Intelligence in the Twitter Age
Joshua Rovner
Published online: 21 Feb 2013.

To cite this article: Joshua Rovner (2013): Intelligence in the Twitter Age, International Journal of Intelligence and CounterIntelligence, 26:2, 260-271
To link to this article:  http://dx.doi.org/10.1080/08850607.2013.757996
Intelligence may have a bright future. Advances in imagery and signals processing technology mean that intelligence agencies can deliver remarkably accurate and timely intelligence to civilian officials and military commanders. However much leaders gripe about intelligence, few are likely to disregard such fine-grained information about threats and opportunities, especially when national security is on the line. Others contend that intelligence is central to the kind of wars that the United States is likely to fight in the foreseeable future. Counterterrorism, for example, depends on intelligence agencies to provide detailed descriptions of terrorist organizations, warning of impending attacks, and precise targeting information for offensive actions. U.S. counterterrorism operations will persist long after the country draws down from Afghanistan, because of the geographic expansion of groups associated with al-Qaeda, and because of the growing enthusiasm for special operations forces (SOF) and unmanned aerial vehicle (UAV) strikes against them.¹ Most importantly, policymakers have invested lavishly in intelligence for over a decade. President George W. Bush called for a large increase in the intelligence personnel in the wake of the 11 September 2001 (9/11) attacks on New York City and Washington, DC. Later, Congress created the Office of the Director of National Intelligence (ODNI), adding a new layer of bureaucracy above an already sprawling constellation of

Dr. Joshua Rovner is Associate Professor of Strategy and Policy at the U.S. Naval War College. He is the author of Fixing the Facts: National Security and the Politics of Intelligence (Ithaca, NY: Cornell University Press, 2011), which won the International Studies Association book award for security studies. The views here are his alone and do not necessarily represent those of the Naval War College, the U.S. Navy, or the Department of Defense.
agencies. And, despite a great deal of criticism, the budget for intelligence has more than doubled since 9/11 and continues to rise.2

But certain signs indicate that intelligence may nevertheless play a smaller role in strategy and policy. The political upheaval in North Africa and the Middle East in 2011–2012 was facilitated by new social networking sites like Twitter and Facebook. These platforms enabled political activists to rapidly mobilize protesters, who could then provide real-time reports via their own social network accounts. The result was a staggering burst of information from thousands of new sources, all offering their own perspectives on complex and changing events. According to some news reports, the U.S. Intelligence Community struggled to make sense of this flood of information, and its apparent failure to do so raised questions about its ability to provide policymakers anything useful beyond what the new media provide.

Intelligence agencies also face new challenges from an expanding number of think tanks and private sector analysis firms. These outfits often portray themselves as quasi-intelligence organizations, and some actively recruit government analysts to bolster their credentials. While social media have created an explosion in new sources of information, the rise of private sector intelligence has intensified competition for policymakers’ attention. Both issues raise important questions about whether and how traditional intelligence agencies can remain relevant to policymakers and contribute something useful to the policy process.

HOW LEADERS USE AND MISUSE INTELLIGENCE

In theory, intelligence agencies and policymakers need each other. Intelligence needs policy attention or else its work will be irrelevant. Even the best intelligence products are ultimately worthless if they do not find a receptive audience. Intelligence also requires close and continuing policy guidance so that it can tailor its products to suit policymaker needs. Routine interaction is needed to ensure that intelligence is providing timely answers to important questions; the Intelligence Community exists to serve policy, not to provide knowledge for its own sake.

Policymakers also need intelligence. International politics are characterized by ambiguous information open to a range of possible interpretations. Intelligence can help reduce the bounds of uncertainty by adding secret information to open sources, and by distilling it all into digestible estimates. As Columbia University’s Richard Betts put it, “The intelligence community is the logical set of institutions to provide what one may call the library function for national security: it keeps track of all sources, secret or not, and mobilizes them in coherent form whenever nonexpert policymakers call for them.”3
Ideal intelligence-policy relations are characterized by candor. In a perfect world, intelligence analysts and officials would produce objective estimates on important issues without concern for policy preferences, and deliver bad news without fear of recrimination. Policymakers would be active consumers in this world, criticizing sloppy or unhelpful intelligence products and demanding better work without being accused of bullying. In sum, intelligence and policy would routinely challenge each other in the best sense of the word.

