

DEPARTMENT OF DEFENSE  
**DEFENSE SCIENCE BOARD**

**Task Force on  
Department of Defense Strategy to Counter  
Violent Extremism Outside of the United States**



**APRIL 2015**

**OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS  
WASHINGTON, D.C. 20301-3140**



This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB Task Force on Department of Defense Strategy to Counter Violent Extremism Outside of the United States completed its formal information gathering in July 2014, but continued to update factual input through final report review.

This report is UNCLASSIFIED and releasable to the public.



DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

16 April, 2015

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY &  
LOGISTICS)

SUBJECT: Report of the Defense Science Board (DSB) Task Force on Department of Defense Strategy to Counter Violent Extremism (CVE) Outside of the United States

I am pleased to forward the final report of the DSB study on Department of Defense Strategy to Counter Violent Extremism Outside of the United States, chaired by Mr. Michael Bayer. The Task Force concluded that the DoD should more clearly define its role in a multilateral approach to CVE, where the USG leverages its diverse partnerships to bring a complementary package of authorities, resources, and expertise to bear against this challenging and evolving threat.

The Task Force also concluded that there needs to be a more overarching pan-Government U.S. strategic framework for CVE, and within the DoD should be a clearer, common definition of CVE and a more overarching strategy for where DoD fits within that definition. Therefore, implementation of CVE functions into DoD roles and missions is not fully coordinated, and the positive or negative effects of DoD operations on broader USG CVE efforts remain difficult to measure.

The Task Force acknowledges that DoD may not be the right organization—in terms of authority, capabilities, and / or expertise—to carry out many CVE tasks, particularly over the longer term. As DoD transitions away from large-scale deployments with combat missions, it will be more important to specify which CVE responsibilities it should lead, and which it should support.

The Task Force recommended three areas that require immediate action to ensure proper attention is given to the evolving and dangerous threat from extremism. The recommendations focus on: developing an overarching, multilateral strategy for CVE abroad; improving understanding of CVE to establish measurable goals and metrics to guide prioritization of actions and resource allocation; and explicitly clarifying, promulgating, and coordinating the DoD CVE strategy.

I concur with the Task Force's conclusions and recommend you forward the report to the Secretary of Defense.

Craig Fields  
Chairman, DSB





DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

16 April, 2015

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on Department of Defense (DoD) Strategy to Counter Violent Extremism (CVE) Outside of the United States

The final report of the Defense Science Board Task Force on Department of Defense Strategy to Counter Violent Extremism Outside of the United States is attached. The Task Force conducted an independent assessment of DoD CVE efforts outside of the United States to include an exploration of DoD CVE strategy, policy, activities, and role in interagency CVE coordination and decision making. The study was initiated in response to Congressional tasking. The study team was selected by the Defense Science Board to reflect strong experience in DoD strategy and policy development, and was carefully screened to avoid any real or perceived conflict of interest.


The Task Force's findings and recommendations are based on presentations and discussions with senior military and civilian leadership across key organizations associated with CVE. These included Department of Defense representatives from the Office of the Secretary of Defense, the Joint Chiefs of Staff, Combatant Commands, and interagency partners to include the National Counterterrorism Center, the Department of State, the National Intelligence Council, and the U.S. Agency for International Development.

The Task Force identified three key findings in their assessment

- Successfully countering violent extremism abroad will require a multilateral approach in which the USG needs to leverage its diverse partnerships to bring a complementary package of authorities, resources, and expertise to bear against this challenging and evolving threat.
- There needs to be a more overarching USG strategic framework for CVE, with activities better coordinated under more coherent policy goals across the whole of USG. Within the DoD, there needs to be a clearer common definition of CVE and a better articulated overarching strategy for where DoD fits within that definition. Implementation of CVE functions into DoD roles and missions should be better coordinated.
- DoD may not be the right organization—in terms of authority, capabilities, and / or expertise—to carry out many CVE tasks, particularly over the longer term. As DoD transitions away from large-scale deployments with combat missions, it will be important to specify which CVE responsibilities it should lead, and which it should support.

The Task Force identified three sets of recommended actions to address these findings and ensure that DoD most appropriately and effectively uses its authorities, resources, and expertise to support a multilateral CVE strategy. The Task Force assesses that action is urgently needed to address its recommendations given the scope and critical nature of the evolving extremist threat and ongoing political initiatives to the US role in global CVE initiatives.

We would like to express our sincere appreciation to the Task Force members and government advisors whose technical and operational insights, hard work, dedication, and passion for helping the Department resulted in the Task Force report. We would also like to thank the briefers who presented their views on the issues the Task Force addressed. We hope that our sponsor finds the information contained in this report useful and that the specific recommendations we have made are actionable.



Michael Bayer  
Chairman

# Table of Contents

Executive Summary .....	1
Introduction.....	5
Scope Note .....	5
The CVE Challenge .....	6
Understanding Extremism.....	8
Discussion .....	8
Findings.....	9
CVE Strategy, Roles, and Programming.....	11
Discussion .....	11
CVE in DoD.....	12
Authorities.....	14
Findings.....	14
Measuring the Effectiveness of CVE.....	17
Discussion .....	17
Findings.....	17
CVE through Messaging.....	18
Discussion .....	18
Strategic Communication.....	18
Findings.....	19
Task Force Recommendations .....	21
Appendix A: Task Force Terms of Reference .....	A-1
Appendix B: Task Force Membership .....	B-1
Appendix C: Briefings Received .....	C-1
Appendix D: Bibliography .....	D-1
Appendix E: Non-DoD CVE Programming.....	E-1
National Counterterrorism Center .....	E-1
Department of State.....	E-1
United States Agency for International Development (USAID).....	E-2
Broadcasting Board of Governors (BBG).....	E-2
Appendix F: Strategic Communication Roles.....	F-1
Appendix G: Acronyms .....	G-1

# Executive Summary

In May 2011, Congress tasked the Chairman of the Defense Science Board (DSB) to establish a Task Force on Department of Defense (DoD) Strategy to Counter Violent Extremism (CVE) Outside of the United States (“Task Force”). The Task Force members were asked to assess the following areas of interest related to the DoD’s CVE strategy outside of the United States:

1. A review of the current strategy, research activities, resource allocations, and organizational structure of the DoD for CVE outside of the United States;
2. A review of interagency coordination and decision making processes for executing and overseeing strategies and programs for CVE outside the United States;
3. An analysis of alternatives and options available to the DoD for CVE outside of the United States;
4. An analysis of legal, policy, and strategy issues involving CVE efforts outside of the United States as such efforts potentially affect domestic efforts to interrupt radicalization efforts within the United States;
5. An analysis of the current DoD information campaign against violent extremists outside of the United States;
6. Such recommendations for further action to address the matters covered by the report as the DoD considers appropriate; and
7. Such other matters as the DSB determines relevant.

The Task Force convened a series of meetings in 2014 and received briefings on the CVE topic from subject matter experts in the DoD, broader USG, think tanks, and academia. The Task Force focused its discussions and this report on what it believes are the most salient, current CVE issues for DoD, within the broad Terms of Reference.

The breadth of this endeavor is apparent in the variety of “CVE” definitions and scopes found in the literature, used by Task Force briefers, and embodied in government documents. To the extent there are commonalities among definitions of CVE, the Task Force focuses on violent extremism generally targeting innocent civilians vice combatants. This definition includes a full range of activities related to CVE, from countering inspiration and radicalization, to building community resilience and law-enforcement capacity, to countering extremist messaging. The Task Force considers analysis of kinetic operations outside the scope of this report.

This Task Force understands that successfully countering violent extremism abroad requires a multilateral approach in which the USG needs to leverage its diverse partnerships to bring a complementary package of authorities, resources, and expertise to bear against this challenging and evolving threat. Although this Task Force was charged with evaluating DoD CVE efforts (outside the United States), the necessity of a collaborative CVE approach dictates that we



cannot evaluate DoD strategy and programming in isolation, it clearly must be a whole-of-government approach.

