



ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 16, no. 4, Fall 2017



Contents

Vol. 16, no. 4, Fall 2017

Research Articles

- | | |
|---|----|
| NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations <i>Michael Hanna, David Granzow, Bjorn Bolte, and Andrew Alvarado</i> | 5 |
| Examining ISIS Online Recruitment through Relational Development Theory <i>Sarah Ponder and Jonathan Matusitz</i> | 35 |
| India's Counter-terrorism Policy Against Jihadist Terror: Challenges and Prospects <i>Vinay Kaura</i> | 51 |
| Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region <i>Dasha Nicolson</i> | 69 |
| The Prospects of Azerbaijan to Enhance Military Interoperability with NATO <i>Elman Nasirov and Khayal Iskandarov</i> | 89 |



M. Hanna, D. Granzow, B. Bolte, and A. Alvarado,
Connections QJ 16, no. 4 (2017): 5-33
<https://doi.org/10.11610/Connections.16.4.01>

Research Article

NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations

*Michael Hanna, David Granzow, Bjorn Bolte,
and Andrew Alvarado*

Abstract: Current global conflict trends are pulling NATO away from its traditional collective defense mission into stability and reconstruction (S&R) operations with greater frequency. S&R environments require NATO to collaborate with and support host nation governments, international organizations, and a range of non-governmental organizations to address security, political, and social challenges. However, NATO encounters difficulty with collecting and sharing intelligence and information in these environments. This inability to communicate compounds the already complex issues faced by all entities involved.

This article identifies three policy options to help NATO improve its support to S&R operations by enhancing information-sharing mechanisms within NATO and with non-NATO stakeholders. These options are: 1) the completion of the Federated Mission Network that seeks to aggregate classified and unclassified information in a regulated virtual space; 2) the indoctrination of a Joint Information Fusion Cell to act as a physical clearinghouse for information; and 3) the development of Regional Coordination Centers and Stabilization and Reconstruction Teams to implement individual S&R projects.

The progression of policy options represents increases in stakeholder engagement, operational effectiveness, and overall cost. Based on an analysis of the pros and cons associated with each option, we recommend the development of the Joint Information Fusion Cell (JIFC). This option offers a centralized facility capable of collecting, processing, and disseminating information and intelligence, and a separate, neutral facility

for coordinating with non-military entities. This option confers the widest array of benefits to NATO's contributions to S&R operations in both in-area and out-of-area environments.

Keywords: NATO operations, stabilization and reconstruction, intelligence sharing, information sharing, Joint Information Fusion Center

Problem and Importance

A key challenge facing the North Atlantic Treaty Alliance (NATO)—the world's longest lasting and most successful multinational military alliance—is how to reform its information sharing structures to address the complex operating environments NATO will face in the future. This challenge, while seemingly perpetual, has become further complicated since the dissolution of NATO's original opponent, the Soviet Union. Because NATO conducted no military operations during the Cold War, it never truly faced the need to share information in a rapidly evolving conflict scenario. However, since 1991 it has mobilized numerous times in response to new threats and situations that required the expedient flow of information.

Today, NATO's European members face a disparate array of security threats ranging from a revanchist Russia to an influx of refugees from the Middle East and Africa. NATO operations have been as diverse as security and reconstruction in Kosovo and Afghanistan, military and police training for the African Union (AU) and the Iraqi government, disaster relief in Haiti, Pakistan, and the United States, counter-piracy operations near the Horn of Africa and in the Indian Ocean, and rendering humanitarian assistance to members of the Commonwealth of Independent States.¹ These operating environments require NATO to move beyond Cold War-era structures that stifle information sharing.

Threats today often involve actors operating outside of formal legal and security apparatuses, requiring a more comprehensive understanding of the economic, social, and political elements that often drive modern conflict.² To meet the security challenges of today and tomorrow, NATO must rethink how it shares information within the Alliance and with external partners.³

Current Alliance intelligence structures do not facilitate the needed capacity for sharing. At the corps level, NATO units often have insufficiently sized intelligence staffs.⁴ At the Alliance level, no central authority exists with the power to

¹ NATO, "Operations and Missions: Past and Present," http://www.nato.int/cps/en/natohq/topics_52060.htm.

² *Guiding Principles for Stabilization & Reconstruction* (Washington, D.C.: United States Institute of Peace, United States Army Peacekeeping and Stability Operations Institute, 2009), https://www.usip.org/sites/default/files/guiding_principles_full.pdf, 11.

³ "Information Sharing with non-NATO Entities," NATO Joint Analysis and Lessons Learned Centre, November 13, 2012, http://www.jallc.nato.int/products/docs/factsheet_info_sharing.pdf

⁴ Interview with Source J, US official at NATO Allied Rapid Response Corps (ARRC), March 14, 2016.

vet, empower, and lend accountability to NATO members and non-NATO organizations to share intelligence.⁵ Sharing at this level is further hindered by a lack of trust between NATO member states.⁶ NATO's ability to share intelligence and information with outsiders is similarly compromised by a lack of trust and the absence of well-developed mechanisms for sharing.⁷ Mechanisms that do exist tend to be under-utilized.⁸

International confidence in the willingness and ability of NATO to provide an effective response to international crises is waning in the wake of operations such as those in Afghanistan and Libya. Yet it is exactly these types of conflicts in which the Alliance and its member states are most likely to engage in the future. At the start of this decade, five out of six NATO operations took place outside of the Alliance's territory.⁹ It is for exactly these types of conflicts new information-sharing structures need to be designed and implemented.

