Open Source: A New Horizon for Information and Intelligence

Lt. Gen. Michael K. Nagata, U.S. Army (Ret.), Strategic Advisor and Senior Vice President, CACI International Inc

In 2014, U.S. military forces rushed back to Iraq to confront the sudden emergence of the Islamic State (IS). In early efforts to understand this threat and begin effective targeting, the U.S. military and its allies had to overcome a significant intelligence deficit, since most intelligence assets were withdrawn when American forces left Iraq in 2011. However, many Iraqis, Kurds, Syrians, and others began using their personal cellphones to transmit large amounts of operationally useful “open source” data and intelligence to U.S. and coalition forces. This information substantially aided early military actions against IS until more traditional capabilities could be repositioned into theater.

More broadly, the rapidly increasing operational and strategic value of open source intelligence (OSINT) information is a trend the U.S. Government has been slow to grasp. Consider this provocative, but nonetheless probable future reality: As these trends continue, someday the U.S. President’s Daily Brief (PDB) – for decades compiled for the President’s daily consumption almost exclusively from classified information and intelligence – will instead be compiled primarily from OSINT.

The reality of the growing importance of open source information exploitation, which will only continue to expand, poses several crucial questions for both U.S. Government and defense industry leaders to consider:

- As American national security activities become more and more dependent on the effective harvesting and employment of open source information, how will this trend alter traditional mission and enterprise national security capability needs?
- What will U.S. Government customers need from industry to conduct the training and education for government personnel required to effectively operate in the rapidly expanding open source information arena?
- As government becomes more dependent on open source information, what will it need from industry to ensure its own open source activities and capabilities are capable of withstanding, or rapidly recovering from, adversary cyber intrusions or attacks?