Following are the Task Force recommendations:

**The President should ensure the CVE Interagency Coordination Group (ICG)—chaired by the Global Engagement Group at the National Counterterrorism Center—advances an overarching, multilateral strategy for CVE abroad. The ICG would:**

- Strengthen the coordination process (i.e., connective tissue) between actors to improve cooperation and increase agility against the transnational CVE threat. To the extent current U.S. CVE efforts are organized by country, our efforts will miss the crucial regional nature of the CVE phenomenon.
- Maximize efficiencies by matching CVE responsibilities to authorities, resources, and accesses.
- Facilitate decentralization of the CVE strategy’s implementation by those representing the U.S. on the ground. CVE will not succeed with centralized operational control from the highest reaches of the USG.
- Refine the formula for recognizing and correcting potential implementation errors—without overreaction. Likely errors include programs that do not work (e.g., wasteful expenditure of funding) or programs that backfire (e.g., culturally insensitive programming).
- Institutionalize the following components of a successful CVE strategy abroad:
  - Strengthen or build institutions, particularly police and law enforcement. It is difficult to overstate the role that ineffective—indeed, often corrupt and predatory—governments play in providing an environment in which violent extremism can flourish. The USG should attempt wherever possible to work with other governments in building these institutions, deferring as appropriate to their standing expertise, even if it leads to approaches that would not be the U.S. first choice.
  - Provide meaningful economic opportunities to potentially disaffected youths to limit the pool of followers/adherents from which extremism can draw, and thus circumscribe the reach and consequences of those who would pursue violent extremism. However, emphasis on broad economic development (e.g., building dams, infrastructure) as a CVE strategy is misplaced.
  - Undertake humanitarian efforts as an important building block in a CVE strategy.
  - Develop messages to address all violent extremist ideologies—not just Sunni narratives—and tailor the messages and the delivery method to a local context.

- Support our messages with our actions, and our actions with our messages.

**The CVE Interagency Coordination Group, with Department of State in the lead, should take action to continuously improve understanding of CVE, to use that improved understanding to establish measureable goals and metrics for CVE, and to use these goals and metrics to guide prioritization of actions and allocation of resources.**

- Conduct a major analytic effort to better understand the complex issues associated with the “funnel” this report notes. This result will be critically important to reducing long-term risks to the U.S.
- Improve assessment of CVE programs and institutionalize findings through the following initiatives:
  - Continuously refine evaluation methods for CVE grounded in historical evidence/case studies providing insight into the causes of violent extremism and successful antidotes. Among past examples that might be studied are the Irish-British struggle, the Khmer Rouge in Cambodia, the Balkans (most recently in the 1990s), Rwanda, the Congo since independence, Sudan in the last two decades, and Palestine and its long aftermath.
  - Survey experts on effective measures for CVE programs.
  - Survey afflicted populations and correlate findings with CVE effects; although, this will not establish causality.
  - Borrow from commercial utilization of data and measurement tools, to include analysis of Big Data.

**The Secretary of Defense should clarify the role of the ASD/SO/LIC, or the Departmental officer of his choice, to explicitly develop, promulgate, and coordinate the DoD CVE strategy. This individual would:**

- Serve as DoD liaison to interagency CVE efforts, vetting requests for DoD CVE support. DoD leadership for CVE should be limited to tasks central to DoD’s mission and best supported by DoD’s authorities and resources.
- Develop a mechanism to transition leadership of other CVE functions to more appropriate actors, in the event DoD has undertaken these tasks as a critical interim gap filler.
- Identify opportunities for the DoD to support CVE tasks undertaken by other agencies and partners in a manner consistent with DoD mission, authorities, and resources. For example, DoD could provide security support to agricultural teams, but should not provide agricultural development assistance.

- Integrate CVE into COCOM mission planning, including all relevant activities within theater engagement plans. CVE should not be a standalone activity or one that is not coordinated with other elements of theater engagement plans. COCOM planning should incorporate CVE into peacetime activities—including Phase Zero/shaping tasks—not just wartime, and should embed CVE goals when building partnership capacity.
- Ensure that plans for counterinsurgency (COIN)/Stability Operations incorporate the classic principle: First, do no harm (re: CVE). When those plans are triggered, monitor their execution to buttress this principle.
- Foster linkages for CVE planning between COCOMs and between COCOMs and DoS partners in theater. Successful CVE cannot occur in a stovepipe: coordination starts with an enabling strategy for CVE cooperation and then flows down to those on the ground.
- Examine the funding and resourcing mechanisms for CVE to identify opportunities to support DoD CVE initiatives beyond ad hoc, one-off allocations at the request of the combatant commander.
- Cultivate institutional knowledge and education in CVE across the Department to fortify a “do no harm approach” which is sensitive to cultural context and the messages our words and actions send.
  - Work to improve the cultural competence of future DoD leaders, so they can understand the context of the operations they will lead. For officers this should start as officer candidates and continue throughout their careers; senior non-commissioned officers should be included as they are prepared for advancement. The emphasis should be on deep preparation in one or more specific cultures, rather than generic training.
  - Seek to modify the personnel system to keep track of who is prepared in which area, to enable them to be reassigned as the need arises. Volunteering should be the first principle in assigning areas of specialization, but incentives to focus on areas where staffing falls short should be considered.
  - Advocate continued investment in foreign leaders via War Colleges—adding opportunities for civil leaders—in order to cultivate partners for DoD’s approach to CVE.

# Introduction

## Scope Note

In May 2011, Congress tasked the Chairman of the Defense Science Board (DSB) to establish a Task Force on Department of Defense (DoD) Strategy to Counter Violent Extremism (CVE) Outside of the United States (“Task Force”). The Task Force members were asked to assess the following areas of interest related to the DoD’s CVE strategy outside of the United States:

1. A review of the current strategy, research activities, resource allocations, and organizational structure of the DoD for CVE outside of the United States;
2. A review of interagency coordination and decision making processes for executing and overseeing strategies and programs for CVE outside the United States;
3. An analysis of alternatives and options available to the DoD for CVE outside of the United States;
4. An analysis of legal, policy, and strategy issues involving CVE efforts outside of the United States as such efforts potentially affect domestic efforts to interrupt radicalization efforts within the United States;
5. An analysis of the current DoD information campaign against violent extremists outside of the United States;
6. Such recommendations for further action to address the matters covered by the report as the DoD considers appropriate; and
7. Such other matters as the DSB determines relevant.

The Task Force convened a series of meetings to receive briefings on this topic from subject matter experts in the DoD, broader USG, think tanks, and academia. A list of the offices and entities the Task Force received briefings from is at Appendix C. The Task Force focused its discussions and this report on what it believes are the most salient, current CVE issues for DoD, within the broad Terms of Reference.

The breadth of this endeavor is apparent in the variety of “CVE” definitions and scopes found in the literature, used by our briefers, and embodied in government documents. To the extent there are commonalities among definitions of CVE, the Task Force focused on violent extremism generally targeting innocent civilians, vice combatants. This definition includes a full range of activities related to CVE, from countering inspiration and radicalization, to building community resilience and law-enforcement capacity, to countering extremist messaging. The Task Force considers analysis of kinetic operations outside the scope of this report.

It is also important to note that diverse actors—from USG agencies outside the DoD, to host nation leadership, to non-governmental organizations—play a critical and oftentimes lead role in CVE. In fact, in most cases DoD is in a supporting, vice leading role, for most CVE

activities. However, this Task Force focuses its analysis on DoD CVE activities; references to non-DoD initiatives are limited to information that provides context for DoD CVE activities.

The Guidance for Employment of the Forces (GEF) and the Joint Strategic Capabilities Plan (JSCP) focus on shaping and stabilizing the global environment so it is inhospitable to violent extremism by: enabling partners to combat violent extremist organizations; deterring tacit and active support to extremist organizations; and eroding support for extremist ideologies. DoD capabilities to accomplish this guidance include foreign internal defense, security force assistance, civil military operations, and military information support operations.

However, for nearly all of these activities (without a deployment or execution order), the DoD is generally in a supporting role for U.S. and Coalition efforts. The level of effort and intensity of these activities vary by region and political circumstances, and the pace of operations is generally set by the Department of State (DoS), working through the host nation government. Coordination on CVE between the DoD and inter-governmental partners occurs in-country at U.S. embassies, at the National Security Strategy Communication Interagency Policy Committee (IPC), the Global Engagement IPC, the Counterterrorism (CT) Security Group, the CVE Interagency Coordination Group (ICG), and the Senior Interagency Support Team.

The Task Force observes that the definition of CVE activities is ad hoc and fluid, budgeting is often piecemeal and difficult to track, and it is challenging to measure and evaluate what is success in CVE.

## **The CVE Challenge**

Violent extremism at the small group or individual level is nearly impossible to predict. The radicalization<sup>1</sup> process can be likened to a very wide and very tall funnel: certain conditions (inequality and injustice, for example) may predispose groups of people to radicalization, while enablers of radicalization (such as weak governance or lack of alternatives) may push some individuals further along in the process, and catalysts (such as opportunity for violence) may drive people still further. There is, however, no method to predict which individual will mobilize and emerge from the funnel as a violent extremist.

Because of this challenge, and the myriad circumstances that may influence radicalization (e.g., populations, cultures, economic conditions), it is extremely difficult to mount CVE interventions at scale. Even if one could be persuaded that a customized, targeted intervention prevented a certain person from becoming a violent extremist, the intensity and focus of that effort could not be applied at large scale—reflecting the diversity of motivations, grievances, conditions, and goals across even a modestly sized community. Thus the “eaches” pile up to something that overwhelms every conceivable remedial course of action.