Shortcomings of Current NATO Policy

Intelligence policy specific to NATO is lacking standardized practices and products, mostly due to the consensus requirement for NATO decision-making.¹⁰ Within NATO, there exists a wide array of offices working on intelligence production and dissemination with little coordination at the working and leadership levels.¹¹ A review of intelligence actors within NATO conducted by the authors of this article reveals an organizational landscape of competition, politicization, and hoarding similar to the US intelligence community prior to 9/11. In lieu of guiding policy, intelligence sharing within the Alliance remains problematic and each organization has little incentive to share. Agencies have internal rules against sharing and no rewards for sharing. NATO intelligence analysts often resort to their individual country's production and disclosure standards, reducing the timeliness and utility of shared intelligence products.¹²

NATO does have a more developed policy toward sharing information with non-NATO partner states and International Organizations (IOs). NATO often uses

⁵ Interview with Col. James Sadler, US Army officer at NATO ARRC, March 14, 2016.

⁶ Interview with Source A, US DoD official, March 8, 2016.

⁷ Interview with Source M, non-US official at NATO ARRC, March 15, 2016.

⁸ Stewart Webb, "Improvements Required for Operational and Tactical Intelligence Sharing in NATO," *Defence Against Terrorism Review* 6, no. 1 (Spring / Fall 2014): 47-62, quote on p. 59.

⁹ Ivo Daalder, "NATO's Finest Hour," *The Wall Street Journal Europe*, September 12, 2011, <https://www.wsj.com/articles/SB10001424053111903285704576559422200245388>.

¹⁰ See the North Atlantic Treaty, signed in Washington, D.C., April 4, 1949, http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf

¹¹ Interview with Source J, US official at NATO ARRC, March 14, 2016.

¹² These shortcomings were expressed by most, if not all, of the interviews conducted by the authors of this article.

bilateral sharing agreements, which include non-disclosure clauses, network security and hardware inspections, provision of software in some cases, and other information assurance measures.¹³ Because information NATO provides to these kinds of external actors is not necessarily meant to be actionable, delays in information sharing with IOs do not pose the same security risks as it does among military partners. However, NATO continues to struggle to produce a coherent policy that facilitates the efficient and productive sharing of information with Non-Governmental Organizations (NGOs).

Unsurprisingly, many NGOs do not meet NATO's strict information security or "need-to-know" requirements. Moreover, while NATO could benefit from on-the-ground information owned by NGOs, the absence of cooperative planning and direct lines of communication often renders such information nonexistent.¹⁴ Finally, NATO has a tendency to treat NGOs as subordinates rather than equal partners in stabilization and reconstruction (S&R) operations. This creates a poor working relationship and lack of trust between NGOs and NATO military forces.¹⁵

Finally, with regard to S&R operations, NATO has failed to produce a doctrine (or agree on an established one) at the Alliance level. In fact, within the last NATO Strategic Concept published in 2010, the gap is clearly identified:

To be effective across the crisis management spectrum, we will... further develop doctrine and military capabilities for expeditionary operations, including counterinsurgency, stabilization and reconstruction operations.¹⁶

Again, however, NATO's consensus-driven decision-making continues to impede progress. Lacking a common strategy recognized by all members of the Alliance, operational planning is often ad hoc, rushed, and subject to mission creep.¹⁷ These pitfalls are easily identifiable in all of NATO's out-of-area interventions since the end of the Cold War, including Kosovo, Afghanistan, and Libya. Without a common strategy within the Alliance, S&R operations often suffer from duplicative and contradictory strategies.

Information Needed to Support S&R Operations

Support for an S&R operation will undoubtedly require NATO to work with and in support of the host nation government, relevant IOs, and a range of NGOs to address a wide range of security and humanitarian concerns. Because NATO has yet to appropriate or produce a comprehensive S&R doctrine, we utilize the end

¹³ Interview with Source K, US DoD official, March 16, 2016.

¹⁴ Interview with Source N, US Mission to NATO, March 17, 2016.

¹⁵ Interview with Michael Klosson, VP for Policy and Humanitarian Response, Save the Children, April 18, 2016.

¹⁶ See Annex A.

¹⁷ Interview with Dr. Charles (Chuck) Barry, Distinguished Research Fellow, Institute for National Strategic Studies, US National Defense University, January 20, 2016.

states and cross-cutting principles outlined in *Guiding Principles for Stabilization and Reconstruction* to outline the efforts to which NATO is most likely to provide support.¹⁸ This manual offers a general framework for addressing complex environments of instability and identifies common gaps and challenges to conducting S&R operations.

NATO’s humbling experiences in Kosovo and Afghanistan have made it very clear that emphasis must be placed on political primacy. By adopting military-dominated strategies, NATO unintentionally allowed governance issues that preceded drivers of insecurity to remain unaddressed. In order to close this self-reinforcing feedback loop, it is necessary that NATO is prepared to take on not only security roles but also play a supportive role to civilian-led S&R operations. In this way, NATO will be supporting a unified effort to build the governing capacity of the host nation government by positioning itself in such a manner that

