The Institute for Stabilization and Transition

Finding solutions to global challenges for policy-makers, practitioners, eductators and media

www.StabilizationAndTransition.org

GUEST ESSAY

Guest Essay to the IST **No. 6 | September 2, 2014**

Stabilization and Transition Operations Need Counterintelligence Awareness

By William Brooke Stallsmith

Spying and counterintelligence should be serious concerns for any organization involved in international stabilization and transition. This is not for the usual reason, which is the accusations of espionage that insecure governments regularly and publicly level against NGO's, governmental development agencies, and other aid groups. Rather, it's because stabilization and transition operations themselves are often the targets of intelligence collection.

The word "counterintelligence" can appear scary to many people. It has connotations of gray, paranoid men in vaulted, windowless rooms conjuring enemy spirts from the vasty deep, or of the Stasi's informant networks that penetrated every niche of East German society. More accurately—and for the purposes of this paper—counter-intelligence is really the process of identifying, understanding, and countering espionage operations. It is akin to safety programs aimed at reducing the threat from fire and highway accidents, and to security programs about awareness and prevention of street crime. What sets counterintelligence apart is that the dangers it seeks to control come from sophisticated adversaries who are backed by the resources of a nation-state, terrorist network, or transnational criminal organization.

The United States Defense Intelligence Agency defines counterintelligence as "(i)nformation gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.

Who, why, and how?

Post-conflict relief and aid programs attract attention from threat actors[i] for three main reasons. First, aid and relief programs involve financial flows that are significant on a global scale and colossal in local terms; the United States Government alone has spent $104 billion on reconstruction projects in Afghanistan and another $60 billion in Iraq since 2002. A second and related reason is that, because of these financial and other resources, the activities of aid organizations often have an outsized political impact in post-conflict countries, whether or not the aid providers are pursuing explicit political or governance goals. Finally, threat actors may view aid agencies as a lightly guarded back door for gaining access to donor countries' diplomatic and military secrets.

Host-country governments are naturally interested in aid and reconstruction organizations whose activities may form a core part of the national economy—foreign aid accounted for some 47 percent of Afghanistan's Gross Domestic Product and more than 20 percent of GDP in eight other post-conflict states for the period 2008-2011, according to World Bank estimates.[ii] Gathering confidential information on aid groups can be seen as essential for formulating economic policies, tracking political opposition groups perceived as controlled by outside donors (especially those engaged in governance activities), and identifying opportunities for corrupt officials to siphon off funds. Even governments of the poorest states have ample

means for clandestine intelligence collection. The most fruitful method is likely to be exploitation of local information technology and communications networks. Nearly every government has "lawful intercept" legislation that grants law enforcement and related government agencies access to communications networks for collecting evidence for criminal investigations, and many—including in post-conflict and less-developed countries—exercise this power broadly. Ethiopia, for example, has a widespread program of electronic surveillance that takes advantage of the government's control of the national telecommunications monopoly, according to Human Rights Watch.

Host-country intelligence and law enforcement agencies can also employ longstanding human-based tactics, such as physical surveillance by fixed and mobile teams, elicitation of information from unsuspecting contacts, and "social-engineering" people into opening e-mails or accessing thumb-drives loaded with malicious code. Of particular concern to aid agencies, local security services can easily recruit informants within foreign organizations by appealing to employees' patriotism, offering financial inducements, or threatening dire consequences in the event of non-cooperation.

Third-country governments use the same range of intelligence tradecraft to collect information about stabilization and transition operations. Former National Security Agency contractor Edward Snowden has alleged that the United States routinely intercepted the communications of international relief and aid organizations, and the cybersecurity firm Mandiant[iii] in 2013 reported that a Chinese military intelligence unit had penetrated the computer systems of international development and cooperation agencies, as well as scores of Western government agencies and private-sector businesses. Whether regional neighbors or global powers, third-country governments may be interested in information about the underlying military or humanitarian crisis that has led to aid and relief operations. Such actors may also view aid organizations as proxies for other states and conduct espionage against them as a way to penetrate a rival government. Finally, non-state actors have been observed employing intelligence tradecraft against government agencies and private-sector companies, and are probably targeting aid and relief organizations as well.

