

resources; and the tiers allow an organization to view its approach to and processes for managing cyber risk.

Also, in an effort to boost framework use, the Department of Homeland Security (DHS) has established the Critical Infrastructure Cyber Community, or C3 (C-Cubed), Voluntary Program, a public-private partnership that connects companies and federal, state, local, tribal and territorial partners to DHS and other federal government programs and resources for help managing their cyber risks. **IAJ**

Joint Publication on Counterinsurgency Reviewed by CSIS

In early February, the Center for Strategic and International Studies (CSIS) released their review of recently updated Joint Publication (JP) 3-24 Counterinsurgency (COIN). JP 3-24 was updated in November 2013 and amends the original JP that was published in 2009.

The review of the updated JP credits the revised COIN manual with addressing some of the issues with the original document, including what were seen as unrealistic and overly ambitious expectations for societal and institutional change. However, the CSIS review also notes five shortcomings to the JP.

According to the review, JP 3-24 overestimates the influence the U.S. has with host-nation leaders and power brokers. The updated JP also overestimates the willingness of U.S. political leaders to insist on whole-of-government coordination and of bureaucratic leaders to give up existing decision-making privileges. Additionally, the JP underplays the importance of actors outside the U.S., and does not recognize that any U.S. COIN strategy should be designed to support the host-nation's strategy. Finally, while the JP acknowledges the need to identify and address the root causes of an insurgency, it underestimates the time and resources required to sustainably address these causes.

The review recognizes that it is unlikely that this JP will be used after U.S. involvement in Afghanistan diminishes at the end of this year. Still, the review suggests expanding civilian capacities for conflict diplomacy, prevention, and mitigation to reduce demand for military intervention, but recognizes that the demand for civilian capacity is usually unmet. **IAJ**

State, USAID Launch Second QDDR

On April 22, the State Department announced the launch of its second Quadrennial Diplomacy and Development Review (QDDR). Several top representatives from State and the U.S. Agency for International Development (USAID) spoke at the launch, including Secretary of State John Kerry, Deputy Secretary of State Heather Higginbottom, USAID Administrator Rajiv Shah, and Special Representative Tom Perriello.

The QDDR focuses on human rights, democracy, and civilian security, while recognizing the importance of engaging diplomats, development experts, and other stakeholders, including NGOs. The first QDDR was released in December 2010, enumerating the diplomacy and development efforts of State and USAID, and outlining several reforms for the agencies. Some of the reforms suggested in the 2010 QDDR have already been implemented, while others remain underway.

In his remarks at the April launch, Special Representative for the QDDR Tom Perriello said

“I know that diplomacy and development work because I’ve been blessed to witness it myself. Done right, diplomacy and development can prevent wars, it can reduce extreme poverty, it can transform the rights of girls, and advance transparency over corruption.”

Secretary of State John Kerry also shared his hopes for the future of diplomacy and development, saying “I want to see us advance diplomacy and advance development.” He continued, explaining the importance of the QDDR. “[The QDDR is] also a preview of what State and USAID need to do in order to put the United States of America in the strongest position to face the challenges and seize the opportunities of tomorrow.”

The review will take place over the course of a few months. **IAJ**

Research Suggests Use of DoD-Developed Technology along U.S. Border

Earlier this year, the RAND Corporation completed research into whether or not the Department of Homeland Security (DHS) and the Drug Enforcement Administration (DEA) could use intelligence, surveillance, and reconnaissance technologies developed by the Department of Defense (DoD) to help secure the U.S. southern border.

RAND’s report, which was published in May, focused on the legality of DHS and DEA using DoD-funded technology. The new sensor technologies were created to support military forces operating in Iraq and Afghanistan, and were tested along the U.S. southern border because the field conditions along the border closely resemble those in current military theaters of operation. The technology demonstrations would also reveal if the new technologies would be useful in domestic law enforcement led counterdrug operations along the U.S. border.

This report explores the legality of these technology demonstrations, and whether the DoD sensors can legally be used in domestic counterdrug operations when operated by U.S. military forces. The researchers examined federal law and DoD policy, and found that parts of U.S. law mandate information sharing among federal departments and agencies for national security purposes and direct the DoD to play a key role in domestic counterdrug operations in support of U.S. law enforcement agencies. However, other parts of the law place restrictions on when the U.S. military may participate in law enforcement operations.

After reviewing relevant federal law and DoD policy, the authors concluded that there is no legal reason why a DoD sensor should be excluded from use in an interagency technology demonstration or in an actual counterdrug operation as long as a valid request for support is made by an appropriate law enforcement official. The authors recommend DoD policy on domestic counterdrug operations be formally clarified and that an approval process should be established for technology demonstrations with a counterdrug nexus. **IAJ**