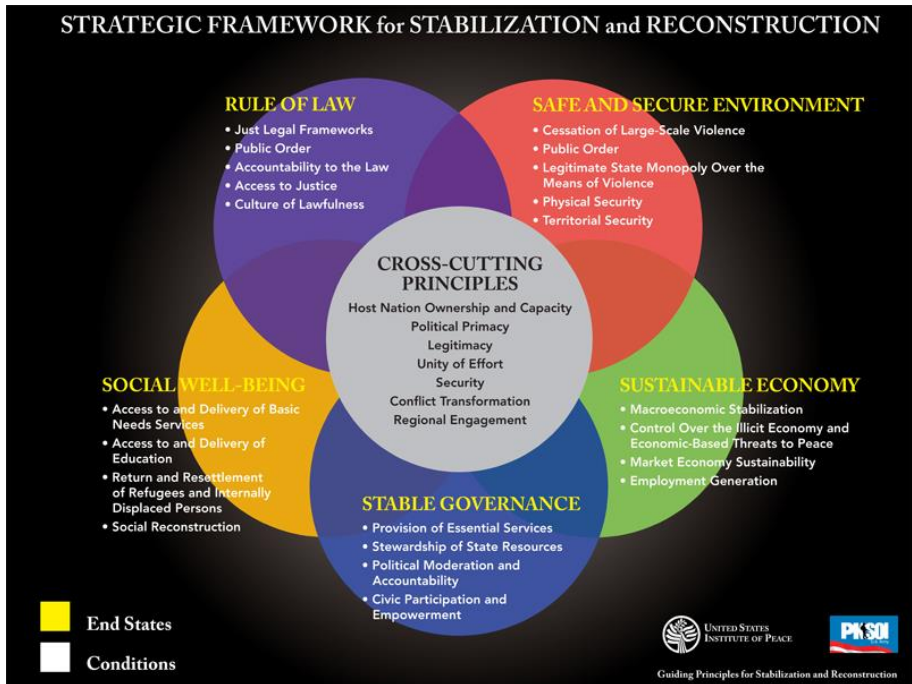


Figure 1: Strategic Framework for Stabilization and Reconstruction.

¹⁸ Developed by the United State Institute for Peace (USIP) and the United States Army Peacekeeping and Stability Operations Institute (PKSOI) in 2009. Annex B outlines a more detailed role for NATO in S&R operations as well as excerpts on the necessary conditions for each endstate. The full electronic version can be downloaded at http://www.usip.org/sites/default/files/guiding_principles_full.pdf.

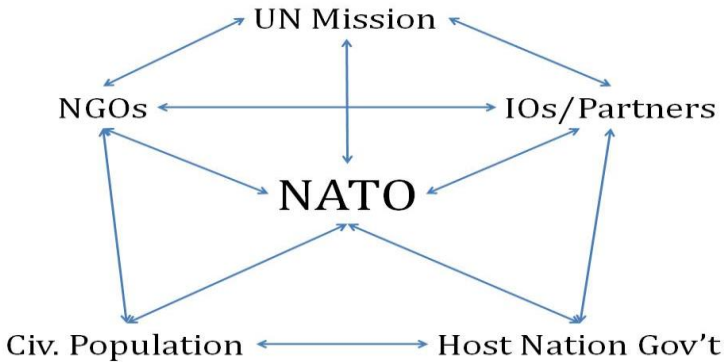


Figure 2: NATO in Relation to Non-NATO Entities.

leverages its unique capabilities in intelligence and information gathering, along with command and control, strategic lift, and communications technologies.

To achieve this goal, NATO will need to gather, analyze, and disseminate spatial information related to refugees, internally displaced persons (IDPs) and other at-risk populations, damaged housing and critical infrastructure, formal and informal border crossings, and hazardous material sites. NATO will require robust engagement with NGOs, IOs, the civilian population, and the host government in order to obtain the information necessary to support a successful S&R operation.

Options for NATO

The biggest challenges facing NATO will center on the degree to which it can collect, process, and disseminate information not only within NATO, but also with the range of non-NATO entities working together toward a successful S&R operation. How NATO chooses to organize its contribution will present different implications for the mission as a whole. In the following section, we analyze three options for NATO strategy specific to intelligence and information sharing in both in-area and out-of-area S&R operations. The options are presented in increments: each one builds on the previous option and requires an increased degree of financial, material, and human contribution.

Option A. The Federated Mission Network (FMN)

Subject: A packaged, distributable network that can be used simultaneously by NATO and its partners to share classified intelligence, and by IOs, NGOs, and NATO actors to share unclassified information in a common, minimally regulated space.

Description

NATO established the Afghan Mission Network (AMN) in 2010. It provided a federated, classified network that allowed all NATO member states contributing forces to the International Security Assistance Force (ISAF) mission to exchange data and intelligence. Certain non-NATO states were then read on to the AMN using bilateral security agreements. However, ISAF partners continued to struggle with sharing information with non-NATO actors providing much-needed services in Afghanistan. Efforts to use unclassified interfaces, including the All Partners Access Network (APAN), Civil-Military Fusion Center (CFC), Protected Information Exchange (PIX), and RONNA-HarmonieWeb, did not resolve recurring issues of structural obstacles or lack of buy-in.¹⁹

NATO has since endeavored to develop a hybrid network, known as the Federated Mission Network (FMN), to hold both classified and unclassified material on a single network.²⁰ As the FMN is still under development, this paper will outline what functions and considerations should be taken into account for the final product:

- A labeling scheme allowing registered users to submit information across the classification spectrum, and an access management scheme to limit information by clearance level
- A layered archive and search function to store classified intelligence at the NATO Top Secret, NATO Secret, NATO unclassified, and open source levels, respectively
- A user-generated, Wiki-type database for unclassified information, with an open edit function regulated by a NATO administration team²¹
- Chat functions across the classification spectrum to provide for direct communication between users
- A fillable-forms portal allowing NATO and non-NATO entities to submit requests for information (RFIs) in both directions, and
- A financial trust fund management function for tracking donations, pairing needs with resources using an open proposal scheme.

The resulting network would take the form of a distributable, off-the-shelf product that NATO could deploy to areas of instability and be used by NATO and non-NATO entities simultaneously.

Pros

¹⁹ Interview with Melissa Sinclair, former USAID employee and NGO worker, April 7, 2016.

²⁰ Interview with Jean-Rene Couture, NATO Communications and Information Agency, March 17, 2016.

²¹ These standards include, among others, the stipulation that deliberate attempts to spread disinformation or engage in cyber-vandalism will result in the removal of editing privileges by the site's administration team.

Firstly, the FMN brings multiple actors onto a common network and provides different levels of access to vetted users. Through the RFI function, the FMN provides an open line of communication, albeit indirectly, for requesting specific information from NATO and vice-versa. Admittedly, not all requests will be approved, especially when the sources and methods used to obtain the information requested are particularly sensitive. Further, the Wiki function establishes a one-stop clearinghouse for open-source and unclassified information, opening new channels for information exchange.