---

<sup>1</sup> Radicalization is defined as the process by which individuals come to believe that their engagement in or facilitation of non-state violence to achieve social and political change is necessary and justified.



Moreover, violent extremism does not operate in a vacuum or even in one place; it occurs in the context of evolving current events, which makes it even more difficult to counter. Today's networked and oftentimes instantly interconnected environment can expedite the radicalization process, exposing many vulnerable populations to ideas and opportunities that might push them further along the radicalization process and provide them with an outlet for violent extremism. For example, what started as a geographically contained radicalization funnel in Iraq and Syria now draws fighters from around the world; as violent extremists concentrate in these regions, they grow stronger and more problematic.

# Understanding Extremism

*“There is no effective formula for predicting violent behavior with any degree of accuracy.” DSB Task Force on Predicting Violent Behavior at Page 2 (August 2012)*

## Discussion

There is no single template or standard progression by which individuals become radicalized or decide to engage in violence. There is no uniform process against which the USG can track an individual except in the grossest terms. An overview of factors influencing radicalization follows; it is not exhaustive.

- **Personal factors:** The interaction of personality traits (individual characteristics, drivers, and needs) and contextual and situational factors such as a person’s demographic background and history may make an individual vulnerable to radicalization.
- **Group factors:** Becoming part of a larger entity which shares a set of collective grievances helps lower individuals’ thresholds for participation in extremist activities, to include—for some—the use of violence.
- **Community factors:** When grievances such as alienation or religious discrimination, combine with insularity, isolation, and lack of trust in societal and political institutions, they can create the conditions that encourage a small minority to adopt a radical ideology. The situation is often aggravated by charismatic ideologues.
- **Sociopolitical factors:** Political and societal level conditions, events, and grievances can help drive an individual to seek an ideological explanation or reinforce existing beliefs. For example, drivers could include political disenfranchisement or economic inequality.
- **Ideological factors:** Ideology provides individuals with an interpretive framework for world and life events, as well as a set of values, beliefs, and goals for a movement or social entity. It also establishes the rationale for individual and collective action. In some cases, violent extremist ideology is linked to religious beliefs; although, religion in and of itself is not a cause of violent extremism.

It is important to note that DoD activities—from detention operations, to CT, to stability operations—might feed into perceptions of grievances by causing collateral damages. One of the most important issues for the DoD is reducing the chances that U.S. military activities feed the radicalization the USG is trying to counter. As the 2006 COIN manual states: “an operation that kills five insurgents is counterproductive if collateral damage leads to the recruitment of fifty more insurgents.”

After an individual becomes radicalized, catalysts such as social media, familiar and social networks, and financial incentives can shift him or her toward mobilization to violent extremism, while inhibitors such as law enforcement, community outreach, credible voices, or family might blunt the move toward violent extremism. The final steps to becoming a violent extremist will often hinge on opportunity and capability to act, and access to a target.

In any given environment, with any given individual, the radicalization mechanism is often unknown and almost always unpredictable. For some, the radicalization process can take years and will never result in violent extremism. For others, the transformation to violent extremism can occur suddenly. Although some factors—such as grievances or an explanatory violent narrative—are common among the radicalization paths of most individuals, by themselves they do not explain why one individual will turn to violence and another does not. No single factor fully explains the radicalization process of any particular individual. Moreover, factors often interact; if examined independently they will usually fail to provide insight into the most likely causes of violent extremism.

## Findings

Current USG efforts are focused on countering violent Sunni narratives (e.g. Al Qaeda, Da'esh) with little attention to other violence-inspiring narratives (extant or anticipated). The challenge is, however, not limited to Sunni narratives but extends to radical ideologies more broadly. Radical ideologies diagnose and place blame for injustices, and then provide the justification and roadmap for an immediate response. Radical ideologies can prod individuals to act and justify the right to use violence. Motivational guidance helps potential recruits overcome apathy, fears, and aversion to violence.

Effective CVE requires an examination of radical ideologies *writ large* to identify commonalities; however, radical ideology also needs to be understood in the specific context. While certain themes endure, the context in which those themes occur varies. This local context frames and shapes an ideology and makes it resonate for potential violent extremists.

Although the United States can better shape and focus its efforts to more broadly and effectively counter violent extremist ideology, these initiatives are likely insufficient to counter violent extremism absent efforts to ameliorate other radicalizing factors. Efforts to eliminate only the transmission of these ideas are likely to fail and, thus, insufficient to counter the radical ideology without addressing the broader context.

Individuals and groups prone to radicalization have modified or adopted new radical ideologies to meet their ends. For example, Da'esh's radical ideology has been revised by its adherents, and remains salient despite rejection of the group by its parent, Al Qaeda. Moreover, Sunni groups have shown tremendous flexibility to confer ad hoc legitimacy; the rise of new influential individuals within radical ideologies demonstrates their resilience. The resilience of radical ideologies and the persistence of other drivers of radicalization suggest that extremism

may be likened to a chronic disease. Therefore, U.S. CVE efforts abroad should focus on keeping the disease in check.

Further, there is no one solution to counter violent extremism. Even if it were possible to prove that a particular approach were effective, it would have to be modified in whole or in part to be applied in other environments. It will always be a struggle to find appropriate mechanisms to respond to unknowable, diverse circumstances.

# CVE Strategy, Roles, and Programming

## Discussion

There are no Presidential directives outlining a national strategy for U.S. CVE efforts abroad. The 2011 *National Strategy for Counterterrorism* treats CVE—and related activities such as countering radical ideologies and building partner capacity for law enforcement—as subsets of counterterrorism (CT) strategies aimed at Al Qaeda.

The strategy emphasizes a “whole of government” approach by integrating the capabilities and authorities of each department and agency to foster a rapid, coordinated, and effective counter to terrorism/violent extremism. The strategy also calls on the United States to work with multilateral institutions and partners at the international, regional, and sub-regional levels to increase legitimacy. Finally, the strategy plans to counter violent extremist ideologies while promoting U.S. ideals.

With the recent uptick in violent extremist activities in Syria and Iraq, President Obama has increased his public emphasis on CVE and CT. President Obama’s September 2014 United Nations speech called violent extremism a “cancer” that has—despite the best U.S. efforts—expanded to the Middle East and North Africa. The President called on the international community to collectively counter violent extremism through four efforts (some of which are kinetic):

1. Degrading and ultimately destroying Islamic State of Iraq and the Levant (ISIL) through support to partner nations, air strikes, and limits on financing and travel;
2. Countering the violent extremist ideology through strategic communication and bolstering moderate ideological alternatives;
3. Ending the cycle of violent sectarian conflicts that feed extremism, for example in Syria; and
4. Bolstering opportunities for at-risk populations, particularly youth.

Shortly after President Obama’s UN speech, the U.S. supported a resolution condemning violent extremism and underscoring the need to prevent travel and support for foreign terrorist fighters. As of publication, there is still no overarching strategy per se driving USG CVE activities abroad.

Although this report primarily focuses on reviewing DoD strategy to counter violent extremism abroad, DoD does not operate in a vacuum. CVE requires a whole-of-government approach. Therefore, evaluating DoD CVE strategy requires understanding DoD’s role in broader USG CVE initiatives. Additionally, the Task Force Terms of Reference (at Appendix A) calls for a review of interagency coordination and decision making processes for executing and overseeing



strategies and programs for CVE outside the United States. A review of USG CVE initiatives can be found at Appendix E.

### **CVE in DoD**

There is no DoD strategy or directive on CVE per se, although the 2014 *Quadrennial Defense Review* (QDR) touches on CVE broadly. The QDR lists CVE—particularly in the Middle East and Africa—as defense priority number 3 (out of 5). According to the QDR, the United States will maintain a worldwide approach to CVE and terrorist threats using a combination of economic, diplomatic, intelligence, law enforcement, development, and military tools. There will be a greater DoD emphasis on building partnership capacity—especially in fragile states—while retaining robust capability for direct action, including intelligence, persistent surveillance, precision strike, and special operations forces.

