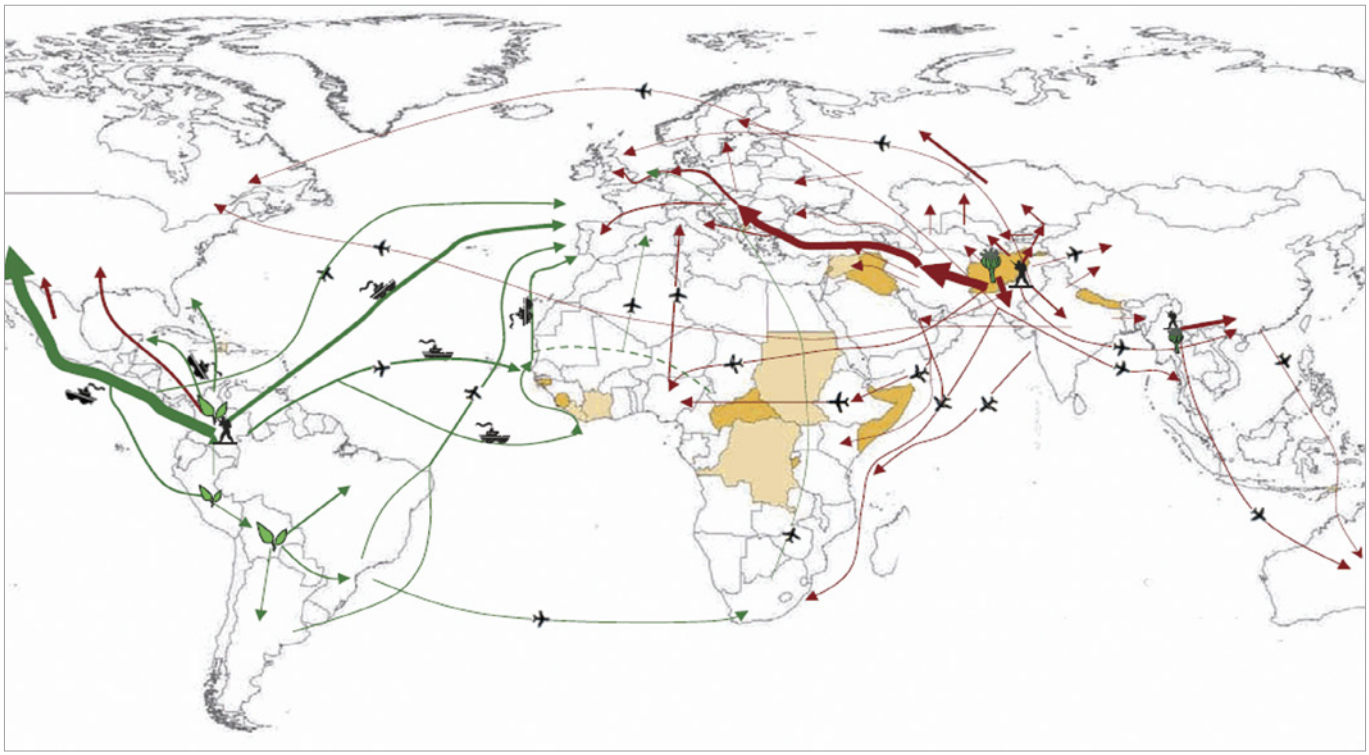


HOW NATO CAN SUPPORT COUNTERING THREAT NETWORKS

A growing danger to the international community consists of highly complex adversary networks with international span that employ criminal financing as well as terror attacks and other destructive capabilities. To effectively counter these dynamic and violent illicit networks NATO should champion the creation of an international and multifunctional framework to share information on these networks as well as collaborative multinational countermeasures.

By Jeffrey V. Gardner,
Lieutenant Colonel, U.S. Army (Ret)

THE THREAT

"Governments are faced with a broad spectrum of national security threats that emanate from non-state actors as well as traditional nation-states. Illicit networks that include transnational crime organisations, drug traffickers, gangs, and terrorist groups are among these non-state actors…what is novel today is the pervasive, prolific, and converging nature of illicit networks around the world. These networks threaten the rule of law, government institutions, the economy, and society." [1]

These adaptive and amorphous threat networks operate locally, regionally, and globally and they have significant nefarious effects both inside and outside the traditional military Area of Operations.

