"A Global Battleground: The Fight against Islamic Extremist at Home and Abroad"
Testimony: US House of Representatives, 24 March 2014
Philip Mudd

The terror battleground has undergone a revolution during the 14 years after the 9/11 attacks. Among the most significant changes Intelligence Community agencies face are the rapid spread of the physical geography of terrorism and the virtual geography of terror propaganda, radicalization, and recruitment.

When I returned to the CIA from a White House assignment in January 2002, the CIA Counterterrorist Center faced a clear terror target: the architects of the 9/11 attacks. Most of those al-Qa'ida terrorists fled from Afghanistan to Pakistan -- though some went to Iran -- and their geographic footprint was small; overall, the al-Qa'ida organization was not large. Before 9/11, though, the dissemination of the al-Qa'ida message had spread across the globe, as far afield as East Asia, North Africa, and Western Europe. The methods of disseminating that message had not yet entered the Internet age. Today, like the rapid spread of the locations in which al-Qaida-inspired groups operate, the virtual efforts by these groups have ridden the Internet and social media wave. What was once an al-Qa'ida group is now an al-Qa'idist revoltuion.

Both these stories, then -- the physical reach of violent extremism and its virtual influence -- have changed, and they continue to evolve quickly:

- We do not have an adversary's leadership that operates within within one clearly defined geographic area. The al-Qa'idist revolution, now morphed into the new and different ISIS ideology, includes leadership and groupings in areas as far-flung as northern Nigeria, Libya, Syria, Iraq, Yemen, and the West.
- We cannot target individuals who are radicalization nodes; now, the nodes are virtual, difficult to trace, and easily altered, sheltered, or moved by the adversary.

We can talk about the evolution of these changes and the emerging virtual nodes, but we might consider focusing as well on how we respond to them, in both the public and private sectors. Following are a few questions we might consider discussing during the hearing on 24 March:

- What kind of public/private partnerships might we consider as we enter an era in which private companies -- phone, Internet, shopping, and other digitally-driven firms -- hold information that can help locate, track, and apprehend adversaries?
- How should the US Government engage with NGOs and private sector companies in developing strategies to counter this ideology? Should the government lead or follow?

Thank you for inviting me to the hearing. I look forward to the conversation about the future of counterterrorism, and the future of intelligence and federal law enforcement in the digital age.