The GEF and JSCP provide principal planning guidance for CT; CVE is included as an aspect of CT. Guidance is encapsulated in *Joint Publication 3-26*, summarized below:

*The National Strategy is to defeat violent extremism as a threat to our way of life as a free and open society, and create a global environment inhospitable to violent extremists and all who support them. As such, we will continue to lead an international effort to deny violent extremist networks the resources and functions they need to operate and survive. There are three key elements that represent the critical efforts for achieving success: protecting and defending the homeland; attacking terrorists and their capacity to operate effectively at home and abroad; and supporting mainstream efforts to reject violent extremism.<sup>2</sup>*

To support mainstream efforts to reject violent extremism, planning guidance focuses on shaping and stabilizing the global environment so it is inhospitable to violent extremism by: enabling partners to combat violent extremist organizations (VEOs); deterring tacit and active support for VEOs; and eroding support for extremist ideologies. The following military capabilities can help accomplish these tasks (this list is not exhaustive):

- **Foreign Internal Defense (FID):**<sup>3</sup> FID conducted by conventional forces and special operations forces (SOF) can help the host nation reduce contributing factors to terrorism such as subversion, lawlessness, and insurgency. The FID strategy focuses on building viable political, economic, military, security infrastructure, and social institutions for the

---

<sup>2</sup> Planning guidance provides for direct and indirect approaches to accomplish this strategy. The direct approach requires the USG to directly act against terrorists and their organizations to neutralize an imminent threat and degrade the operational capability of a terrorist organization. The line between CT and CVE is blurred both in theory and in practice. Distinctions drawn between CT and CVE in this study are to facilitate analysis of CVE, and are not intended to reflect doctrinal or policy recommendations.

<sup>3</sup> FID is the participation by civilian and military agencies of a government in any of the action programs taken by another government or designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats. (JP3-22)

needs of the local population. FID operations involve military training and building infrastructure (e.g., schools, roads, wells) in conjunction with foreign aid programs administered by DoS.<sup>4</sup>

- **Security Force Assistance (SFA):** SFA encompasses joint force activities conducted within unified action to train, advise, assist, and equip foreign security forces in support of a partner nation's efforts to generate, employ, and sustain local, host nation, or regional security forces and their supporting institutions.
- **Civil Affairs Operations (CAO):** CAO facilitates Civil Military Operations (CMO), which in turn support the overall operation/campaign by enhancing the relationship among military forces, civil authorities, and the private sector in functional specialty areas (e.g., governance, economic stability, infrastructure).
- **Military Information Support Operations (MISO):**<sup>5</sup> MISO, previously Psychological Operations (PSYOP), along with Information Operations (IO),<sup>6</sup> Public Affairs (PA), Public Diplomacy (PD), and Strategic Communication (SC) more broadly, can also contribute to CVE. See the Section entitled "Strategic Communication" for detailed discussion of DoD's messaging contributions to CVE.

The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SO/LIC)) is responsible for the development, coordination, and oversight of the implementation of policy and plans for DoD participation in all USG CT activities, including programs designed to counter violent extremism. U.S. Special Operations Command (USSOCOM) is the global synchronizer for the war on terrorism and is responsible for synchronizing planning, and as directed, executing operations against terrorist networks on a global basis in coordination with other combatant commands, the Services, and appropriate USG agencies.

For U.S. and Coalition CVE efforts, DoD is generally in a supporting role. The level of effort and intensity of these activities varies by region and political circumstances, and the pace of operations is generally set by the DoS, working through the host nation government. Activities

---

<sup>4</sup> JP 3-26 acknowledges that bolstering the will of other states to fight terrorism is primarily the responsibility of the DoS; however, it suggests that effective FID programs can improve public perceptions of the host nation and U.S. military. Additionally, military-to-military contacts can help make host nation officials advocates of potential operations against terrorist capabilities.

<sup>5</sup> MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. MISO are used to establish and reinforce foreign perceptions of U.S. military, political, and economic power and resolve.

<sup>6</sup> IO is defined in DoD Directive 3600.01 as the integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations (now MISO), Military Deception, and Operations Security, in concert with specific supporting and related capabilities to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

range from supporting the U.S. embassy and DoS plans and programs, to supporting efforts to persuade and influence populations. There is a Senior Defense Official at every U.S. embassy; he or she is required to inform the embassy of DoD operations and positions.

In fostering interagency coordination, DoD is represented at the National Security Council Staff Strategic Communication IPC, the Global Engagement IPC, and the CT Security Group. The DoD also participates in the CVE ICG and the Senior Interagency Support Team chaired by the National Counterterrorism Center (NCTC).

## **Authorities**

Without a deployment or execution order from the President or Secretary of Defense, U.S. forces may be authorized to make only limited contributions during operations that involve Foreign Internal Defense. The request and approval may go through standing statutory authorities in Title 22, USC, which contains the Foreign Assistance Act (FAA) and Arms Export Control Act authorizing security assistance, developmental assistance, and other forms of aid. The request and approval might also occur under various provisions in Title 10, USC, which authorizes certain types of military-to-military contacts, exchanges, exercises, and limited forms of humanitarian and civic assistance in coordination with the U.S. ambassador in the host nation. This cooperation and assistance is limited to liaison, contacts, training, equipping, and providing defense articles and services. It does not include direct involvement in operations.

Generally, DoD is not the lead government department for assisting foreign governments. DoS is the lead when U.S. forces provide security assistance—military training, equipment, and defense articles and services—to host nation military forces. All training and equipping for foreign security forces must be specifically authorized by Congress. U.S. law also requires the DoS to verify that the host nation receiving the assistance does not commit gross violations of human rights. Usually, DoD involvement is limited to a precise level of man hours and materiel requested by DoS under the FAA. The President may authorize deployed U.S. forces to train or advise host nation security forces as part of the mission. Absent a Presidential directive for DoD’s “train and equip” efforts, DoD lacks authority to take the lead in assisting a host nation in training and equipping its security forces.

## **Findings**

There is no overarching USG strategic framework for CVE, nor are activities coordinated under coherent policy goals across the whole of the USG, let alone DoD. There is no clarifying, single focus of instruction or budgetary unity. Perhaps this is because the full scope of what is really CVE is challenging—especially because it means different things to different organizations and, therefore, warrants different programmatic inputs.

Moreover, within the DoD, there is no clear, common definition of CVE and no overarching strategy for where DoD fits within that definition. This risks the implementation of CVE functions into DoD roles and missions could be piecemeal and ad hoc. The Task Force saw little

evidence that, below the Secretary of Defense, there is a single responsible person or organization from which or to which direction is flowing, guiding the combatant commanders on allocating resources and focusing attention on CVE.

Beyond—but linked closely with—definitional challenges, there is uncertainty within the DoD and USG *writ large* about the appropriate DoD role within CVE. In the last couple of years, the DoD has begun to exercise a direct role in CVE—in part because its operational actions comprise part of the CVE space. However, the DoD lacks a strategic framework for how it should fit into a broader, USG CVE approach: which tasks are best accomplished by the DoD, which are best undertaken by others, and which should be approached holistically through an interagency process.

CVE is a diversified problem across theaters, capabilities, and motivations. It is a spectrum of activity within which DoD's responsibilities are relatively narrow compared to the responsibilities of other organizations. DoD's CVE role outside of a committed theater of operations is likewise unclear. Even in theater and beyond Phase Zero—and even Phase One—there are gaps, overlaps, and conflicts among MISO and Information Operations (IO) in terms of the CVE activities and goals, and even between Public Affairs (PA) and IO activities (see section on Strategic Communication).<sup>7</sup> Moreover, DoD CVE funding is distributed among the commands, not centralized, and that funding appears to be not well coordinated.

The Task Force acknowledges that there is a natural inclination to turn to DoD for CVE because it has developed the command and control mechanisms to operate at scale—especially overseas. DoD is expeditionary, mission-oriented, risk accepting, has very high-quality personnel, is well resourced, and has historically filled critical gaps. However, DoD may not be the right organization—in terms of authority, capabilities, and/or expertise—to carry out many of the CVE tasks, particularly over the longer term. As DoD transitions away from large-scale deployments with combat missions, it will be important to specify which CVE responsibilities it should lead, and which it should support.

While non-governmental organizations (NGOs) may play a significant role in societies burdened by violent extremism, effective engagement by the USG with NGOs is ad hoc at best. Where DoD—and the USG more broadly—has little capacity, credibility, or authority to counter violent extremism, CVE efforts will depend on USG relationships with actors that have

---

<sup>7</sup> According to JP5-0, a phase is a definitive stage of an operation of campaign during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose. Phase Zero consists of shaping activities to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies. They are designed to ensure success by shaping perceptions and influencing the behavior of both adversaries and partner nations, developing partner nation and friendly military capabilities for self-defense and multinational operations, improving information exchange and intelligence sharing, and providing U.S. forces with peacetime and contingency access. Phase One consists of actions to deter undesirable adversary action by demonstrating the capabilities and resolve of the joint force. It includes activities to prepare forces and set conditions for deployment and employment of forces in the event that deterrence is not successful.

capabilities to address those issues of concern. More effort will be needed to strengthen these relationships.