"Violent non-state actors, including terrorist organisations and insurgent movements, seek to collaborate with criminal networks – and in some cases become criminal networks – in order to finance acts of terrorism and purchase the implements of destruction and killing." [2]

Given the current trends, we can surmise that we will see an increased convergence of illicit groups of terrorists, insurgents, and transnational criminal organisations in the future. For example, several of the 2004 Madrid train bombers were drug dealers and funded the attack with criminal activities. Some terrorist and insurgent groups today such as the Revolutionary Armed Forces of Colombia (FARC) and al Qaeda in the Islamic Magreb in North Africa have turned significantly to illicit trafficking as well as kidnapping for ransom to fund their violent actions. The terrorist Abu Sayyaf Group in Southeast Asia often resorts to piracy, extortion, and

9/11 attack.

other criminal enterprises. Other groups such as Iranian-backed Hezbollah have extensive global networks of both legal and illegal activities to finance their nefarious enterprises and prepare for future terrorist attacks.[3]

"Although the fields of diplomacy, information, military, and economic power have generally belonged to states since the 1700s, modern illicit transnational networks have expanded their operations into these areas." [4]

The benefits of globalisation work both ways and make it easier for these threat networks to thrive. Terrorists, insurgents, and other adversary networks can recruit, train, finance, command, and control the globalised civil communications infrastructures, and they employ asymmetric weapons like Improvised Explosive Devices (IEDs), cyber-attacks, and other counter-alliance techniques.

"The use of advanced IED technology and sophisticated tactics, techniques, and procedures provide individuals and transnational networks with cheap and easily accessible means to achieve high visibility effect. The extremist networks that employ IEDs have proven to be resilient, adaptive, interconnected, and extremely violent. Globalisation, the Internet, and social media have extended the reach of these organisations, providing platforms for recruiting, technical exchanges, training, planning, funding, and social interaction." [5]

... MODERN ENEMIES ARE MORE LIKELY TO USE ASYMMETRIC TACTICS AND POSSIBLY EVEN HAVE ASYMMETRIC OBJECTIVES ...

THE CHALLENGE

Understanding and countering these complex threat networks will be the premier challenge for the North Atlantic Treaty Organisation (NATO) and the rest of the world for generations to come, and it is vital for global security. After the September 2001 Terrorist attacks (9/11) on the United States, that government worked hard to break down the agency "stovepipes" that inhibited effective information sharing and cohesive interagency action. Many interagency centres were created over the years such as the National Counter Terrorism Center (NCTC), the National Drug Intelligence Center (NDIC), the National Counter-Proliferation Center (NCPC), International Organized Crime Intelligence and Operations Center (IOC-2), as well as many interagency efforts to counter threat finances. These efforts did improve inter-organisational data fusion and information sharing, but they just replaced the old agency stovepipes with new functional or topic stovepipes. Unfortunately, modern illicit networks are increasingly converging and span across all of these areas without boundaries, thus hampering government countermeasures with bureaucratic and jurisdictional firewalls. These problems are greatly compounded when you additionally consider the challenges of coordinating multiple nations and many international organisations.

"The problem is too large for any one government to solve. It requires a net-centric approach at the bilateral, subregional, regional, and global levels based on information-sharing and coordination to break the financial strength of criminal and terrorist networks, disrupt illicit trafficking networks, defeat transnational criminal and terrorist organisations..." [6]

NATO was originally set up by the Western powers to guard against a military threat from the Eastern Bloc and has historically focused, as an organisation, on traditional war-fighting. NATO needs to maintain the capability to act against a military aggressor and in this way remain a deterrent in itself reducing the likelihood that the capability will be needed. Much more likely operations, as witnessed in Afghanistan, Kosovo and

Ocean Shield, are in a different part of the conflict spectrum and require a quite different approach. Modern enemies are more likely to use asymmetric tactics and possibly even have asymmetric objectives; they are likely to be hidden amongst the populations. Consequently, the Alliance has less than optimal policies, procedures, or infrastructure in place to counter these dynamic threat networks across the continuum of conflict. More positively, NATO does have a military framework for Attacking the Networks (AtN) that is effective at neutralising adversary IED and insurgent networks in theatres of war.[7] However, recent experiences have shown that the networks operating within a theatre of war will undoubtedly have further connection to regional and transnational networks which will be outside the reach and authorities of NATO Commanders to take action against. This will necessitate a comprehensive approach, through other governmental agencies and international organisations. Effectively countering these transnational illicit networks will therefore require synchronising actions across the many intergovernmental and primarily civilian international sectors such as diplomatic, intelligence, financial, and law enforcement. Unfortunately, NATO currently finds itself ill-configured organisationally or in terms of process to handle the complexity of these pan-Governmental issues. The challenge is how transformation can best be implemented to support these various civilian authorities to harmonise the actions of all the elements of international power against these dynamic threat networks.

"The resourcefulness, adaptability, innovativeness, and ability of illicit networks to circumvent countermeasures make them formidable foes for national governments and international organisations alike. Their increasing convergence gives them ever-improved ability to evade official countermeasures and overcome logistical challenges as well as ever better tools for exploiting weaknesses and opportunities within the state system, and attacking that system.