Social networking sites (SNS) such as Facebook and LinkedIn are a powerful tool for intelligence collectors. People publish personal and professional information—sometimes inadvertently and sometimes because they have been socially-engineered into doing so—that otherwise might have taken months of investigation to uncover. Intelligence services, criminals, and other threat actors use SNS data to analyze professional and personal networks and refine their targeting.

- Criminal groups want information about aid organizations to help steal funds. Programs in post-conflict situations may appear particularly tempting targets because they are typically under pressure to deliver resources quickly and without the usual bureaucratic controls. Criminal groups' interests range from collecting inside information to help rig bidding processes to the penetration of information and computer systems that contain marketable financial information.

- In many stabilization and transition situations, terrorists foment instability as a strategic tool against the local government or its international allies, and they view aid efforts as support to the enemy. Such groups may therefore seek to collect information on aid organizations' links to the host government and international partners, as well as to prepare for possible kinetic strikes or kidnappings of aid personnel. The US inspectors general for Iraq and Afghanistan have also noted that terrorists, like other criminals, are interested in siphoning off assistance money, making information on aid groups' in-country contracting a priority for intelligence collection

What is to be done?

Espionage has been a staple element of the ways different groups of people have dealt with each other for millennia—according to the Bible, since Joshua sent two men to spy on the land of Canaan[iv]—and states,

terrorist organizations, criminal gangs, and other groups show no signs of halting efforts to learn the secrets of enemies and partners. Aid and relief organizations need to face up to this ongoing threat, assess their vulnerability to losing control over critical information and to having their programs manipulated, and take realistic steps to protect themselves.

The first step should be to inventory your organization's operations and information. What is the most important and sensitive information you possess? Where is this information located, whether in virtual or physical form? What would be the consequences of having it compromised? What steps are you currently taking to protect it? Are members of your organization aware of the importance and vulnerability of this information?

At the same time, develop situational awareness. Look at your organization from outside-in. That is, consider how the local security services, third-country governments, terrorists, criminals, and others look at your organization. What is it about your organization that might cause it to be targeted by intelligence collectors? What do you know about these potential threat actors, what their priorities are, and how they might operate?

The boundaries between the types of threat actors discussed in this paper are not hard and fast. Different threat actors often cooperate with each other. In the Sahel, for example, kidnappings of international aid workers often appear to be the work of joint efforts by terrorist groups and criminal gangs. Similarly, many governments out-source to independent hacker groups their efforts to penetrate computer networks of interest.

Don't play James Bond. On the reasonable assumption that someone—or many someones—is monitoring your communications, make sure you don't appear to be something you aren't. Avoid red-flag words such as "intelligence" or "kinetic." Exercise discretion in any electronic communication, which may be subject to interception. Even if you're certain your organization is being targeted by intelligence collectors, resist the temptation to engage in cinematically inspired counter-measures, such as aggressive driving to shake suspected surveillance vehicles.

Plan for the worst. What would you do if sensitive information—say, personal or financial data concerning local employees or a memo that frankly evaluates shortcomings of your local government counterparts—is compromised? Fast, effective response can mitigate much of the damage that might otherwise occur.

Finally, don't over-react. You will never attain zero risk of penetration by intelligence collection. But you can increase the protection of what is most important by intelligent and pro-active awareness.

William Brooke Stallsmith is an intelligence analyst who worked in the US Intelligence Community on economic espionage, counter-intelligence, regional stability in Africa and the Near East, and international economic issues. He retired from the Central Intelligence Agency in 2007. He earned an MBA from Columbia University and a BA from the University of Virginia.

[i] By "threat actor," I mean any group that uses intelligence tradecraft—including human and technical operations—to clandestinely collect non-public information or manipulate the behavior of a targeted organization or individual to achieve a covert objective.
[ii] The eight other countries identified in the World Bank study are Liberia, Timor-Leste, the Palestinian Territories, Burundi, Haiti, Democratic Republic of Congo, Mozambique, and Rwanda.
[iii] Mandiant has since been acquired by another cyber security company, FireEye.
[iv] Joshua 2:1 seems to confirm that spying is the second-oldest trade; in Canaan, the two spies were lodged at the house of a "harlot"—a practitioner of the oldest profession.

An IST Publication