Secondly, the donations management function, modeled after the Afghanistan Reconstruction Trust Fund, will improve the efficiency of resource allocation and will limit cases of fraud.²² This mechanism holds all registered monetary donations in a common account managed by the overarching political lead in a S&R context, be it the host nation government, a UN support mission, or another entity. Because all entities supporting the overall S&R operation will have access to the information contained in this element, the opportunity for graft, embezzlement, and misallocation is greatly reduced. The Request for Proposal (RFP) function allows local and foreign actors to post needs, ranging from reconstruction projects to training seminars, and for NGOs to compete for resource awards designed to fulfill specific, widely identified needs.

Finally, by developing a packaged, distributable network, NATO will be able to deploy the FMN alongside the initial contingent of NATO personnel sent to a S&R environment. From the first day of an operation, the FMN can be installed, activated, and have all dysfunctional elements worked out as the full scope of the mission is being developed. The FMN can be set up in multiple locations at once, using dedicated communications systems to manage operations separately. In this way, NATO can support multiple S&R, disaster relief, humanitarian aid, and other operations simultaneously.

Cons

The most obvious risk to the FMN's common network structure is its increased vulnerability to hacking compared to closed networks. Despite a plethora of advanced network security products available, and the likelihood of even more advanced measures reserved for individual customers, the threat of hacking is inherently greater than with air-gapped networks. Moreover, awareness of a hacking incident is normally delayed by hours at the least, meaning sensitive information obtained through nefarious means has the potential to be used against NATO before the Alliance becomes aware of the intrusion.

²² "The Afghanistan Reconstruction Trust Fund (ARTF) was established in 2002 to provide a coordinated financing mechanism for the Government of Afghanistan's budget and priority national investment projects. Today, the ARTF remains the vehicle of choice for pooled funding, with low transaction costs, excellent transparency and high accountability, and provides a well-functioning arena for policy debate and consensus creation." Quoted from <http://www.artf.af/>.

A second challenge is NATO's ability to design and fund the development of a FMN. There can be no certainty that NATO member states will be able to come to a consensus on the technical specifications of the FMN's sharing functions. Past approaches have always included separate, or air-gapped, networks for housing classified and unclassified information, respectively. Judging by NATO's enduring reliance on a centralized paper records policy, due to its inability to agree on digital storage standards,²³ member states are unlikely to agree on the structure of the FMN. It is also unlikely that all NATO member states will be willing and able to declassify information on a network shared with states, IOs, and NGOs with which there may be sour relations. Additional obstacles include how to train and pay the analysts and disclosure officers tasked with transferring information between classification layers.²⁴

Finally, the FMN provides a mere technical solution to a much larger policy problem. Should NATO even come to agreement on its design, there is no guarantee that NGOs will buy in to the common network idea. Especially dubious is the assumption that all contributing entities to an S&R operation will be de facto allies. Some NGOs may be willing to contribute information to the network, but with the stipulation that certain NATO member states or IOs be barred from viewing it. Gaining the buy-in from the host-nation government itself is not guaranteed. To repurpose a line from *Field of Dreams*,²⁵ "If you build it, they will come," may not apply to the development of the FMN.

Option B. The Joint Information Fusion Center

Subject: The Joint Information Fusion Center (JIFC) is a centralized facility through which NATO collects, processes, and analyzes intelligence and information. The JIFC would be capable of analyzing both threat activity and atmospheric information. Acting as a physical clearinghouse, with dedicated personnel, it is a mechanism to help create a more focused civilian-military coordination effort.

Description

The JIFC will be staffed with intelligence analysts to conduct both threat assessments and atmospheric analyses relating to the wellbeing, governance, infrastructure, and economy of the local populace.²⁶ While the analysts conducting threat assessments will work in access-restricted areas, those conducting atmospheric analyses will be involved in fieldwork by meeting with active

²³ Interview with Catherine Gerth, Head of Archives and Information Management, NATO HQ, March 17, 2016.

²⁴ Interview with Catherine Gerth.

²⁵ Universal Studios' 1989 movie directed by Phil Alden Robinson.

²⁶ Michael T. Flynn, Matthew F. Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, D.C.: Center for a New American Security, 2010), 17-18, www.dtic.mil/dtic/tr/fulltext/u2/a511613.pdf, accessed June 12, 2017.

contributors to the S&R operation. This will allow NATO personnel to gain an on-the-ground understanding of the situation and exchange information regarding known threats to S&R projects throughout the conflict area.²⁷ These analysts would then collate information into cogent, unclassified products and disseminate the information to the widest audience possible, perhaps using the FMN.²⁸ These analysts would act as "...information integrators vacuuming up data already collected by military personnel or gathered by civilians in the public realm and bringing it back to a centralized location."²⁹

The intelligence analysts within the JIFC would be comprised of National Intelligence Cells (NICs). NICs are made up of intelligence analysts from individual NATO member states (i.e. Italian NIC, Spanish NIC, etc.).³⁰ Ideally, each NATO nation involved in a S&R operation would have its own NIC in the JIFC that could conduct their work on the FMN while retaining the capability to 'reach back' to their national intelligence architecture.³¹ Theoretically, the JIFC could also include disclosure officers whose sole duty is to facilitate the downgrading of national intelligence to transferrable levels.³² A subsequent tier of officers would consider how to transfer that information or intelligence from national networks to the FMN and vice-versa, otherwise known as 'air-gapping.'³³ This would provide safeguards against spillage.