# Measuring the Effectiveness of CVE

## Discussion

It is challenging to measure the effectiveness of CVE because it is difficult to identify which factors in any given context may lead to violent extremism in particular individuals. It is even more difficult to monitor and evaluate the success of targeted interventions on these personal and contextual factors. Often inputs and/or outputs are not quantifiable. Moreover, a successful outcome is a non-event (absence of violent extremist actions) and therefore nearly impossible to prove. For these reasons, the body of evaluative work too often relies on qualitative research comprised of anecdotal evidence and surveys.

Challenges monitoring and evaluating the effectiveness of CVE narrative programs reflect the broader difficulty of measuring CVE success. The USG can measure the number of views a counter-message receives online. It may even be able to see who has viewed the message and whether the person has forwarded the message to others. However, it cannot reliably measure whether that message has resonated with any individuals. The USG only knows its message was seen, but not whether the message changed minds.

This challenge is compounded when extrapolating from the individual to the group. While it might be understood whether a particular CVE intervention worked for a given person—based on surveys or anecdotes—whether the intervention reduced violent extremism in a larger population cannot be measured with any reliability. The USG can look broadly, over time, at whether the incidence of violent extremism has decreased in a population; however, it should not assume correlation equals causation and that any particular intervention has caused the reduction. Moreover, the further away from traditional CT missions one gets (e.g., capacity building, development, counter-ideological messaging), the more difficult it is to evaluate the effectiveness of CVE in reducing violence.

## Findings

The Task Force notes that much research and investment has gone into trying to measure CVE effectiveness. However, the Task Force found no evidence demonstrating that CVE has been measured effectively. This lack of reliable and agreed upon measures of effectiveness/ineffectiveness (and the data inputs for those measures) impairs DoD's ability to determine which CVE activities warrant which level of funding. At the same time, the Task Force recognizes that just because CVE effectiveness cannot be measured does not mean it is necessarily ineffective. The lack of metrics should not preclude DoD from undertaking CVE programming, but does warrant further inquiry.

# CVE through Messaging

## Discussion

There is a widespread view by practitioners that messaging/counter-messaging can reduce violent extremism. Our review of CVE reveals the preference of many for “messaging” as an important CVE instrument. This report has already provided an overview of DoS messaging programs. Below, this report reviews DoD Strategic Communication (SC), which aims expressly or implicitly to counter violent extremism.

## Strategic Communication

SC is the focused USG effort to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancements of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. While there are no Presidential directives specifically outlining U.S. CVE strategy abroad, the *National Framework for Strategic Communication*, lays out interagency coordination for public diplomacy and strategic communication—a key activity supportive of CVE. The strategy calls for synchronizing words and deeds—including actively considering how U.S. actions and policies will be interpreted—as well as deliberate efforts to communicate and engage with intended audiences. In general, communications should emphasize mutual respect and interest to foreign audiences; U.S. communications related to U.S. CVE efforts should focus more directly on discrediting, denigrating, and delegitimizing Al Qaeda and violent extremist ideology.

The DoD SC objectives in the war on terrorism are to: support partner nations; convert moderates to become partner nations; weaken sympathy and support for violent extremist organizations; provide support to moderate voices; dissuade enablers and supporters of extremists; counter ideological support for terrorism; and deter and disrupt terrorist acts. DoD SC uses the functions of PA, defense support to public diplomacy (DSPD), military diplomacy, MISO, and IO. Combatant commanders receive their SC guidance from and coordinate their SC activities with various offices in the Office of the Secretary of Defense (OSD). The integration and oversight of DoD policy and plans to achieve national security objectives flows from the Secretary of Defense to the Under Secretary of Defense for Policy (USD(P)). The Office of the Deputy Assistant Secretary of Defense for Plans has the primary responsibility, in close coordination with the Office of the USD(P) Global Strategic Engagement Team (GSET)<sup>8</sup> and Office of the Assistant Secretary of Defense for Public Affairs, for ensuring that guidance for Strategic Communication is included in strategic planning guidance documents, such as the GEF and Global Force Posture, and for reviewing COCOM plans directed by the GEF to ensure

---

<sup>8</sup> The Global Strategic Engagement Team is tasked with facilitating the strategic communication process within OUSD(P) and liaising with other DoD components as appropriate.

strategic communication considerations have been integrated into the plans. A more detailed delineation of leadership for SC is at Appendix F.

National-level interagency coordination of Strategic Communication takes place in the Strategic Communication IPC, led by the NSC staff. The Deputy National Security Advisor for Strategic Communications is responsible for ensuring the message value and communicative impact of actions are considered during decision-making and the mechanisms to promote strategic communication are in place within the NSC staff and are developed across the interagency.

At the operational level, the Country Team and the Joint Interagency Coordination Group (JIACG) are the two standing interagency coordination bodies. The Country Team, headed by the chief of the U.S. diplomatic mission, is the USG's senior coordinating and supervising body in-country. The JIACG is established at each Geographic Combatant Command headquarters and coordinates with the USG civilian agencies to conduct operational planning; however, the JIACG has no operational authority.

## Findings

There is no agreed upon method(s) to evaluate on a firm basis upon which to measure the impact of counter-messaging on the conduct of individuals or groups. As previously discussed, the USG may be able to quantify whether an individual has read a message, but it has difficulty evaluating resonance. Beyond anecdotal evidence and surveys, the Task Force has not found any reliable methods for gauging resonance—particularly on a group.

Assuming we can measure outputs effectively, the Task Force assumes that successful USG messaging programs will be based on broad themes, but tailored to the local context—both in terms of content and delivery. Indeed, targeted messaging requires sophisticated knowledge of local issues, groups, and leaders. Messages will need to address and counter diverse drivers of violent extremism in disparate environments. The challenge is not only understanding the relevant radical ideologies and narratives in any given context, but identifying authoritative actors (often religious figures) who confer legitimacy on these narratives. Leveraging or discrediting these legitimate actors will be key for countering radical ideology through messaging. Moreover, the means of communication (computer, SMS, paper) will vary based on location, depending on the proliferation of technology. In contrast, the broader the messaging—which is suited to a general audience—the less valuable it is in altering the attitudes or actions of discrete individuals who are already disposed to violent activity.

Moreover, coordinating messaging programs across the DoD is key for avoiding inconsistency or hypocrisy; however, timeliness of communications is also critical. The current structure for coordinating CVE Strategic Communication requires combatant commanders to liaise with USSOCOM, various nodes in OSD, and the DoS before dissemination. In contrast, violent extremists have few—if any—coordination requirements; their decentralized communications model provides them with flexibility to rapidly generate relevant messages. U.S. coordination requirements—coupled with complicated requirements for attribution—therefore hamper our

ability to win a tactical counter-messaging campaign. Attempts to improve and enhance our messaging coordination within the DOD—and the interagency and non-government community *writ large*—are essential, but should be accomplished with an eye towards efficiency and timeliness.

It is clear to the Task Force that actions speak louder than words. Actions create messaging that may not be part of any larger thought about the U.S. image. Combatant commanders create messages with their actions. Exercises can send messages that may not be desired with respect to extremism. The U.S. partnering with country militaries also sends a message, especially if the military is resented. Even U.S. choices for basing locations send messages. The U.S. goal should be to align our actions with our messages.

In some cases, however, the Task Force recognizes that the USG may have difficulty aligning its actions with its messages. Military missions sometimes require actions that may undermine U.S. CVE messaging, and may even feed the violent extremist narrative. For example, personnel providing humanitarian and disaster relief while wearing necessary body armor, may in some cases be a negative and diminish the “good” message about U.S. assistance. The USG needs to always consider its messaging as it frames its actions so as to rightly characterize our motivations.<sup>9</sup>

---

<sup>9</sup> The DSB has reviewed USG Strategic Communication in three Task Forces: DSB Task Force on the Creation and Dissemination of All Forms of Information in Support of PSYOP in Time of Military Conflict (May 2000); DSB Task Force on Strategic Communication (September 2004); and DSB Task Force on Strategic Communication (January 2008). Please see final Task Force reports for additional, supporting insights into Strategic Communication.

## Task Force Recommendations

This Task Force understands that successfully countering violent extremism abroad requires a multilateral approach in which the USG needs to leverage its diverse partnerships to bring a complementary package of authorities, resources, and expertise to bear against this challenging and evolving threat.

Although this Task Force was charged with evaluating DoD CVE efforts (outside the United States), the necessity of a collaborative CVE approach dictates that we cannot evaluate DoD strategy and programming in isolation.

