“Have you got a minute?” Understanding elicitation approaches

October 26, 2018 *Product of the Research & Information Support Center (RISC)*

Introduction

Foreign governments and businesses place a high value and priority on U.S. personal and proprietary information. Travelers may assume that they will not be targeted because they believe foreign actors are only after classified government intelligence; however, foreign actors try to collect sensitive defense, technical, political, economic, proprietary, trade, and personal information from businesspeople, government employees, academics, and researchers.

Foreign intelligence services, companies, and academic institutions may attempt to elicit information from travelers regardless of their affiliation or level of responsibility. Elicitation is a non-threatening intelligence-gathering technique used by intelligence collectors seeking to gain information through what appears to be ordinary conversation and interaction. Elicitation is easy to disguise, deniable, and effective, and can be done in person, over the phone, through electronic correspondence, or in writing. The specific purpose of elicitation is to collect information that is not readily available, and to do so without raising suspicion. When conducted by a skilled collector, elicitation will appear to be a normal social or professional conversation, and a person may never realize that they were targeted or that they provided meaningful information to an adversary.

Elicitation Techniques and Why it Works

To gain access to desired information, foreign adversaries can use a number of techniques, including computer hacking, forced joint-ventures, and technology transfers. They also attempt to develop human assets through elicitation. A professional trying to elicit information will use certain techniques in an attempt to exploit human or cultural predispositions. The natural tendencies that an elicitor may try to exploit include:

- desire to be polite and helpful, even to strangers or new acquaintances;
- desire to appear well informed, especially about one’s profession;
- desire to convert someone to one’s opinion;
- desire to feel appreciated and believe we are contributing to something important;
- tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used;
- tendency to believe others are honest, or a disinclination to be suspicious of others;
- tendency to answer truthfully when asked an “honest” question;
- tendency to expand on a topic when given praise or encouragement;
- tendency to gossip; and
- tendency to correct others.

To develop a target, elicitors will exploit the desires and tendencies noted above, often using multiple techniques in an elicitation attempt. The following chart provides descriptions of some of those techniques:

Technique	Description
Appeal to Ego / Flattery	Use praise to coax a person into providing information. Also called "Teach Me," as the collector claims to know little about a topic and asks the expert to tell them all about it.
Assumed Knowledge	Pretend to have knowledge or associations in common with a person.
Bracketing	Provide a high and low estimate in order to entice a more specific number.
Can you top this?	Tell an extreme story in hopes the person will want to top it.
Confidential Bait	Pretend to divulge confidential information in hopes of receiving confidential information in return.
Criticism	Criticize an individual or organization in which the person has an interest in hopes the person will disclose information during a defense.
Deliberate False Statements / Denial of the Obvious	Say something wrong in the hopes that the person will correct your statement with true information.
Feigned Ignorance	Pretend to be ignorant of a topic in order to exploit the person's tendency to educate.
Good Listener	Exploit the instinct to complain or brag, by listening patiently and validating the person's feelings (whether positive or negative).
Leading Question	Ask a question to which the answer is "yes" or "no," but which contains at least one presumption.
Macro to Micro	Start a conversation on the macro level, and then gradually guide the person toward the topic of actual interest.
Mutual Interest	Suggest you are similar to a person based on shared interests, hobbies, or experiences, as a way to obtain information or build a rapport before soliciting information
Oblique Reference	Discuss one topic that may provide insight into a different topic.
Opposition / Feigned Incredulity	Indicate disbelief or opposition in order to prompt a person to offer information in defense of their position.
Provocative Statement	Entice the person to direct a question toward you, in order to set up the rest of the conversation.
Questionnaires and Surveys	State a benign purpose for the survey. Surround a few questions you want answered with other logical questions. Or use a survey merely to get people to agree to talk with you.
Quote Reported Facts	Reference real or false information so the person believes that bit of information is in the public domain.
Ruse Interviews	Someone pretending to be a headhunter calls and asks about your experience, qualifications, and recent projects.

Target the Outsider	Ask about an organization that the person does not belong to.
Three-step Approach	Start conversation on an irrelevant topic to build rapport, then shift the conversation to the topic of interest to elicit. Finally move the topic back to something irrelevant before ending the conversation. Over time, individuals tend to recall the beginnings and ends of conversations, but forget what was said in the middle.
Volunteering Information / Quid Pro Quo	Give information in hopes that the person will reciprocate.
Word Repetition	Repeat core words or concepts to encourage a person to expand on what he/she already said.

Elicitation attempts can occur anywhere – at social gatherings, conferences, “chance” encounters on the street, or in someone’s home – and range from simple to sophisticated. These efforts include creating fake social media accounts to recruit specific individuals, and paying academics and researchers for scholarly or professional papers and speaking engagements. Elicitors may also attempt to collect information about individuals or their colleagues to facilitate future targeting attempts.