Recently, NATO acquired an Alliance Ground Surveillance (AGS) system comprised of five Global Hawk unmanned aerial vehicles (UAVs). These assets will allow the JIFC to collect and 'own' aerial imagery intelligence (IMINT), which is a critical element to individual S&R projects focused on security, large-scale infrastructure repair, border control, etc. Memorandums of understanding (MoUs) will outline which NATO member states dedicate trained personnel to analyze the information collected by those assets.³⁴ These MoUs would further clarify that the JIFC commander has the authority to share the information gathered with members of the Alliance, non-NATO states involved in the S&R operation, and with outside observers.

Lastly, the JIFC would have a physically separate and unclassified facility in which NATO leaders and intelligence analysts could hold meetings with civilian agencies, NGOs, or private entities. This facility would serve as a location for high-level coordination meetings between NATO leadership and other parties involved. In addition to civil-military coordination, this facility could also be used

²⁷ Flynn, Pottinger, and Batchelor, *Fixing Intel*, 19.

²⁸ Interview with LTC Karsten Vestergaard, CIMIC Director at NATO ARRC, March 15, 2016.

²⁹ Flynn, Pottinger, and Batchelor, *Fixing Intel*, 19.

³⁰ Interview with Source J, March 14, 2016.

³¹ Interview with Source B, non-US official at NATO ARRC, March 14, 2016.

³² Interview with Source P, US DoD official, March 8, 2016.

³³ Interview with Source A, US DoD official, March 8, 2016.

³⁴ Interview with Col. James Saddler, Deputy Assistant Chief of Staff, G-5 Plans and Policy at NATO ARRC, March 15, 2016.

as a meeting place to hold discussions between host nation government entities, NATO, NGOs, civilian agencies, and private firms, ensuring complete synchronization with all stakeholders in the region.

Pros

The JIFC has the potential to provide a robust information and intelligence clearing house between NATO members, civilian agencies, NGOs, and private entities. The freedom of information sharing, particularly on the unclassified side, would allow entities to collaborate at an unprecedented level, ensuring a high degree of civil-military unity of effort. In past operations and exercises, the existence of a separate, unclassified area for civil-military coordination received increased buy-in from involved actors, especially NGOs, as they found the information exchange beneficial for their missions or projects.³⁵ The information shared among NATO allies would create a shared, holistic understanding of the S&R environment.³⁶

The NICs allow intelligence analysts to collaborate with fellow analysts from their nation in a secured environment. The 'reach back' capability allows forward deployed analysts to request complex analysis from their respective national intelligence agencies. While the proximity to other NICs will foster an environment for collaboration among NATO analysts, the physical security protocols will protect against spillage or direct efforts to obtain classified information. The dedication of disclosure and safeguard officers would increase the speed at which information is approved for release to, or sharing with, the desired network or audience. Such measures reduce the lag time in which information can be transferred between networks and increases the timeliness of intelligence products.³⁷

By allowing NATO to 'own' more intelligence collection assets, the delay in disseminating information will be reduced at the operational and tactical levels. NATO operational commanders would have access to collection assets, such as UAVs, which he or she can directly task to fulfill intelligence gaps and share with other member states and non-NATO entities involved in the operation. This capability increases the utility of NATO's intelligence products and will further incentivize information sharing between NATO and non-NATO entities by offering enhanced information collection capability to all those involved.

Cons

A major obstacle to successful implementation of the JIFC model is fielding a properly trained staff. In the event multiple NATO intelligence units are deployed simultaneously, they would be considerably under strength in terms of intelligence analysts and other critical staff functions.³⁸ Thus, a NATO JIFC could

³⁵ Interview with LTC Karsten Vestergaard, CIMIC Director, NATO ARRC, March 15, 2016.

³⁶ Interview with Source A, US DoD official, March 8, 2016.

³⁷ Interview with Source K, US DoD official, March 16, 2016

³⁸ Interview with Source L, non-US official at NATO ARRC, March 14, 2016.

find itself with an insufficient number of personnel to conduct the necessary analyses. This personnel shortage would be difficult to overcome, especially in the event of a renewed threat from Russia. With Russia becoming more of a concern for NATO members, it is increasingly unlikely that many of the smaller member states would provide personnel support to an out of area S&R operation, leaving the burden to the wealthier and larger NATO members.

Another obstacle is the continued unwillingness of nations to share information. Though NATO member states and non-NATO states are more likely to share unclassified information during an S&R campaign, there will still be hesitancy to share developed intelligence products. This is increasingly true for the United States, where intelligence leaks by Bradley Manning and Edward Snowden have resulted in tighter intelligence sharing access. Today, intelligence professionals often possess an increased apprehension to intelligence sharing for fear of breaking federal laws or contributing to intelligence spillage.³⁹

Compounding this hesitancy to share is the slow process by which many member nations approve intelligence for release. The US has a rather liberal sharing policy in terms of empowering lower echelons to share information, compared to many other NATO member states. In fact, many NATO members do not possess occupational specialties in military intelligence, and those that do often have no foreign disclosure standards. As a result, analysts tend to overclassify their work. When asked to share intelligence products, analysts with no disclosure training are required to request authorization from their national agencies. The time it takes for this turnaround often renders the intelligence useless.⁴⁰

Getting NGO buy-in is the main concern. The establishment of a JIFC in and of itself will not necessarily encourage NGOs to share information with NATO. Based on research, NGOs and other civilian agencies are willing to work with NATO forces only once they experience the benefits gained from information sharing. Not only does this exchange of information help to establish a greater security environment, it also enables coordination amongst them and other organizations and agencies to more effectively and efficiently coordinate projects.

Option C. Regional Coordination Centers and Stability and Reconstruction Teams

Subject: The Regional Coordination Center (RCC) and Stability and Reconstruction Team (SRT) would coordinate civil-military efforts at a regional level. The role of the SRTs is to carry out reconstruction efforts within RCC areas of responsibility.

³⁹ Anna-Katherine Staser McGill and David H. Gray, "Challenges to International Counterterrorism Intelligence Sharing," *Global Security Studies* 3, no. 3 (2012): 76-86, quote on pp. 83-84.