Following are the Task Force recommendations:

**The President should ensure the CVE Interagency Coordination Group (ICG)—chaired by the Global Engagement Group at the National Counterterrorism Center—advances an overarching, multilateral strategy for CVE abroad.** The ICG would:

- Strengthen the coordination process (i.e., connective tissue) between actors to improve cooperation and increase agility against the transnational CVE threat. To the extent current U.S. CVE efforts are organized by country, our efforts will miss the crucial regional nature of the CVE phenomenon.
- Maximize efficiencies by matching CVE responsibilities to authorities, resources, and accesses.
- Facilitate decentralization of the CVE strategy’s implementation by those representing the U.S. on the ground. CVE will not succeed with centralized operational control from the highest reaches of the USG.
- Refine the formula for recognizing and correcting potential implementation errors—without overreaction. Likely errors include programs that do not work (e.g., wasteful expenditure of funding) or programs that backfire (e.g., culturally insensitive programming).
- Institutionalize the following components of a successful CVE strategy abroad:
  - Strengthen or build institutions, particularly police and law enforcement. It is difficult to overstate the role that ineffective—indeed, often corrupt and predatory—governments play in providing an environment in which violent extremism can flourish. The USG should attempt wherever possible to work with other governments in building these institutions, deferring as appropriate to their standing expertise, even if it leads to approaches that would not be the U.S. first choice.

- Provide meaningful economic opportunities to potentially disaffected youths to limit the pool of followers/adherents from which extremism can draw, and thus circumscribe the reach and consequences of those who would pursue violent extremism. However, emphasis on broad economic development (e.g., building dams, infrastructure) as a CVE strategy is misplaced.
- Undertake humanitarian efforts as an important building block in a CVE strategy.
- Develop messages to address all violent extremist ideologies—not just Sunni narratives—and tailor the messages and the delivery method to a local context.
- Support our messages with our actions, and our actions with our messages.

**The CVE Interagency Coordination Group, with Department of State in the lead, should take action to continuously improve understanding of CVE, to use that improved understanding to establish measureable goals and metrics for CVE, and to use these goals and metrics to guide prioritization of actions and allocation of resources.**

- Conduct a major analytic effort to better understand the complex issues associated with the “funnel” this report notes. This result will be critically important to reducing long-term risks to the U.S.
- Improve assessment of CVE programs and institutionalize findings through the following initiatives:
  - Continuously refine evaluation methods for CVE grounded in historical evidence/case studies providing insight into the causes of violent extremism and successful antidotes. Among past examples that might be studied are the Irish-British struggle, the Khmer Rouge in Cambodia, the Balkans (most recently in the 1990s), Rwanda, the Congo since independence, Sudan in the last two decades, and Palestine and its long aftermath.
  - Survey experts on effective measures for CVE programs.
  - Survey afflicted populations and correlate findings with CVE effects; although, this will not establish causality.
  - Borrow from commercial utilization of data and measurement tools, to include analysis of Big Data.

**The Secretary of Defense should clarify the role of the ASD/SO/LIC, or the Departmental officer of his choice, to explicitly develop, promulgate, and coordinate the DoD CVE strategy. This individual would:**

- Serve as DoD liaison to interagency CVE efforts, vetting requests for DoD CVE support. DoD leadership for CVE should be limited to tasks central to DoD’s mission and best supported by DoD’s authorities and resources.
- Develop a mechanism to transition leadership of other CVE functions to more appropriate actors, in the event DoD has undertaken these tasks as a critical interim gap filler.
- Identify opportunities for the DoD to support CVE tasks undertaken by other agencies and partners in a manner consistent with DoD mission, authorities, and resources. For example, DoD could provide security support to agricultural teams, but should not provide agricultural development assistance.
- Integrate CVE into COCOM mission planning, including all relevant activities within theater engagement plans. CVE should not be a standalone activity or one that is not coordinated with other elements of theater engagement plans. COCOM planning should incorporate CVE into peacetime activities—including Phase Zero/shaping tasks—not just wartime, and should embed CVE goals when building partnership capacity.
- Ensure that plans for counterinsurgency (COIN)/Stability Operations incorporate the classic principle: First, do no harm (re: CVE). When those plans are triggered, monitor their execution to buttress this principle.
- Foster linkages for CVE planning between COCOMs and between COCOMs and DoS partners in theater. Successful CVE cannot occur in a stovepipe: coordination starts with an enabling strategy for CVE cooperation and then flows down to those on the ground.
- Examine the funding and resourcing mechanisms for CVE to identify opportunities to support DoD CVE initiatives beyond ad hoc, one-off allocations at the request of the combatant commander.
- Cultivate institutional knowledge and education in CVE across the Department to fortify a “do no harm approach” which is sensitive to cultural context and the messages our words and actions send.
  - Work to improve the cultural competence of future DoD leaders, so they can understand the context of the operations they will lead. For officers this should start as officer candidates and continue throughout their careers; senior non-commissioned officers should be included as they are prepared for advancement.



The emphasis should be on deep preparation in one or more specific cultures, rather than generic training.

- Seek to modify the personnel system to keep track of who is prepared in which area, to enable them to be reassigned as the need arises. Volunteering should be the first principle in assigning areas of specialization, but incentives to focus on areas where staffing falls short should be considered.
- Advocate continued investment in foreign leaders via War Colleges—adding opportunities for civil leaders—in order to cultivate partners for DoD’s approach to CVE.

# Appendix A: Task Force Terms of Reference



ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

MAY 11 2011

## MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on Department of Defense (DoD) Strategy to Counter Violent Extremism Outside the United States.

In accordance with section 1239 of the National Defense Authorization Act for FY 2011 (H.R. 6523, 267-268), the DSB is directed to create a Task Force to conduct an independent assessment of the Department's strategy to counter violent extremism outside the United States. The assessment shall include the following areas of interest:

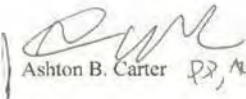
- (1) A review of the current strategy, research activities, resource allocations, and organizational structure of the DoD for countering violent extremism outside the United States.
- (2) A review of interagency coordination and decision making processes for executing and overseeing strategies and programs for countering violent extremism outside the United States.
- (3) An analysis of alternatives and options available to the DoD to counter violent extremism outside the United States.
- (4) An analysis of legal, policy, and strategy issues involving efforts to counter violent extremism outside the United States as such efforts potentially affect domestic efforts to interrupt radicalization efforts within the United States.
- (5) An analysis of the current DoD information campaign against violent extremists outside the United States.
- (6) Such recommendations for further action to address the matters covered by the report as the DSB considers appropriate.
- (7) Such other matters as the DSB determines relevant.

A final report on the results of the assessment shall be submitted to the congressional defense committees upon completion not later than January 7, 2012.

This Task Force will be sponsored by me as the Under Secretary of Defense for Acquisition, Technology and Logistics and co-sponsored by the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict & Interdependent Capabilities. Mr. Michael Bayer and GEN John M. Keane, U.S. Army (Retired) will co-chair the Task Force. Ms. Pauline Kusiak, Office of the ASD(SOLIC/IC), will serve as Executive Secretary. Lieutenant Commander Doug Reinbold, U.S. Navy, will serve as the DSB Secretariat Representative.

---

The Task Force will operate in accordance with the provisions of Public Law 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of title 18, U.S. Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

  
Ashton B. Carter *PR, ACTING*

# Appendix B: Task Force Membership

## Chairman

Mr. Michael Bayer

## Members

Dr. David Chu

ADM William Fallon, USN (ret.)

Honorable Judith Miller

Mr. Alan Schwartz

## Government Advisors

Mr. Robert Presler                      OSD (Policy)

COL Michael Lwin, USA                OSD (Policy)

LTC Albert Armonda, USA            OSD (Policy)

## Executive Secretary

LTC John Gallagher, USA            CJCS

Mr. John Matheny  
(through July 2014)                    OSD (SO/LIC)

## DSB Secretariat

Dr. David Jakubek                      Defense Science Board

CAPT James CoBell III, USN        Defense Science Board

Lt. Col. Michael Harvey, USAF       Defense Science Board

## Support

Ms. Karen Love                         SAIC



# Appendix C: Briefings Received

## 24 – 25 March 2014

### **DoD & NCTC CVE Efforts**

NCTC

### **DoD CVE Efforts – Cyber Focus**

Office of the DASD for Cyber Policy

### **DoD CVE Efforts – Special Operations Focus**

Office of the ASD (SO/LIC)

### **JS CVE Efforts**

Office of the CJCS

### **Intelligence Assessment of Extremist Threat**

NIC

### **DOS CVE Efforts – Strategic CT Communications**

DOS CSCC

### **Extremism and CVE**

Sageman Consulting, LLC

### **CVE Programs**

USIP

## 24 – 25 April 2014

### **CVE: Two Administrations, One Tale**

Palantir Technologies

### **Thoughts on Campaigning Against (Countering) Violent Extremism**

USSOCOM/J5

### **Capacity Building for CVE: The International Counterterrorism Fellowship Program**

NDU

### **NCTC CVE Efforts**

NCTC

### **CVE: Insights & Evidence from the Field**

ARTIS Research

### **CVE: Pathways to De-radicalization of Sub-State and Non-State Violent Groups**

ARTIS Research

**Gaps in Measuring the Influence of Extremist Communications**  
NCTC

**18 July 2014**

**CVE in USAFRICOM**

Independent Consultant

**Media in the Lives of People on the Edge**

Independent Consultant

**Leveraging the Entertainment Industry to Advance U.S. CVE Efforts**

Pherson Associates

**USAID Countering Violent Extremism Policies and Programming**

USAID

**The American People as Partners in U.S. Missions Abroad**

Spirit of America

**USAFRICOM CVE Efforts**

USAFRICOM/J5





## Appendix D: Bibliography

Bjelopera, Jerome P., “Countering Violent Extremism in the United States,” Congressional Research Service, May 31 2012. <http://www.fas.org/sgp/crs/homesecc/R42553.pdf> (accessed on October 27, 2014)

Briggs, Rachel and Sebastien Febe. “Review of Programs to Counter Narratives of Violent Extremism: What Works and What are the Implications for Government?” Institute for Strategic Dialogue. London: 2013.