But healthy tension is hard to sustain. Indeed, despite the fact that both sides need each other to varying degrees, intelligence-policy relations are characterized by friction, in part because the policy and intelligence communities are different tribes. Intelligence work is somewhat akin to scholarship, but policy work is action-oriented. Intelligence analysts are comfortable with uncertainty, but policymakers cannot let uncertainty get in the way of making decisions. Intelligence officials believe they provide a unique product because of their control of secret sources, but policymakers do not necessarily see things that way. They come into office with their own world views and their own networks that provide information and insight. They may express doubt that formal intelligence estimates and briefings offer any added value. For these and other reasons, friction is the norm.

Occasionally, normal friction descends into something more toxic and damaging. Relations may fall apart in several ways. The most important kinds of breakdown—what I call the pathologies of intelligence-policy relations—are neglect and politicization. Neglect occurs when policymakers ignore intelligence altogether or cherry-pick for analyses that support their preexisting views. Leaders ignore intelligence for many reasons. They may ignore intelligence that does not appear to be relevant to their pressing concerns. They may come into office trusting their own sources and their own instincts. Or, simplest of all, they may be unimpressed with the quality of analysis and decide it is not worth their time. Intelligence agencies can exacerbate the problem if they deliberately remove themselves from the policy process in order to protect their independence and objectivity. Regardless of who is to blame, neglecting intelligence can have large consequences for strategy and policy because it potentially deprives leaders or important information, as well as of an institutional check on their own preferences and beliefs.

**Politicization’s Effect**

The other main pathology is politicization, defined as the manipulation of intelligence to reflect policy preferences. Such manipulation comes in many forms. Direct politicization involves crude efforts to bully analysts into
supporting policy views, while indirect politicization involves more subtle signals about the direction of desired estimates. Both policymakers and intelligence officials are capable of manipulating estimates. Policymakers are guilty if they pressure intelligence agencies to change their findings in ways that are politically convenient. They sometimes discover that releasing intelligence is a useful way of overcoming public skepticism about policy plans, and when they face serious domestic hurdles to policy successes, they may push intelligence towards predetermined conclusions rather than objective assessments. Intelligence officials may be more or less willing to provide this “intelligence to please.” They may also politicize intelligence by indulging their own biases and letting their personal beliefs affect their analyses.

Politicization has three main effects on intelligence and intelligence-policy relations. First, it skews the content and tone of estimates, because politicized intelligence tends to downplay ambiguous or contentious data and presents findings with an unusual sense of certainty. Policymakers who use intelligence to win public debates cannot abide estimates that are cautious and conditional. They pressure intelligence to reach for conclusions that go beyond the underlying data, and normal analytical errors are magnified as a result. The process of politicization also inhibits reassessment. Intelligence agencies are less likely to revisit the kind of bold and unequivocal statements that are characteristic of politicized estimates, even after dissonant or contradictory information appears that might otherwise lead to a reexamination of previous conclusions. Finally, episodes of politicization can poison intelligence-policy relations for many years after the fact. Severe breakdowns tend to exacerbate mutual mistrust and reinforce old stereotypes that divide intelligence and policy officials. Policymakers in subsequent interactions are more likely to suspect that intelligence agencies are trying to obstruct their plans, and intelligence officials may become overly sensitive to anything that smacks of policy meddling. The upshot is a smaller role for intelligence in policy planning and implementation. Rather than using intelligence estimates to inform their judgment, policymakers will increasingly rely on their own instincts.

THE GREAT CACOPHONY

Changes in the media environment are also likely to exacerbate intelligence-policy problems. The rapidly expanding marketplace for information has given policymakers a huge number of alternatives to formal intelligence. Having more sources than ever on issues traditionally in the Intelligence Community’s portfolio, they are less dependent on intelligence agencies for updates on current events.