Since illicit actors have expanded their activities throughout the global commons, in the land, sea, air, and cyber domains, nations must devise comprehensive and multidimensional strategies and policies to combat the complex transnational threats posed by these illicit networks." [8]

THE RESPONSE

Effectively responding to these networked illicit groups and the challenge of effectively synchronising the actions of many nations and international organisations calls for a new approach to Countering Threat Networks (CTN). While each instrument of international power has its own individual role to play, such as law enforcement and financial controls, what is needed is a platform for systematic information sharing and effective collaboration. As an example, NATO has formally adopted a "Comprehensive Approach" framework to address security challenges:

"Our operational experience has taught us that military means, although essential, are not enough on their own to meet the many complex challenges to our security. Both within and outside the Euro-Atlantic area, NATO must work with other actors to contribute to a comprehensive approach that effectively combines political, civilian and military crisis management instruments. Its effective implementation requires all actors to contribute in a concerted effort, based on a shared sense of responsibility, openness and determination, and taking into account their respective strengths, mandates and roles, as well as their decision-making autonomy." [9]

Future success in CTN requires that NATO and its security partners fully comprehend these adversary groups, and that national governments and inter-organisational agencies develop an international network of their own to counter these illicit groups that span from terrorists, to insurgents, and all sorts of transnational criminal organisations. An international CTN network could facilitate information sharing and thereby enable the harmonisation of all the elements of international power needed to fight these networks cohesively and effectively. NATO needs a truly comprehensive approach to Counter Threat Networks by proposing and supporting an international CTN network of civil and military entities that span the

FUTURE SUCCESS IN CTN REQUIRES THAT NATO AND ITS SECURITY PARTNERS FULLY COMPREHEND THESE ADVERSARY GROUPS, AND THAT NATIONAL GOVERNMENTS AND INTER-ORGANISATIONAL AGENCIES DEVELOP AN INTERNATIONAL NETWORK OF THEIR OWN TO COUNTER THESE ILLICIT GROUPS THAT SPAN FROM TERRORISTS, TO INSURGENTS, AND ALL SORTS OF TRANSNATIONAL CRIMINAL ORGANISATIONS

sectors of diplomatic, intelligence, law enforcement, financial, and informational entities.

"A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act." [10] - General Stanley McCrystal.

While NATO may not be the ideal organisation to effectively synchronise actions across the primarily civilian elements of international power, a NATO comprehensive approach framework for a CTN network could provide the necessary stimulus to initiate such a civilian led enterprise. NATO is a key stakeholder in countering threat networks and has significant international political and military stature in the security arena to offer such a suggestion. The implications for NATO itself are likely to be truly transformational and as such Allied Command Transformation could be the appropriate place to initiate this drive from within NATO. Law enforcement, intelligence, and financial control functions clearly fall within the primacy of nation states and other civil international organisations, but effectively countering threat networks requires that NATO play a part in supporting these civilian international security, financial, and legal agencies. A CTN network could ensure a shared understanding of these different illicit networks and enable effective collaborative countermeasures across the elements of international power. This is in alignment with NATO's priority to cooperate on "increasingly global threats, such as terrorism, the proliferation of weapons of mass destruction, their means of delivery and cyber-attacks."[11] NATO may also have a defence diplomacy role in enabling capability beyond the alliance to influence partners and friendly nations and gain their trust and support.

"The old paradigm of fighting terrorism and transnational crime separately, utilising distinct sets of tools and methods, may not be sufficient to meet the challenges posed by the convergence of these networks..."[12]

... INFORMATION SHARING BETWEEN AGENCIES EVEN WITHIN A SINGLE NATION IS CHALLENGING, BUT THE LACK OF SUCH SHARING ALSO RESULTS IN TRAGEDIES SUCH AS THE 9/11 ATTACKS ...

NECESSARY FIRST STEPS

Effectively countering these adversary networks starts with a shared international understanding of these threat groups and their linkages. The sharing of intelligence, criminal, and financial information about these illicit groups and it is the foundational element of any effective CTN network. Information sharing between agencies even within a single nation is challenging, as described earlier within the United States, but the lack of such sharing also results in tragedies such as the 9/11 attacks.[13] Just because international information sharing will be challenging does not lessen the imperative of doing so for effective CTN. There are already widespread bilateral information sharing regimes in place for counter-terrorism, and many law enforcement agencies share information through frameworks such as EUROPOL and INTERPOL.[14] NATO can begin CTN work in this area by expanding some existing information sharing initiatives already in place like those for Counterterrorism as well as exchanges of information gathered during maritime operations.