Case Study: Targeting Academia

Foreign governments target the academic community for a number of reasons, including gaining insights into U.S. policy, or building relationships with individuals either connected to government officials or who may eventually hold high-level government positions themselves. Foreign adversaries also target the academic community to acquire valuable research, information, and technology developed at U.S. universities. This enables them to bypass expensive research and development, gain access to restricted products or information, identify valuable recruits, and allows foreign countries or companies to gain an economic or technological edge.

In the FBI-produced short film, "Game of Pawns: The Glenn Duffie Shriver Story," the true story of an American student studying in China is dramatized to show the incremental steps taken by Chinese intelligence officers to recruit Shriver to work for the Chinese Ministry of State Security. The Ministry targeted Shriver for his political and language knowledge, and the foreign intelligence service was able to appeal to his ego and desire for easy money. He had initially responded to an advertisement to write an unclassified paper about U.S.–China relations with regard to Taiwan and North Korea, reportedly for the local Shanghai government. Shriver’s government contact, “Amanda,” praised his paper and paid him for his effort. This was a type of low-key initial elicitation, which later developed into full recruitment as “Amanda” paid Shriver to apply for jobs with the U.S. Department of State and the Central Intelligence Agency. Shriver was subsequently arrested and sentenced to four years in prison for making false statements and conspiring to provide information to a foreign intelligence service.

The risks to students and professors are both real and preventable, and universities should take steps to prevent elicitation from the potentially damaging consequences to their student body, reputations, and intellectual property.

Case Study: Exploiting Cultural Exchanges

In 2013, multiple media outlets reported an FBI investigation into a Russian government-run cultural exchange program that paid for more than 100 U.S. citizens – political aides, nonprofit directors, business executives, and graduate students – to visit Russia on extravagant group trips. The reports stated that the organizers of the exchange program, which was run by *Rossotrudnichestvo*, a Russian government agency, and the Russian Cultural Center in Washington D.C., could have used the trips clandestinely to assess and recruit Americans to work as intelligence assets for the Russian government. In April, the director of the cultural center was one of 60 Russian officials expelled from the U.S. because they were reportedly known intelligence officers. Between 2011 and 2013, *Rossotrudnichestvo* organized and paid for 1,000 politicians, scientists, and business people from 50 countries to visit Russia on cultural exchanges.

Case Study: Contacting Former Cleared Personnel through Social Media

Foreign intelligence services are reported to aggressively use fake social media accounts in making contact and recruiting individuals with access to sensitive commercial or government information. In February 2017, a Chinese intelligence officer used LinkedIn to contact Kevin Mallory, a former U.S. defense and intelligence contractor who was then working as an independent security consultant. The Chinese official, who claimed to be a think tank representative, recruited Mallory to be a foreign policy consultant. Mallory took two trips to China to meet with his contacts, where he was asked questions about missile defense, the South China Sea, and currency manipulation, and given a mobile device with special encryption capabilities to continue communicating while in the U.S. Upon returning to the U.S., Mallory sent at least two classified documents to the Chinese officials in exchange for $25,000. Mallory was arrested and charged with espionage and lying to the FBI, and in June, was convicted on four counts.

How to Respond

There are a number of appropriate responses to an uncomfortable conversation, including:

- stating that you don't know the information;
- giving a vague or non-descript answer;
- referring the questioner to public sources (websites, press releases);
- deflecting attention by asking a question of your own (e.g. "Why do you ask?"); and
- stating that you need to clear a discussion on this topic with your security office.

The key to handling these situations is to ignore or deflect the conversation, and report the encounter. If you believe that someone was trying to elicit information from you or someone in your organization, report the incident to the appropriate authority, including a program director or international security manager, or the nearest U.S. embassy or consulate. Upon return to the United States, you may also report suspected elicitation to your local FBI field office.

Protecting your Organization

The first step to protect your organization is to identify critical information. Organizations should draw clear lines as to what information should not be shared, and be suspicious of individuals who seek that information. Organizations should train personnel to protect critical information from unauthorized disclosure, including knowing what information is critical, being aware of who needs to know about it, understanding who might want it, and recognizing and appropriately handling an elicitation. Attempts to elicit critical information by foreign adversaries may occur in the U.S. as well, so personnel should be cautious in conversations no matter their location. Preparing individuals for elicitation should be conducted in conjunction with the implementation of other physical and electronic access controls to protect personal and proprietary information.

Additional Information

For additional information, please contact OSAC's Cyber Analyst and see the FBI's Elicitation Brochure.