that stress and crisis can play in motivating a vulnerable person to seek a solution through espionage.

Carney was released in 2002 after serving 11 years of a 38-year sentence. He attempted to return to Germany, claiming German citizenship, but he was denied entry because the East Germans had never granted him citizenship.

---

a. In his memoir Carney quotes himself as asking the OSI officers arresting him "What took you so long?" (*Against All Enemies*, 592); he also claims to have made several attempts during the arrest to assert rights as a German citizen but was told to shut up. FBI Special Agent Robert Hanssen also contemptuously asked the FBI colleagues arresting him, "What took you so long?" Both Hanssen and Carney demonstrated the reflexive grandiosity described in the personality section of this article in this sarcastic comment. When he was arrested, Ames said, "You're making a big mistake! You must have the wrong man!" demonstrating the automatic cunning and slipperiness characteristic of psychopaths.

risk and personal sacrifice."[a] During this same period, Pollard had several heated discussions with his supervisor regarding chronic tardiness, conflicts with coworkers, and inability to complete assignments. Moreover, the Pollards frequently were late paying their rent or their rent checks bounced; the Navy Federal Credit Union reported him delinquent in repaying a loan. He and his wife were witnessed using cocaine and marijuana at parties, and an anonymous call to the Navy's security service reported that Pollard had been involved in an altercation in Georgetown.[b]

Robert Hanssen began spying after an assignment to the FBI's New York Field Office caused such financial strain on his family that, on one occasion, his wife broke into their children's piggy banks to collect enough change to carry the family through until the next paycheck. Air Force spy Jeffrey Carney impulsively defected to East Germany in the course of a night of drinking alone, contemplating suicide, and brooding on his loneliness and ill-usage by family, friends and supervisors.

States of crisis often result in patterns of thinking that degrade judgment and behavior. A person in crisis typically experiences a sense of threat alongside a severe loss of control. The combined result frequently is a feeling of paralysis or helplessness, a desire to either fight the situation

States of crisis often result in patterns of thinking that degrade judgment and behavior.

or to find a way to escape it at all costs. Most significant with respect to motivation for espionage, a person in this state of mind can acquire "tunnel vision," in which the person's attention becomes riveted on the current crisis. This fixation on the present can degrade long-term planning and the capacity to anticipate lasting consequences. Such mental conditions make a person vulnerable to taking badly judged actions.

While life crises are ubiquitous, criminal responses remain rare. Personality flaws that weaken moral reasoning, judgment, and control over impulsive behavior are aggravated by the sense of immediate threat, urgent need to escape, and tunnel vision common to crises. A person with personality problems is therefore doubly vulnerable to misjudgments and misconduct in a crisis. Conversely, people who as a rule have strong judgment, good self-control, and healthy consciences have more insulation against tendencies to impulsive action or misconduct when under the pressures of crisis.

Special Handling

Journalist: *Why did you make the decision to work for the other side?*

Spy: *Some of that started in the 70's in New York* [before volunteering to spy for the Russians in the 1980's]

Journalist: *Why?*

Spy: *As you know, I knew some Soviets in New York who were very interesting. The chief* Pravda *representative in New York and I had lunch together every couple of weeks for about three years. And he didn't directly teach me a lot, but indirectly I learned an awful lot . . . in terms of what the Soviets are all about.*

Journalist: *How would you arrange to contact the other side* [KGB] *and meet?*

Spy: *Through a go-between, a Soviet Embassy officer, who's not a KGB officer. We had an overt relationship–I was assessing the guy* [for CIA] *to see if he'd be of value as a target and did develop him a little bit–so this* [meeting with a Soviet] *is all approved* [by the CIA][c]

—CIA mole Rick Ames

"You need to show us that you are serious." His voice had mellowed. "You can be a soldier on the Invisible Front. What good are you here? [in East Germany]*" he asked rhetorically. "Here, you are one person with perhaps a little ability to make a difference. There* [as a mole inside the US Air Force]*, working for peace – and you don't even have to be Communist or Socialist – you can make a great difference! You will have earned your right to come and stay here." . . . There are those who say I was brainwashed, but that is not true. While it is true that I originally lacked the conviction I claimed that fateful April morning, I would soon need little prodding to betray my former colleagues* [in the US military]*. . . . In my naiveté I also was*

a. Director of Central Intelligence, Foreign Denial and Deception Analysis Committee, *The Jonathan Jay Pollard Espionage Case: A Damage Assessment,* 30 October 1987 (MORI DocID: 1346933). Available at https://www.archives.gov/files/declassification/iscap/pdf/2007-010-doc1.pdf.

b. Ibid.

c. "Why I Spied: Aldrich Ames," *New York Times* interview with Tim Weiner, 31 July 1994.

