GlobalResearch
Center for Research on Globalization

The CIA's Latest Greatest Failure

By Philip Giraldi
Global Research, November 08, 2018
Strategic Culture Foundation

Region: USA
Theme: Intelligence

Government agencies that are skilled at invading nearly everyone's privacy worldwide are sometimes totally inept at keeping their own internal communications secure. The problem is particularly acute for the Central Intelligence Agency (CIA), which must maintain secure contact with thousands of foreign agents scattered all over the world. By secure contact one means being able to provide specific targeting to the agents and received in return detailed information that responds to what is being sought without any third party being able to intercept or interpret what is being shared.

Communicating is the most vulnerable element in any foreign agent operation, particularly as counter-intelligence services commit major resources to cracking the systems used to link an agent in the field with his case officer or handler, who might be in the same country under diplomatic cover but just as easily might be in another nearby country or halfway around the world.

Various media reports have lately been detailing a catastrophic communications security failure by CIA that took place between 2007 and 2013. In simple terms, what took place was this: the Agency developed a method of covertly communicating with its agents through the internet that involved sites which enabled two way communications that were believed to be both secure and efficient. It presumably operated like social media sites where you have to log in, provide a password and then are able to send and receive messages. It almost certainly had some level of encryption built into it and there may have been several layers of passwords and/or questions that the user had to answer to gain access.

Once developed, the system, which was originally intended only for occasional low-level use, was then deployed to handle nearly all the CIA's agent communications worldwide, including a number of key countries targeted by Washington, to include Iran and China. Each country had a separate site and the sites themselves were set up under innocuous business or social cover arrangements which presumably would have made them of no interest to prowling counterintelligence services.

What exactly went wrong is not completely clear, but the mechanism was discovered by Iranian counterintelligence, possibly employing information provided by a double agent. The Iranians determined what kind of indicators and components the CIA site had and then went on a Google search to find other similar sites. They then watched their site as well as the others, noting both their activity and their idiosyncrasies, and were presumably were able to penetrate the site directed against them. At some point, they passed what they had learned on to the Chinese and possibly others.

The Chinese expanded on the Iranian work by breaking through the firewall in their

country's site and getting into the entire system. It was possible to identify all the CIA agents in China. More than two dozen were arrested, tortured and killed and a like number were found and executed in Iran, though some were warned by CIA and were able to escape.

Agents in other countries were also exfiltrated as a security measure because it was not known to what extent the information on the system had been compromised and shared. The damage is still being assessed, but one thing that is known is that the United States knew little or nothing about what was going on in China and Iran at a critical time when negotiations over nuclear programs and North Korea were taking place.

The internet communications system was used so extensively because it was easy to use. When it eventually crashed, fully 70% of CIA communications with agents were potentially compromised. Ironically, a CIA contractor had, in 2008, warned that the internet system had major flaws that could be exploited. He was fired for his pains.

Secret communications to protect spies are as old as the Greeks and Romans, who used codes and substitution ciphers. The leap into internet communications by the CIA demonstrated that no system is infallible. The CIA got lazy and did not do its homework when setting up communications plans with agents. The reality is that running agents in a hostile foreign country is more an art than a science. You communicate with a spy in a way that fits in with his lifestyle so as not to arouse suspicion. He or she might be able to take phone calls, or receive letters with invisible writing. They might have the privacy to do burst communications from a computer to a satellite. Or they might prefer to use the old-fashioned methods — to include chalk marks signaling dead drops, brush passes and encrypted communications using one-time pads. CIA, which lost many of its skilled spies post 9/11 after it went crazy over electronics, drones and paramilitary operations, will now have to relearn Basic Espionage 101. It will not be easy and will take years to do if it is even possible. Some might argue, perhaps, that the world would be a better and safer place if it is not done at all.

*

Note to readers: please click the share buttons above. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Philip M. Giraldi *is a former CIA counter-terrorism specialist and military intelligence officer who served nineteen years overseas in Turkey, Italy, Germany, and Spain. He was the CIA Chief of Base for the Barcelona Olympics in 1992 and was one of the first Americans to enter Afghanistan in December 2001. Phil is Executive Director of the Council for the National Interest, a Washington-based advocacy group that seeks to encourage and promote a U.S. foreign policy in the Middle East that is consistent with American values and interests. He is a frequent contributor to Global Research.*

Articles by: **Philip Giraldi**