Perhaps the first important change in contemporary media occurred when cable television’s CNN took to the airwaves in 1980. The network rapidly
expanded the scope of its coverage and, by the end of the decade, Central Intelligence Agency (CIA) officials fretted about the “unspoken competition” between the two organizations. Today, dozens of U.S. and international full-time cable news channels are available to interested policymakers. The second change occurred when the World Wide Web appeared in the early 1990s. News-related sites and policy-oriented blogs appeared soon after. In 1999, about 50 blogs were available on the Web; today they number in the millions. In addition, social networking sites like Twitter and Facebook allow individuals to share text, images, and movies in near-real time from places where reporters have little or no access. Occasionally, they provide raw and vivid reports, as they did during Iran’s 2009 “Green Revolution,” when protesters used Twitter to send news about ongoing events after the government had shut down other communications networks. While policymakers might not be able to judge the veracity of their information, they are unlikely to ignore it.

The upshot of all this has been an explosion in news and commentary: traditional media, cable news, the Internet, and social networking sites all compete with intelligence agencies for policy attention. This creates serious dilemmas for both intelligence collectors and analysts. The problem for collectors is a trade-off between reliability and relevance. If they vet their own sources carefully, they risk being left behind by alternative media that face less serious consequences for reporting misinformation. But if collectors loosen their standards, they risk delivering bogus information to policymakers.

**Institutional Competition**

The problem for analysts is getting heard over all the noise. Intelligence analysts now compete not only with cable news commentators and bloggers, but also with an extraordinary number of think tank researchers. The number of think tanks has more than doubled over the last quarter century, with nearly 200 focusing on national security and international affairs. Many of them are deliberately designed to influence policy by organizing international meetings, providing avenues for policymakers to float new ideas, and recruiting former officials who are looking for a way-station before returning to the policy world. Meanwhile, private sector analytical firms produce reports that have the whiff of official intelligence estimates. The overlapping worlds of government agencies, think tanks, and analysis firms will make it increasingly hard for intelligence officials to convince policymakers that their estimates are unique and deserve special attention. Moreover, defense contractors and private sector firms lure intelligence professionals away from government service, often paying much higher salaries for analysts who bring their experience and security clearances to the job. Meanwhile, well-informed reports suggest that
government analysts are comparatively young, especially at the CIA. If leaders come to believe that the average analyst is young and rather mediocre, then intelligence products will become less relevant to strategy and policy.

Intelligence officials may try to finesse these dilemmas by changing how they present their work to policymakers. These officials have long struggled with the problems of conveying uncertainty in cases where information is incomplete or ambiguous. The professional obligation to be forthright about the limits of existing knowledge is in tension with the need to provide straightforward judgments to leaders who must make decisions, regardless of whether the underlying data is flawed. Striking the right balance between these two legitimate but contrary obligations has never been easy. But, as alternative sources threaten the relevance of intelligence agencies, intelligence chiefs will be seriously tempted to err on the side of boldness. “In a world in which the information is available to everyone,” one official laments, “the intelligence community is simply a second opinion.” In order to avoid this fate, intelligence leaders may overstate the quality of dubious data, and deliver certain inferences based on uncertain information.

ARAB PROTESTS AND CHINESE TUNNELS

Two recent cases highlight the problem. The first was the Arab Spring, a wave of protests against longstanding regimes in North Africa and the Middle East. The uprisings transformed the regional political landscape, directly or indirectly causing the fall of leaders in Egypt, Libya, Tunisia, and Yemen. They also set the stage for the bloody government crackdown in Bahrain and the ongoing civil war in Syria.

Obama administration officials were unhappy with the Intelligence Community’s failure to anticipate the uprisings and for failing to keep them abreast of changing events. The President apparently told Director of National Intelligence James Clapper that he was “disappointed with the intelligence community.” One senior intelligence official later admitted that the Community underestimated the depth of the Arabs’ popular anger and the possibility that it would lead to regime change. Of course, this was not the first time that intelligence agencies have been caught by surprise. But the fact that the Arab Spring protests were organized online suggested that traditional intelligence indicators were especially irrelevant. Now, the best way to keep up with major political change was seemingly not through espionage but by paying close attention to new media. The Intelligence Community was especially oblivious to new sources of information, according to critics, because it was so accustomed to working cooperatively with various Middle Eastern intelligence services. “I have
doubts whether the intelligence community lived up to its obligation in this area,” Sen. Dianne Feinstein (D-California) concluded during a Senate Intelligence Committee hearing. “Was someone looking at what was going on on the Internet?”