⁴⁰ Interview with Source B, non-US official at NATO ARRC, March 15, 2016.

Description

The Regional Command (RC) model was used in Afghanistan to coordinate all regional civil-military activities conducted by the military elements of the PRTs in their area of responsibility, under the control of ISAF.⁴¹ Each RC had an established command and control component that provided logistical support for civilian projects within the RC's area of responsibility. Subcomponents of the RC, the Provincial Reconstruction Teams (PRTs) were "joint-civil military organizations that aspired to promote progress in governance, security, and reconstruction."⁴² At the operational level, the RC developed coordinated lines of effort between civilian agencies, private firms, NGOs, and ISAF. At the tactical level, the PRTs conducted S&R activities such as building schools, police stations, repairing infrastructure, and other projects.⁴³

Changing the nomenclature to Regional Coordination Center and Stability and Reconstruction Team recognizes that political considerations, not military end-states, have primacy in S&R operations. However, by retaining a similar organizational structure to the RC model, the proximity of actors and close coordination maintains an environment conducive to information sharing. This proximity includes collaborative interactions such as daily briefings, intra-agency reporting requirements, and informal information exchanges. Furthermore, NATO would not attempt to subordinate NGOs and other non-NATO actors, but instead incorporate their unique skills and resources into the larger effort. This acknowledges the neutral space between political and military objectives that NGOs often occupy.

Pros

The relationship established between NATO forces and NGOs under the RCC and SRT model would be mutually beneficial. The security and logistical capability provided by the RCC would allow civilian agencies, NGOs, and even private enterprises to conduct their operations under the security of NATO forces. In turn, the governance and reconstruction efforts of the civilian agencies, NGOs, and private entities could create a more secure and stable environment. The close vicinity of actors would facilitate information pertaining to security and atmospheric being shared between NATO forces and civilian entities. NATO forces could coordinate logistical capabilities between military and civilian entities as well as facilitate coordination amongst each other via communication technologies.

⁴¹ ISAF Regional Command Structure, October 22, 2009, accessed June 10, 2017, http://www.nato.int/ISAF/structure/regional_command/.

⁴² Robert Perito, *U.S. Experience with Provincial Reconstruction Teams in Afghanistan: Lessons Identified*, Special Report 152 (U.S. Institute of Peace, October 2005), 6.

⁴³ Kristian Fischer and Jan Top Christensen, "Improving Civil-Military Cooperation the Danish Way," *NATO Review* (Summer 2005), <https://www.nato.int/DOCU/review/2005/Peace-Building/civil-military-cooperation-Danish/EN/index.htm>.

An example of such information sharing occurred in 2011, when the US 82nd Airborne Division headquarters assumed responsibility of RC South. At the time, the Headquarters and its subordinate forces were focused on fighting Taliban forces in the area, leaving few military personnel to assist in reconstruction operations. However, the PRTs operating in the area provided invaluable information concerning infrastructure, social well-being, and governance in areas where ISAF forces did not have the manpower to operate. Likewise, the Division Headquarters was able to relay information to the PRTs and NGOs concerning the security environment, a necessity given the amount of violence occurring in the area at the time.⁴⁴

The RCC concept allows NATO to implement some of the more flexible aspects of its intelligence sharing structure. Though NATO may be the primary security provider in a S&R operation, the involvement of other non-NATO states will require inclusion into planning and information sharing efforts. The RCC commander can facilitate the signing of security assurance agreements, which outline the limits to which non-NATO states can receive and utilize shared intelligence.⁴⁵ The same goes for NGOs; the RCC commander has the discretion to share information with any party that could benefit from it. The empowerment of the RCC commander to approve intelligence and information sharing circumvents otherwise lengthy bureaucratic processes and allows them to manage access to intelligence and information as contributing entities in S&R operations come and go.⁴⁶

Cons

The RCC concept does not provide for a unity of civil-military effort at the national level. Rather, each RCC is led by a different NATO member state, subjecting operations and information sharing to the perceived needs of that particular nation's military and political priorities. In Afghanistan, "American PRTs had less than 100 personnel and stressed force protection and quick impact assistance projects... [the] British PRT was somewhat larger, emphasized Afghan security sector reform, and helped defuse confrontations between rival warlords... [the] German PRT had over 300 members and was strictly bifurcated between its military and robust civilian component."⁴⁷ Lacking a central authority to guide RCCs, each individual SRT will succeed or fail based on chance rather than strategy.⁴⁸

The RCC model does not guarantee buy-in from NGOs, especially those who wish to maintain the appearance of neutrality or whose reputation is built upon their independence from military forces. Larger NGOs have coordinated with

⁴⁴ Interview with Source A, US DoD official, March 8, 2016.

⁴⁵ Interview with Catherine Gerth, March 17, 2016.

⁴⁶ Interview with Source C, non-US official at NATO ARRC, March 15, 2016.

⁴⁷ Perito, *U.S. Experience with Provincial Reconstruction Teams*, 3.

⁴⁸ Michael J. McNerney, "Stabilization and Reconstruction in Afghanistan: Are PRTs a Model or a Muddle?" *Parameters* 35, no. 4 (Winter 2005-06): 32-46.

NATO to varying degrees at the RC level and will likely do so in the future. Others will be resistant to cooperate with the RCC in future operations due to intractable concerns about neutrality. The RCC also has the potential to be overwhelmed by an encumbering cornucopia of actors, hampering effective civil-military coordination. Further, there is no guarantee that smaller entities will understand how to interact with the RCC, in which case the smaller entity could place itself and its members at risk.⁴⁹

Findings

NATO has demonstrated that it is aware of the issues regarding information sharing with NATO and non-NATO members and is working to correct them. Through trial and error, NATO has developed many ad-hoc policies and mechanisms for sharing information in crises. Despite this, many common obstacles remain persistent. Intelligence sharing within the alliance remains problematic and each organization has a lack of incentive to share. Agencies have internal rules against sharing and no rewards for sharing. For the individual analyst, there are only risks for disclosing information to foreign partners.