Broadcasting Board of Governors. “About.” <http://www.bbg.gov/about-the-agency/> (accessed on October 27, 2014)

Broadcasting Board of Governors. *Impact through Innovation and Integration: BBG Strategic Plan 2012 – 2016*. [http://www.bbg.gov/wp-content/media/2012/02/BBGStrategicPlan\\_2012-2016\\_OMB\\_Final.pdf](http://www.bbg.gov/wp-content/media/2012/02/BBGStrategicPlan_2012-2016_OMB_Final.pdf) (accessed October 23, 2014).

Fink, Naureen Chowdhury, Peter Romaniuk, and Rafia Barakat. *Evaluating Countering Violent Extremism Programming: Practice and Progress*. September 2013. [http://globalcenter.org/wp-content/uploads/2013/07/Fink\\_Romaniuk\\_Barakat\\_EVALUATING-CVE-PROGRAMMING\\_20132.pdf](http://globalcenter.org/wp-content/uploads/2013/07/Fink_Romaniuk_Barakat_EVALUATING-CVE-PROGRAMMING_20132.pdf) (accessed on October 27, 2014)

Global Counterterrorism Forum. “Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism.” <https://www.thegctf.org/documents/10162/88482/Final+Ankara+Memorandum.pdf> (accessed on October 27, 2014)

Global Counterterrorism Forum. “Countering Violent Extremism Working Group: Community Engagement Practitioners’ Workshop.” Chair’s Summary.” 2013. [https://www.thegctf.org/documents/10295/39127/13Apr18\\_CE+Meeting+Summary\\_Washington+22+March.pdf](https://www.thegctf.org/documents/10295/39127/13Apr18_CE+Meeting+Summary_Washington+22+March.pdf) (accessed on October 27, 2014)

Global Counterterrorism Forum. “Countering Violent Extremism Working Group: CVE through Communications Work Stream Practical Seminar on Monitoring and Evaluation Techniques for CVE Communication Programs.” 2013. [https://www.thegctf.org/documents/10295/34757/13Mar22\\_Co-Chair+Summary+CVE+Comms+Seminar\\_Abu+Dhabi.pdf](https://www.thegctf.org/documents/10295/34757/13Mar22_Co-Chair+Summary+CVE+Comms+Seminar_Abu+Dhabi.pdf) (accessed on October 27, 2014)

Global Counterterrorism Forum. “Countering Violent Extremism Working Group: Workshop to Develop a Plan of Action for Community-Oriented Policing as a Tool for Countering Violent Extremism.” 2014. <https://www.thegctf.org/documents/10295/93228/Meeting+Summary+-+Workshop+on+COP+as+a+Tool+for+CVE+-+Doha+3-4+March+2014.pdf> (accessed on October 27, 2014)

Global Counterterrorism Forum. “Good Practices on Community Engagement and Community Oriented Policing as Tools to Counter Violent Extremism.” 2013.

[https://www.thegctf.org/documents/10162/72352/13Aug09\\_Community+Engagement+and+Community-Oriented+Policing+Good+Practices+++pdf](https://www.thegctf.org/documents/10162/72352/13Aug09_Community+Engagement+and+Community-Oriented+Policing+Good+Practices+++pdf) (accessed on October 27, 2014)

Hoffman, Bruce. "Who Fights? A Comparative Demographic Depiction of Terrorists and Insurgents in the Twentieth and Twenty-First Centuries." In *The Changing Character of War*, edited by Hew Strachan and Sibylle Schneipers, 282-301. Oxford: Oxford University Press, 2011.

Horgan, John and Kurt Braddock. "Rehabilitating the Terrorists?: Challenges in Assessing the Effectiveness of De-radicalization Programs" in *Terrorism and Political Violence*, 22:267-291, 2010.

Nasser-Eddine, Minerva, et al., "Countering Violent Extremism (CVE) Literature Review," Defense Science and Technology Organisation, Edinburgh, Australia, March 2, 2011.  
<http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10150/1/DSTO-TR-2522%20PR.pdf> (accessed on October 27, 2014)

U.S. Agency for International Development. *The Development Response to Violent Extremism and Insurgency*. September 2011. [http://pdf.usaid.gov/pdf\\_docs/pdacs400.pdf](http://pdf.usaid.gov/pdf_docs/pdacs400.pdf) (accessed October 23, 2014).

U.S. Department of Defense. *Department of Defense Directive Number 3600.01: Information Operations*. May 2, 2013. <http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf> (accessed on October 27, 2014)

U.S. Department of Defense, Defense Science Board. *Task Force Report: Creation and Dissemination of All Forms of Information in Support of PSYOP in Time of Military Conflict*. May 2000.  
<http://www.acq.osd.mil/dsb/reports/ADA382535.pdf> (accessed on December 15, 2014)

U.S. Department of Defense, Defense Science Board. *Task Force Report: Predicting Violent Behavior, Executive Summary*. August 2012. <http://www.acq.osd.mil/dsb/reports/PredictingViolentBehavior.pdf> (accessed on October 27, 2014)

U.S. Department of Defense, Defense Science Board, *Task Force Report: Strategic Communication*. September 2004. <http://www.acq.osd.mil/dsb/reports/ADA428770.pdf> (accessed on December 15, 2014)

U.S. Department of Defense, Defense Science Board, *Task Force Report: Strategic Communication*. January 2008. <http://www.acq.osd.mil/dsb/reports/ADA476331.pdf> (accessed on December 15, 2014)

U.S. Department of Defense. *Quadrennial Defense Review 2014*. 2014.  
[http://www.defense.gov/pubs/2014\\_Quadrennial\\_Defense\\_Review.pdf](http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf) (accessed October 23, 2014).

U.S. Department of Defense. *Sustaining U.S. Global Leadership: Priorities for 21<sup>st</sup> Century Defense*. January 2012. [http://www.defense.gov/news/defense\\_strategic\\_guidance.pdf](http://www.defense.gov/news/defense_strategic_guidance.pdf) (accessed October 23, 2014).

U.S. Department of State. *Annual Report on Assistance Related to International Terrorism: Fiscal Year 2013*. February 11, 2014. <http://www.state.gov/j/ct/rls/other/rpt/221544.htm> (accessed October 23, 2014).

U.S. Department of State. "Bureau of Counterterrorism." <http://www.state.gov/j/ct/> (accessed October 23, 2014).

U.S. Department of State. “Center for Strategic Counterterrorism Communications.” <http://www.state.gov/r/cscc/index.htm> (accessed October 23, 2014).

U.S. Department of State. *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review*. 2010. <http://www.state.gov/documents/organization/153108.pdf> (accessed October 23, 2014).

U.S. Department of State. “Programs and Initiatives.” <http://www.state.gov/j/ct/programs/index.htm> (accessed October 23, 2014).

U.S. Department of State. “Under Secretary for Public Diplomacy and Public Affairs.” <http://www.state.gov/r/> (accessed October 23, 2014).

*U.S. Government Efforts to Counter Violent Extremism: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, United States Senate, One Hundred Eleventh Congress, Second Session, March 10, 2010*. 111<sup>th</sup> Congress. Washington, D.C.: United States Government Printing Office, 2011.

U.S. Joint Chiefs of Staff. *Joint Publication 3-22, Foreign Internal Defense*. July 12, 2010. [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_22.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf) (accessed on October 27, 2014)

U.S. Joint Chiefs of Staff. *Joint Publication 3-26, Counterterrorism*. November 13, 2009. [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_26.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_26.pdf) (accessed on October 27, 2014)

U.S. Joint Chiefs of Staff. *Joint Publications 5-0, Joint Operation Planning*. August 11, 2011. [http://www.dtic.mil/doctrine/new\\_pubs/jp5\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf) (accessed on October 27, 2014).

