Role of Militaries in Facing Non-Traditional Threats
Presented by
Colonel Mitch Cassell
United States Department of Defense (The Joint Staff)

Thank you Madam Chairman. As we all know the list of Non-Traditional Threats (NTT) is very long, and includes transnational crime (human/narcotics trafficking), climate change, natural disasters, environmental, food/water security, economic, health - including threats from HIV, MERS, SARS, Ebola, malaria - and many-many others.

The Department of Defense (DoD) works diligently to harmonize and leverage various defense resources to stay ahead of NTTs, to include working with other USG agencies, as well as partner nations and allies abroad.

Transnational Crime (TNC). In combating transnational organized crime to degrade the nexus between crime, terrorism, and insurgency, DoD focuses its countering transnational organized crime support activities on criminal organizations and networks with links to terrorist groups or that otherwise significantly threaten U.S. national security interests. In this, DoD brings a number of important skills and capabilities to address TNC, such as:

- Intelligence capabilities that simply do not exist in most other Gov't agencies
- Forward presence – in areas of importance where transnational crim'l orgs operate with impunity, such as Africa, the Middle East, and Indo-Asia-Pacific.
- Expertise in operational planning, strategy development, and C2.
- The skills and expertise of Armed Forces personnel, particularly within the Guard and Reserve components, who may be bankers, lawyers, accountants, or logistics professionals in their civilian career who can serve as financial forensics specialists and trace the origin and flow of money, and in turn help to prosecute leaders of criminal organizations, or target them.
    - DoD's counter threat finance capability is one area where we see close collaboration between all the tools of government. By working together to identify, follow, and seize illicit funding, we effectively support our interagency and international partners in countering national security threats, using tools such as sanctions, asset seizure/freeze, indictments, and international engagement.
- Vital intelligence analysis, capacity building and training, equipment, infrastructure, and logistical support to partner states, to help build interagency collaboration to confront unconventional threats.

Outer Space. Societies have become dependent on capabilities and information delivered to, from, and through space. We are highly dependent on space for more routine communications, be it the use of GPS for everyday mundane transport of goods, people, and service from one location to another, or the transmission of more secure information that is the lifeblood of international financial markets. Resourceful adversaries may leverage asymmetric or unconventional approaches to circumvent traditional strengths in the space domain. They could also exploit vulnerabilities in the space domain by denying the use of reconnaissance, early-warning, communications, navigation, and weather satellite assets that enhance land-based military or commercial operations. Figuring out the rules and codes of conduct that should govern this domain is a commercial, government and military responsibility—and one that demands cooperation.

Cyberspace. Related to outer space is cyberspace. World leaders have repeatedly identified cyber as the greatest single security threat. Cyberspace integration brings new levels of vulnerability and the potential for mass disruption of infrastructures or functions across critical military, political and economic targets. DOD's cyber strategy is a whole of gov,t approach and contains five strategic initiatives (SI):

- SI1: Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential.
- SI2: Employ new defense operating concepts to protect DOD networks/systems.
  - It's worth highlighting that former VCJCS General James Cartwright noted in May 2012 that the U.S. must protect its military systems, such as the stealthy F-35 Joint Strike Fighter, from hackers. Yes, ladies and gentlemen, our next generation top-line fighter plane can be hacked, right from underneath the pilot while flying the plane. This outcome is extremely low, but the point is made that our modern systems are so networked that it creates a serious vulnerability that we must mitigate.
- SI3: Partner with other U.S. government agencies and the private sector to enable a whole-of-government cyber security strategy.
- SI4: Build robust relationships with U.S. allies and international partners to strengthen collective cyber security.
- SI5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

SI4 addresses directly the need for international cooperation. As the strategy notes:

- *"The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious* *code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense.*

<u>Airspace</u>. Terrorists can use drone aircraft and other remotely operated or unmanned systems to ferry a relatively small weapon into areas that previously were highly secure, such as infrastructure hubs or military facilities. To fight this new threat of drone attacks, we need to wrestle with the legal and air space management issues associated with these systems operating over our homelands—and the hand-off challenges as these systems cross international boundaries.

<u>Maritime</u>. Maritime terrorists, modern day pirates, and criminal organizations are acting with increasing frequency and complicate defense challenges in the maritime domain. Swarming as an operational tactic has become increasingly relevant. Since the "enemy" often enjoys the advantages surprise, our forces must also adopt similar attributes of flexibility and speed (and stealth) to be able to respond in time. Outpacing these actors will undoubtedly require cooperation and collaboration in information and intelligence sharing. A few weeks ago, representatives from the ASEAN countries met in Hawaii to discuss the very issue of maritime security threats and ways in which they could cooperate to develop a shared maritime awareness capability to defend against criminal activities occurring in the maritime space that adversely affect them all. Such a goal of shared maritime awareness necessitates the development of an information sharing portal that provides all partners with a common operating picture of what activities are occurring in their maritime space or territorial waters. The Philippines Coastal Watch System is a good example of a system that provides a full picture within their national archipelago. And the Changi C2 Center in Singapore is a good example of a capability that can fuse disparate sources of information and pipe it to all who need it. The PHL CWS can see potential transnational crime or terrorist activity in the tri-border area of Malaysia, Indonesia and the Philippines. It would be a shame if the Philippines can develop this sort of information but have no means to share it in a timely manner with their neighbors.

<u>CONCLUSION</u>. Non-traditional security threats increasingly occupy the time and resources of national security professionals. The Cyber, Space, Air and Land domains are ripe with threats and opportunities for collaboration and cooperation. Given the broad array of threats across a number of domains, the Asia-Pacific region should expand its emphasis in cooperative efforts to reduce the likelihood of war—and if that fails, mitigate its effects. In seeking to support responsible behavior and oppose and dissuade those who seek to disrupt peace and stability, international cooperation will be needed to share warning capabilities, engage in capacity building, and conduct joint training activities.