Although NATO and NGOs are increasingly working together in theaters such as Kosovo and Afghanistan, barriers to effective information sharing remain. NATO forces encounter difficulty collaborating with situational “partners of opportunity” that arise from the NGO community upon the initiation of S&R operations. Some NGOs, in fact, may have been working in the area for several years or have goals that do not align with overall S&R objectives. Many NGOs are simply hesitant to collaborate with military forces due to perceptions that it may compromise their neutrality and credibility.⁵⁰ However, as NGOs feel they are gaining valuable information through information exchanges, they are increasingly likely to collaborate with NATO.⁵¹ Furthermore, NGOs are coming to the realization that more locations throughout the world are becoming increasingly hostile, even towards NGOs.⁵² With an increasing threat towards NGOs, there is an increased necessity to forge relationships between them and NATO. Finally, NATO and military units writ large must stop referring to NGOs as force multipliers or enablers. Doing so disenfranchises NGOs and distorts their stated neutrality.⁵³ Rather, NATO must view NGOs as partners and establish mutually beneficial relationships with them.

Where the US and UK militaries each have a professional intelligence corps within their military structure, other NATO member states do not. For many nations, this issue stems from a lack of resources, either fiscally or simply not having the collection capability to justify an intelligence corps. To remedy this

⁴⁹ Interview with Source A, US DoD official, March 8, 2016.

⁵⁰ Interview with Melissa Sinclair, former USAID and NGO worker, March 7, 2016.

⁵¹ Interview with LTC Karsten Vestergaard, CIMIC Director, NATO ARRC, March 15, 2016.

⁵² Interview with Melissa Sinclair, former USAID and NGO worker, March 7, 2016.

⁵³ Interview with Michael Klosson, Save the Children, April 18, 2016.

lack of intelligence professionals, Alliance members will often assign officers and enlisted soldiers from other branches (i.e. infantry, engineers, fighter pilots) to intelligence positions, with their first intelligence duty sometimes coming late in their careers. Though these officers and enlisted personnel are intelligent and capable individuals, they lack experience in intelligence collection, analysis, and dissemination. This slows the rate at which intelligence is shared, as the individuals must first learn their own intelligence architecture and rules for sharing information.⁵⁴

Many NATO member states have a stovepiped, bureaucratic process to approve the release or classification downgrade of national intelligence products. This sluggish process often results in intelligence losing timeliness. Most NATO states do not have an equivalent position to the US Foreign Disclosure Officers (FDOs) that are trained in US classification regulations and their caveats. FDOs understand what level of intelligence can be shared with other nations and how to release unclassified portions of classified products. However, the process of requesting authority to share intelligence from an external agency can be lengthier still.

Recommendation

A review of the pros and cons associated with the three options supports the Joint Information Fusion Center (JIFC) as NATO's optimal choice for enhancing the sharing of information and intelligence. Although each option builds on the others, shortcomings in policy bandwidth and obstacles to doctrine formation in the FMN and RCC options, respectively, diminish their utility for NATO in a doctrinal sense. The JIFC confers benefits to NATO ability to support S&R operations in both in-area and out-of-area environments.

Mentionable differences exist between in-area and out-of-area operations. In-area operations feature concerns about sovereignty and the unwillingness of the host nation (a NATO member) to relegate authorities to external actors. Such dynamics can obstruct efforts at coordination. Further, the host nation engages in information sharing agreements at potentially significant domestic political cost. Sharing information in out-of-area operations, such as those executed by KFOR and ISAF, can be easier because of the relative absence of sovereignty issues for participating NATO member states. However, concerns by NATO members about protecting sources and methods can still hinder information sharing between partners. In addition, poor relationships between NATO states and other stakeholders can sometimes preclude information sharing. Considering the rising concern among some of NATO's eastern members about hybrid threats coming from Russia, a doctrine that can be applied to both in-area and out-of-area operations is more likely to receive their support.

⁵⁴ Interview with Source M, non-US Official at NATO ARRC, March 15, 2016.

Advocacy

The creation of the JIFC is the only option with a reasonable chance of being developed into doctrine for information sharing. As a purely technical option, the FMN alone fails to provide NATO members with adequate guidance and processes for information sharing in S&R operations. A better network does not address the challenges posed by a lack of trained intelligence personnel. Nor does it guarantee that the information transiting the network will be actionable. The tendency to over-classify, lacking buy-in incentives, and other endemic obstacles cannot be overcome by merely boosting the bandwidth for sharing.

On the other hand, the RCC concept is an oversized doctrinal option because it is heavily affected by context: different geographic environments will require different considerations and distinct RCC models. For example, a RCC model deployed to S&R operations on NATO's southern periphery will not necessarily be as applicable to that on NATO's eastern periphery. For these reasons, NATO will encounter difficulty incorporating the RCC concept into a doctrine that can be applied to both in-area and out-of-area operations.

Following through on the JIFC concept will grant NATO improved processes for sharing information within and outside the alliance during S&R operations. As a centralized center with personnel dedicated to managing disclosure and air gapping, the JIFC has mechanisms that encourage a better flow of information between NATO members and protection against inadvertent spillage. The inclusion of an off-site location for face-to-face meetings with NGOs and IOs can also help foster information transfer between military and non-military entities involved in S&R. Because the JIFC will be operational at all hours, it will foster a cadre of analysts familiar with atmospheric analysis and processes for intelligence moving.

Where the JIFC succeeds is in its flexibility, deployability, and its refrain from necessarily compromising intelligence or the sovereignty of the host nation. The physical risk of spillage or espionage is greatly reduced using the NIC model where only personnel from that respective state can physically have access to national intelligence networks and information. Furthermore, having trained FDOs will help to ensure only authorized intelligence is being shared or released to NATO and other parties.