But predicting the timing or progress of political revolutions is extraordinarily hard, regardless of the technology used by revolutionaries. The notion that the Intelligence Community was particularly slow to understand what was happening in the Arab Spring is belied by the fact that few, if any, scholars saw it coming. Moreover, simply “looking at what was going on on the Internet” is no way to safely predict events, because of the amount and variety of information online. Political forecasting is notoriously difficult, and efforts to be more precise may flounder if analysts are overwhelmed by the avalanche of news and opinions that traffic the Internet. Nonetheless, intelligence agencies may have bureaucratic incentives to avoid future criticism by making confident predictions based on unreliable and even contradictory information.

**Beijing’s Initiatives Assessed**

The new media potentially effect not just warning intelligence but also strategic estimates. Phillip Karber, an adjunct professor at Georgetown University and former defense official, made headlines in November 2011 when he announced that China might possess as many as 3,000 nuclear warheads. This number is almost an order of magnitude higher than most open-source estimates. China watchers have long concluded that Beijing is satisfied that it can deter challengers with a fairly modest stockpile. Intelligence estimates had reportedly concluded that the actual total number of Chinese warheads is in the low hundreds.

Karber’s analytical method was as interesting as his conclusion, not least because he personally apparently did very little of the research that led to his remarkable finding. Instead, he oversaw the efforts of a group of Georgetown undergraduate students who “translated hundreds of documents, combed through satellite imagery, obtained restricted Chinese military documents, and waded through hundreds of gigabytes of online data.” Their efforts were aimed as uncovering information about a large-scale tunneling project run by China’s Second Artillery Corps, which is responsible for the country’s ballistic missile and nuclear arsenal. The students read everything from personal blogs to official military journals. They used Google Earth to survey the country for evidence of tunneling work. They even watched online Chinese fictional programs about life in the Second Artillery to corroborate what they read in government publications.

China formally announced the existence of the project in late 2009, though its long interest in tunneling was no secret. What startled observers was not
the tunnels themselves, but the notion that the Chinese might be using them to store thousands of warheads. Arms control experts were immediately skeptical of this claim. They noted that China would have needed to produce fissile material continuously for decades in order to build such a stockpile, but Beijing stopped its military production of HEU in 1987 and plutonium in 1990.\(^{21}\) Even using very generous assumptions, the known stockpile of fissile material could support an arsenal of only about a thousand warheads, and more realistic assumptions put the upper bound at about half that number.\(^{22}\) Moreover, critics argued that the study’s conclusions required extraordinary leaps of logic. For instance, Karber noted that China’s minimum safe-distance for keeping warheads apart was one mile. The tunnel network totaled about 3000 miles, he reasoned, meaning it was possible that China could safely store as many as 3000 warheads underground.\(^{23}\) But the fact that China has listed a minimum distance requirement does not mean that missiles are lined up every mile throughout the tunnels. More plausible is the notion that the long tunnels enhance the survivability of the relatively small arsenal. Enemies would have a difficult time locating the warheads and would be unsure that they had eliminated all of them in a first strike.\(^{24}\) While the precise motive for the tunnel project remains unknown, this logic is consistent with China’s public shift towards a posture of “assured retaliation.”\(^{25}\)

Finally, critics debunked some of the more dubious sources that found their way into the Karber study, including blog posts quoting other blog posts, and an anonymous comment on an online list serve from 1995.\(^{26}\)

Despite these problems, some policymakers were keen to hear more from Karber. Officials in the Office of the Secretary of Defense were briefed on the study, and some of its findings were reportedly included in the DOD’s annual report on Chinese military capabilities.\(^{27}\) In addition, Karber’s study apparently led lawmakers to include funding for a broad study of the Chinese arsenal in the pending Fiscal Year 2013 defense authorization bill.\(^{28}\) Whatever its shortcomings, consumers may have seen the study as an innovative use of new media with large implications for the strategic balance between China and the United States. They may also have been persuaded by Karber’s persistent claim that no one really knows the size and disposition of China’s nuclear forces. If policymakers come to believe that the Intelligence Community is just guessing in similar future cases, then they are more likely to entertain private sector analyses, no matter how outlandish, that seem to represent creative new approaches to hard problems.