Warner, Lesley Anne. “The Trans Sahara Counter Terrorism Partnership: Building Partner Capacity to Counter Terrorism and Violent Extremism.” CNA. March 2014. <http://www.cna.org/sites/default/files/research/CRM-2014-U-007203-Final.pdf> (accessed on October 23, 2014).

The White House. “National Framework for Strategic Communication.” <http://fas.org/man/eprint/pubdip.pdf> (accessed on October 27, 2014)

The White House. “Remarks by President Obama in Address to the United Nations General Assembly.” September 24, 2014. <http://www.whitehouse.gov/the-press-office/2014/09/24/remarks-president-obama-address-united-nations-general-assembly> (accessed on October 27, 2014)

The White House. *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*. December 2011. <http://www.whitehouse.gov/sites/default/files/sip-final.pdf> (accessed October 27, 2014)



# Appendix E: Non-DoD CVE Programming

## National Counterterrorism Center

NCTC is the primary organization for strategic operational planning for counterterrorism (CT). NCTC operates under the policy direction of the President of the United States and the National Security Council to provide a full-time interagency forum and process to plan, integrate, assign lead operational roles and responsibilities, and measure the effectiveness of strategic operational CT activities of the USG. The Director of NCTC is a Deputy Secretary-equivalent reporting to the President regarding Executive branch-wide CT planning and to the Director of National Intelligence regarding intelligence matters. NCTC addresses CVE as part of the CT goal, working side by side with the Federal Bureau of Investigation, Department of Homeland Security, Department of Justice, DoS, and DoD to build whole-of-government approaches to CVE. Internationally, NCTC works with the DoS to support CVE work in embassies across Europe, North Africa, and South Asia. The Global Engagement Group at NCTC chairs a monthly, senior-level working meeting (CVE Interagency Coordination Group) to coordinate domestic and overseas CVE work.

## Department of State

CVE is a pillar of DoS's strategic approach to CT. Through a mix of local grants developed and managed by U.S. embassies, and larger awards managed from Washington, DC, the CVE program pursues three main lines of effort: 1) provide positive alternatives to those most at-risk of radicalization and recruitment into violent extremism; 2) counter violent extremist narratives and messaging; and 3) increase international partner capacity (civil society and government) to address drivers of radicalization. Most CVE programming uses Economic Support Funds or Nonproliferation, Anti-terrorism, Demining, and Related Programs (NADR) authorities, with \$7 million implemented in FY2013.

The DoS's Center for Strategic Counterterrorism Communications (CSCC) coordinates, orients, and informs government-wide foreign communications activities targeted against terrorism and violent extremism. The CSCC is guided by the National Strategy for Counterterrorism and operates under policy direction of the White House and interagency leadership. The CSCC's Digital Outreach Team actively and openly engages in Arabic, Urdu, Punjabi, and Somali to counter violent extremist propaganda and misinformation about the United States across a wide variety of interactive digital environments.

The Department of States' Regional Strategic Initiative (RSI) brings embassy officials, military, law enforcement, and intelligence officers together under Chief-of-Mission authority to assess terrorist threats, pool resources, and devise collaborative strategies, plans, and policy recommendations. RSI groups are in place for Southeast Asia, East Africa, Eastern Mediterranean, Iraq, South Asia, Western Hemisphere, Central Asia, and the Trans-Sahara. In

FY2013, RSI funds supported programs that included the Uganda Police Force Community Policing Outreach Program, among others.

The Department of State provides senior, Ambassador-ranked personnel as civilian deputy to combatant commands (COCOMs) in addition to existing Foreign Policy Advisors, where such appointments advance national interests. The DoS also plans to increase details of mid- to senior-level DoS personnel to COCOMs to improve working-level cooperation with the DoD. Finally, DoS plans to pursue more regular joint strategic training and planning with the DoD.

### **United States Agency for International Development (USAID)**

USAID identifies development as an important component of CVE. As such, USAID leverages its development and technical expertise, field presence, and mobilization mechanisms to address the development-related drivers of violent extremism. USAID contributes to interagency CVE programs such as the Trans-Sahara Counterterrorism Partnership, designed to enhance the indigenous capacities of governments in the pan-Sahel to confront extremism. USAID also embeds senior development advisors at regional military COCOMs.

### **Broadcasting Board of Governors (BBG)**

The Broadcasting Board of Governors (BBG) is both the name of the independent federal agency that oversees all U.S. civilian international media and the name of the board that governs those broadcasts. Broadcasters within the BBG network include the Voice of America, Radio Free Europe / Radio Liberty, the Middle East Broadcasting Networks, Radio Free Asia, and the Office of Cuba Broadcasting. The BBG's mission is to inform, engage, and connect people around the world in support for freedom and democracy. The BBG's strategic plan prioritizes support for democracy and CVE—particularly in the Middle East and North Africa—by boosting access to credible information and local news, nurturing citizen journalism and user generated content, and facilitating dialogue across religious, national, and ethnic groups.





## Appendix F: Strategic Communication Roles

The following offices each have a lead role for SC:

- Combatant commanders (including the Commander USSOCOM when designated as the supported commander for MISO) plan, support, and conduct SC in support of theater military missions and U.S. national and regional objectives.
- Commander USSOCOM is the designated joint proponent for MISO, which includes leading the collaborative development, coordination, and integration of the MISO capability across the DoD.
- ASD (SO/LIC) exercises policy operations for MISO activities, including Military Information Support Teams. ASD (SO/LIC) is responsible for development, coordination, and oversight of the implementation of policy and plans for DoD participation in all U.S. Government combating terrorism activities, including programs designed to counter violent extremism.
- The Under Secretary of Defense for Intelligence exercises authority for oversight of IO and is a key participant in the strategic communication process at COCOMs and across the DoD.
- The Assistant Secretary of Defense for Public Affairs supports military PA and DSPD and approves public affairs guidance for the COCOMs and other DoD components.
- On the Joint Staff, J-5 is responsible for military diplomacy. In conjunction with the COCOMs and Services, the J-5 develops policy guidance, strategic plans, and enduring communications themes and narratives for senior leadership, based upon policy guidance and directives from OSD. The J-5 also serves as the Joint Staff representative in the interagency process.
- J-3 is responsible for IO expertise and advice to leadership to achieve national, strategic, and theater military objectives.

Geographic Combatant Commands must collaborate with the DoS diplomatic missions within their areas of responsibility on SC. In efforts to persuade and influence, DoD is a supporting entity, taking guidance and focus from the DoS and working in close collaboration with the country team. DoD is in regular dialogue with Under Secretaries of Defense for PD and PA and with the Ambassador at Large for CT, as well as regional bureaus on challenges specific to the area of responsibility. DoD campaigns and products are reviewed and approved by the U.S. Ambassador. In numerous key locations, the DoD provides the U.S. Ambassador with a tailored

military information support team that works through and with the host nation to promote effective strategic communications to counter violent extremism.



## Appendix G: Acronyms

**ASD/SO/LIC** Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

**BBG** Broadcasting Board of Governors

**CAO** Civil Affairs Operations

**CMO** Civil Military Operations

**COCOMs** Combatant Commands

**CSCC** Center for Strategic Counterterrorism Communications

**CT** Counterterrorism

**CVE** Countering Violent Extremism

**DoD** Department of Defense

**DoS** Department of State

**DSB** Defense Science Board

**DSPD** Defense Support to Public Diplomacy

**FAA** Foreign Assistance Act

**FID** Foreign Internal Defense

**GEF** Global Employment of the Forces

**GSET** Global Strategic Engagement Team

**ICG** Interagency Coordination Group

**IPC** Interagency Policy Committee

**IO** Information Operations

**ISIL** Islamic State of Iraq and the Levant

<b>JIACG</b>	Joint Interagency Coordination Group
<b>JSCP</b>	Joint Strategic Capabilities Plan
<b>MISO</b>	Military Information Support Operations
<b>NCTC</b>	National Counterterrorism Center
<b>NGO</b>	Non-Governmental Organization
<b>NSC</b>	National Security Council
<b>OSD</b>	Office of the Secretary of Defense
<b>PA</b>	Public Affairs
<b>PD</b>	Public Diplomacy
<b>PSYOP</b>	Psychological Operations
<b>QDR</b>	Quadrennial Defense Review
<b>RSI</b>	Regional Strategic Initiative
<b>SC</b>	Strategic Communication
<b>SFA</b>	Security Force Assistance
<b>SMS</b>	Short Message Service (SMS) - text messaging
<b>SOF</b>	Special Operations Forces
<b>UN</b>	United Nations
<b>USAID</b>	United States Agency for International Development
<b>USD(P)</b>	Under Secretary of Defense for Policy
<b>USG</b>	United States Government

**USSOCOM** United States Special Operations Command