The "Handling" of Sharon Scranage

Sharon Scranage compromised CIA staff officers, agents, and operations while serving as a secretary and administrator in Africa from 1983 to 1985. Her spying necessitated the exfiltration and resettlement of numerous African agents and their families. The total cost of her espionage has been estimated to be several million dollars.

Scranage joined the CIA in 1976 as a clerk-stenographer. She consistently received favorable performance reports, including appreciative comments about her pleasant and dedicated workplace demeanor. Her private life was less settled, however. She divorced her husband of two years in 1980, after he had become physically and psychologically abusive, including hitting her and threatening her with a gun.

Only two days after Scranage's arrival at her post in Africa in 1983, a State Department communicator introduced her to the man who subsequently became her handler. He quickly drew her into a sexual affair and—apparently working from an accurate assessment of Scranage's susceptibility to psychological abuse—began to use a combination of affection and fear to increase his power over her and to elicit more and more sensitive information from her. In addition to establishing a sexual relationship with her and thus asserting physical control, Scranage's handler also used verbal intimidation and threats to deter her from revealing what she had done to station personnel and to isolate her socially from sources of support in the station and community. He systematically assaulted her trust in CIA and her most senior manager, arguing that this manager had put her in her present position. Her handler also fed her dread of being discovered and made veiled threats to harm those agency personnel and their family members with whom she appeared close. By such means, Scranage's handler positioned himself as her preeminent authority figure and protector rather than the CIA and her managers and colleagues. In hindsight, she described herself as "a puppet" in his hands. After her arrest, Scranage consistently expressed profound remorse for her espionage.

unable to sense my true value to the MfS in those early days, and it would be many years later before I understood the damage I had caused the United States

—Air Force spy Jeffrey Carney, describing his recruitment[a]

I have come about as close as I ever want to come to sacrificing myself to help you, and I get silence. I hate silence. . . . It's been a long time dear friends, a long and lonely time. . . . Perhaps you occasionally give up on me. Giving up on me is a mistake. I have proven inveterately loyal and willing to take grave risks, which even could cause my death, only remaining quiet in times of extreme uncertainty. So far my ship has successfully navigated the slings and arrows of outrageous fortune. I ask you to help me survive.

—FBI mole Robert Hanssen, in letters to his handlers[b]

a. Carney, *Against All Enemies*, 155–56.

b. Excerpts from Hanssen's letters to his Russian handlers, dated 15 July 1988, 14 March 2000, and 17 November 2000.

Exploitation of the Vulnerable

A well-trained espionage recruiter will search for vulnerable targets. Professional intelligence officers are trained to spot outward signs of trouble in a person's history or behavior—such as tumultuous relationships or frequent job changes—and to evaluate the deeper, more enduring psychological dysfunctions that may be at the root of the problems. These professional recruiters are trained to deploy sophisticated psychological control techniques matched to the vulnerabilities they have detected in order to manipulate, apply pressure, or induce a person to commit espionage.

Some intelligence services do not limit themselves to exploiting preexisting problems, but may actively foster crises to enhance the target's susceptibility to recruitment. Common forms of such aggressive pursuit and manipulation of targets include emotional or sexual entrapment and financial manipulation through increasing the target's level of debt. A psychologically vulnerable target's grandiosity, sense of being above the rules, or vengeful impulses can all be manipulated in the service of recruitment.

The role of such manipulations by a potential customer and the prospective spy's own sense of the ease and safety of espionage are often underestimated as key factors in increasing or decreasing motivation. Adept professional handlers depict themselves not only as willing to reward espionage but also as capable of safeguarding their agent. Good professional "handling" is designed not only to collect classified information but also to stabilize and reassure the spy in the interest of sustaining his or her

capacity to commit espionage for as long as possible. As a result, the relationship between an agent and a handler is frequently highly personal, intense, and emotional, at least from the perspective of the spy, and the nature of this relationship is often a powerful force behind an individual's choice to spy.