**TWO FUTURES FOR INTELLIGENCE**

These examples may foreshadow two unhappy future scenarios for intelligence agencies. In the first, they will become increasingly irrelevant as
policymakers turn to other sources of information and insight. The characteristics of new media are speed, volume, and pervasiveness. Social media provide anyone with an iPhone and a Twitter account the ability to report in real time, and the spread of mobile devices means that reports can be sent from otherwise closed societies. The fact that social media users gained so much attention during the Green Revolution, the Arab Spring, and the ongoing Syrian revolt is not coincidental: they are able to send information from places sometimes off limits to traditional media. Any interested policymaker with a computer will be able to access this information almost instantaneously, meaning that institutional intelligence reporting runs the risk of being permanently out of date. Policymakers who previously questioned if the Intelligence Community could keep up with CNN are likely to become more skeptical about the utility of current intelligence in the Twitter age.

Alternately, intelligence leaders may exaggerate the amount or quality of the information they collect in order to overcome policy skepticism. Rather than ignoring new media and hoping that leaders grasp their unique capabilities, they may oversell them, thus making themselves vulnerable to further accusations of failure and incompetence if their reporting is faulty. In addition, they might also become willing to deliver intelligence to please in order to stay in the good graces of policymakers. Politicization will be more likely in this scenario.

Is such pessimism warranted? Social media are still relatively new, after all, and much of my analysis here is speculative. Moreover, the spread of social media and the Internet does not necessarily spell the end of objective and useful intelligence. Perhaps new media will be self-regulating in ways that allow intelligence agencies to remain above the fray. Anybody with a Twitter account can share news, to be sure, but others can quickly debunk bad information or shoddy analysis. It is worth nothing that the critics of Karber’s study of Chinese tunnels were able to track down and challenge his sources simply by following his linked citations. So we can imagine a future in which the online fracas becomes something like a marketplace of ideas operating at breakneck speed. At some point intelligence agencies might be able to convince policymakers that information online should be treated as dubious until proven otherwise, and in so doing stress that they are correct in sacrificing speed for reliability.

They may wisely take advantage of the online marketplace of ideas. Clever intelligence managers are likely to recruit new analysts who are comfortable with social media and adept at searching online for more or less useful information. Incorporating trustworthy online sources will not only improve the quality of their own analyses, but will also help them avoid looking like stubborn Luddites who willfully ignore important information. All of this will help convince policymakers that the modern intelligence
estimate combines the best of the new media with secret information gained clandestinely. The result, intelligence officials might claim, is a unique and indispensable product. Perhaps policymakers will even believe them.

REFERENCES


6 In extreme cases they can fall victim to what Sherman Kent called the “sickness of irresponsibility” and play no role whatsoever. Sherman Kent, Strategic Intelligence and American Foreign Policy (Princeton, NJ: Princeton University Press, 1949), p. 183.

7 This discussion is drawn from Joshua Rovner, Fixing the Facts, Chapter 8.


13 For a recent discussion see Charles Weiss, “Communicating Uncertainty in Intelligence and Other Professions,” International Journal of Intelligence and CounterIntelligence, Vol. 21, No. 1, Spring 2008, pp. 57–85.

24 The United States flirted with a similar program in the late 1970s when it considered building 4600 silos to house 200 MX missiles. These missiles would be moved from silo to silo in a kind of shell game that was meant to give the Soviet Union pause before it considered attacking the U.S. ICBM force. James M. Acton, “The ‘Underground Great Wall’: An Alternative Explanation,” Proliferation Analysis, Carnegie Endowment for International Peace, 26 October 2011, at http://carnegieendowment.org/2011/10/26/underground-great-wall-alternative-explanation/67s0
27 William Wan, “Georgetown Students Shed Light on China’s Tunnel System for Nuclear Weapons.”