"Current strategies to map and combat threat finance — criminal money laundering and terrorist financing — use the authorities of law enforcement, intelligence operations, public designation, and international cooperation with partner nations…all of these strategies are essential for fighting transnational organised crime." [15]

A WAY AHEAD

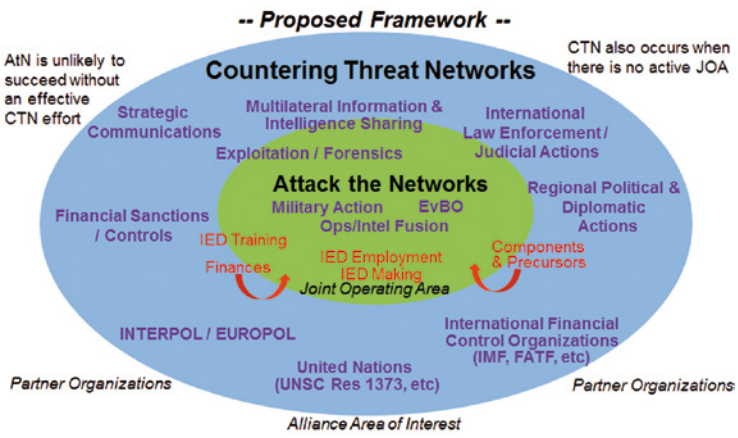
The international community needs a more cohesive, comprehensive, and proactive approach to counter these asymmetric illicit networks that threaten our security. CTN necessitates closer connections and effective collaboration between military, intelligence, law enforcement, financial and many other organisations. Effective multilateral information and intelligence sharing is only the first step. To truly harmonize actions, a framework that allows collaborative CTN countermeasures needs to be established. This article proposes that NATO offer an overarching concept to Counter Threat Networks (CTN) to facilitate dialogue between all appropriate agencies to catalyse

the development of a framework for an international solution.

The graphic on the right describes a proposed framework where tactical and operational AtN (an approved NATO concept) occurs in the Area of Operations (AO) while CTN (a proposed concept) is mutually supportive in the Area of Interest (AI) outside the Joint Operating Area or theatre of operations. ■

DISCLAIMER

"The views expressed in the article are solely those of the author and do not reflect the official views or position of NATO."



AtN: Attack the Networks
CTN: Counter Threat Networks
EUROPOL: European Police Office
EvBO: Evidence Based Operations
FATF: Financial Action Task Force
IMF: International Monetary Fund
INTERPOL: International Police
JOA: Joint Operating Area
UNSC: United Nations Security Council

REFERENCES

1 Celina B. Realuyo, Collaborating to Combat Illicit Networks Through Interagency and International Efforts. Chapter 14, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. p. 244.

2 Michael Miklaucic and Jacqueline Brewer, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. Introduction, p. xiv.

3 John Rollins and Liana Sun Wyler, Terrorism and Transnational Crime: Foreign Policy Issues for Congress, June 11, 2013. Congressional Research Service.

4 Admiral James G. Stavridis, USN, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013, 2013. Forward, p. xv.

5 Lieutenant General Michael D. Barbero, July 12, 2012, JIEDDO Director, House Testimony, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Barbero.pdf

6 David M. Luna, Fighting Networks with Networks, Chapter 12, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. p. 229.

7 Allied Joint Doctrine for Countering Improvised Explosive Devices, AJP 3.15. March 2011.

8 Michael Miklaucic and Jacqueline Brewer, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. Introduction, p. xiv.

9 Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon; 20 Nov. 2010. Para 8. http://www.nato.int/cps/en/SID-3215A85E-37A825CD/natolive/official_texts_68828.htm?selectedLocale=en

10 General Stanley McCrystal – It takes a Network, Foreign Policy, April 2011.

11 Declaration on Alliance Security Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl on 4 April 2009.

12 Michael Miklaucic and Jacqueline Brewer, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. Introduction p. xv.

13 The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States. Government Printing Office, 2011, p.353.

14 Tanaka, Hiroyuki, Rocco Bellanova, Susan Ginsburg, and Paul De Hert. "Transatlantic information sharing: At a crossroads." Migration Policy Institute, January 4 (2010).

15 Michael Miklaucic and Jacqueline Brewer, Convergence: Illicit Networks and National Security in the Age of Globalization, April 2013. Introduction p. xvi.

ABOUT THE AUTHOR

Jeff Gardner is employed by Allen Vanguard International (Counter Threat Solutions) and contracted to work as a C-IED Operations and Intelligence Planner/Advisor at NATO Allied Command Transformation. Prior to his current job he served as the Senior Intelligence Planner in a C-IED Intelligence, Surveillance, and Reconnaissance Task Force in Afghanistan. Before working in Afghanistan he was a U.S. Army Infantry Officer and Military Intelligence Officer serving in many significant assignments over his 26 year career; some highlights include service on the U.S. Joint Chiefs of Staff, a Joint Special Operations Task Force in Iraq, the U.S. European Command Staff, and the NATO Implementation Force in Bosnia. He has expertise in Counter-Terrorism, Strategy Development, Interagency Integration, and is a PhD Candidate in Homeland Security.