Remedies and Risk Management

How people who have the potential to spy gain clearances and secure entry into the Intelligence Community, how they progress and function once inside, and how the risk they pose might be mitigated are questions of critical interest to security and counterintelligence personnel as well as to medical and management professionals. The risk of spying can be mitigated through programs designed to spot and address warning signs at each stage of an employee's career and by providing support services to troubled employees once they have been identified or by disciplining them appropriately.

The entry points into an organization can be safeguarded through rigorous security and psychological evaluations of applicants designed to spot and weed out chronically dysfunctional people unsuitable for clearances. Patterns of personality deficiencies that can result in trouble both at work and in personal lives not only attract the attention of trained observers of human behavior—such as psychologists and case officers—but also can be registered by more incidental observers, such as coworkers and neighbors. For this reason, background checks in the security clearances process are designed to tap into this informal reservoir of observations to identify maladaptive patterns that would put an intelligence organization at risk.

While such medical and security screenings of applicants are the first line of defense, ongoing security reviews of the employee population are the second line, with the intent of detecting personnel who demonstrate patterns of troubling attitudes or behaviors and intervening before serious misconduct occurs. The typology of psychological factors in espionage presented here has been helpful in organizing observations regarding the personalities, behaviors, and life circumstances of captured spies, with an eye to developing countermeasures and risk-mitigation strategies applicable to the workplace.

Routine security and counterintelligence reviews of applicants and staff should not be the only lines of defense, however, because while such reviews can pinpoint problems they do not necessarily ameliorate or fix them. Programs of education and support for the cleared workforce must supplement the safeguards provided by regular reviews. Educational programs regarding danger signs can assist employees and managers in spotting emotional or behavioral problems in colleagues or subordinates, or even occasionally in themselves, before they evolve into serious counterintelligence or security problems.

Effective follow-through once problems have been spotted is imperative in the form of active and well-staffed medical support for troubled employees. It is especially important to make such services available to employees who identify their own problems and come forward to seek support voluntarily.

Finally, case studies of apprehended spies have demonstrated that some

The Anger of Edward Lee Howard

Howard was dismissed from the CIA in 1983 after a polygraph exam indicated he was involved in petty theft and drug use. In the months after his dismissal, he moved to New Mexico with his wife, Mary. His alcohol abuse escalated, and he became increasingly angry at what he perceived to be the agency's unfair treatment. Howard claimed he provided information to the Russian KGB and eventually defected to Russia when he became aware of US surveillance of his activities, while believing he was unfairly targetted and accused. A book about Howard by David Wise and Howard's own memoir, though filled with significant errors of fact, provide good examples of how a vulnerable person's sense of disgruntlement and perceived ill-usage can provide the impetus to turn to espionage and the flawed, but compelling, justification for doing so.[a] Readers will notice similar strands of acrimony and disgruntlement in the Carney, Pollard, and Hanssen cases.

Howard's death in Russia was reported on 22 July 2002. He supposedly broke his neck in a fall at his dacha, but the exact circumstances have never been made public.

a. David Wise, *The Spy Who Got Away: The Inside Story of the CIA Agent Who Betrayed His Country's Secrets and Escaped to Moscow (Random House,* 1988) and Edward Lee Howard, *Safe House: The Compelling Memoirs of the Only CIA Spy to Seek Asylum in Russia* (National Press Books, 1995).

began their espionage in a state of crisis marked by intense anger and frustration, and sometimes by financial desperation, after being fired or in anticipation of termination. (See textbox on Edward Lee Howard on preceding page.)

Prudent risk mitigation in cases of termination or forced resignation should include, when possible, safeguarding the dignity of the person to inhibit feelings of vengefulness and disgruntlement and, on a pragmatic level, making efforts to provide for job placement programs and psychological and financial counseling services to assist the person in establishing a stable lifestyle outside of the Intelligence Community.

The Intelligence Community recoils every time a spy is caught. Laws have been broken, national security has been breached, and the bond among patriotic professionals has been violated. It would be consoling if the capture of major spies in recent years and the end of the Cold War signaled a downward trend in espionage. But the impetus to spy grows out of the human psyche, and personality dysfunctions, personal crises, and opportunities to serve other masters will never vanish. Understanding the elements of espionage is critical to remaining vigilant and safeguarding the vital mission of US intelligence.

❖ ❖ ❖