Response to Counterarguments

Consensus-driven decision-making could potentially weaken the role and capabilities of the JIFC, making it a less capable asset to NATO in a S&R operation. However, NATO has a precedent for establishing the JIFC vis-à-vis the NATO Intelligence Fusion Center (NIFC). Focusing on out-of-area NATO operations, the NIFC consolidates intelligence efforts from member states at one location. The NIFC exemplifies the fact that NATO member states can and will share intelligence within certain security structures. The capability that it currently lacks is

an information sharing aspect with NGOs and other entities outside of NATO member states.

NGOs could forego sharing with the JIFC due to concerns about their neutrality, diminishing the amount and quality of information exchanged. Improvements in this area will require better familiarization and recognition of NGO needs by NATO's higher offices. Despite this, some attributes of the JIFC facilitate better cooperation between both parties. The JIFC's neutral meeting site for analysts and civilian groups working in country can help build familiarity between both parties. Repeated face-to-face meetings can foster a better understanding of NGO capabilities and concerns, and vice-versa. The information exchanged through the JIFC would also be mutually beneficial and contribute to a perception of equality between NGOs and NATO. Better familiarization and communication would improve both parties' ability to respond in complex S&R operations.

The quality of information and intelligence disseminated by the JIFC could suffer if participating NATO members decline to share intelligence. Collection is one of the essential tasks of an intelligence agency, and safeguarding the capabilities of operatives, UAVs, and sensors is of paramount importance. The National Intelligence Cells within the JIFC are designed to expedite this process through the training of disclosure officers, by building relationships between personnel on the ground, and by providing reach-back. However, the JIFC itself will be unlikely to overcome the national proclivity to protect sources and methods. This obstacle may be ameliorated by the appointment of a NATO civilian director of intelligence, as outlined in Annex C. This position could provide a senior-level authority that could advocate for greater intelligence sharing and reform.

Implementation

The foremost task is for NATO to develop the personnel and equipment requirements for the establishment of the JIFC. These requirements can be determined through current intelligence commanders and other staff members relaying what they feel the requirements are. Because different offices will provide different requirements, NATO HQ in Brussels will need to determine the baseline personnel and equipment requirements for the establishment of a JIFC. Finally, NATO will need to produce the cost estimate and request member states to fill the billets and equipment requirements.

Based on the authors' research, it is likely the JIFC will require approximately 100-120 intelligence personnel. However, personnel numbers can increase as more nations become involved in an operation. These would be comprised of all-source, signals, imagery, and human intelligence analysts. Additionally, there would be individuals dedicated to establishing and maintaining a civil-military relationship with both non-military governmental agencies and NGOs alike. Furthermore, the JIFC would need to be self-sustaining with power generation,

vehicles, and tents. This equipment would cost approximately USD 45 million and would increase as the JIFC established more permanent site operations.

Before being indoctrinated, NATO should conduct a two-year test period of the JIFC after it is fully staffed and operational. A two-year period is recommended because of the difficulty associated with training intelligence analysts, establishing standard operating procedures, and gaining a general understanding and comfort with billet specific duties and responsibilities. This should be established in a garrison environment at either of the NATO Response Force (NRF) headquarters in Brunssum or Naples, or at the ARRC in the UK. A two-year test period will allow NATO to determine where personnel and equipment shortages exist. Furthermore, this will allow the JIFC to be tested in training exercises to determine its viability not only through the lens of NATO but also civilian partners and non-state actors as well.

After the two-year test period NATO should examine viability of the test JIFC and address shortcomings of the test period. After shortcomings have been identified, NATO should codify the requirements, role, and responsibilities for the JIFC so that it can become part of NATO doctrine and planning efforts. Once codified, NATO should operationalize a JIFC at the ARRC and the NRF headquarters in Brunssum and Naples. These headquarters are ideal for a JIFC because of the role they play in crisis response.

Because the JIFC will be beneficial to all members of the alliance, funding for the JIFC will come out of the NATO military budget, which is directly funded by NATO member states. Though the costs associated with establishing and operating a JIFC are undetermined at this time, cost estimates will be easy to establish once NATO has identified its personnel and equipment requirements for the JIFC. In the meantime, NATO can use existing costs of its headquarters to begin cost analysis of the JIFC.

As with any other commonly funded program, the JIFC will need to be unanimously approved by the NAC. Given that NATO members perceive threats with varying degrees of importance, unanimous approval of the JIFC and its funding could prove to be a difficult task. Where some NATO members view S&R operations with a critical role in NATO strategy, others view the traditional conventional threat, particularly Russia, as the primary threat to NATO and feel it should constitute the bulk of NATO's attention and financial resources. As more member states begin to contribute 2% of their GDP, as they have pledged, NATO funds will increase to a size appropriate to support NATO efforts to counter conventional threats and properly plan for future S&R operations.

Annex A. NATO Strategic Concept 2010, S&R Excerpts ⁵⁵

- “It commits the Alliance to prevent crises, manage conflicts and stabilize post-conflict situations, including by working more closely with our

⁵⁵ NATO Strategic Concept 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

international partners, most importantly the United Nations and the European Union.” (p. 4)

- “Instability or conflict beyond NATO borders can directly threaten Alliance security, including by fostering extremism, terrorism, and transnational illegal activities such as trafficking in arms, narcotics and people.” (p. 11)
- “Crises and conflicts beyond NATO’s borders can pose a direct threat to the security of Alliance territory and populations. NATO will therefore engage, where possible and when necessary, to prevent crises, manage crises, stabilize post-conflict situations and support reconstruction.” (p. 19)
- “The lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximize coherence and effectiveness of the overall international effort.” (p. 19)
- “Even when conflict comes to an end, the international community must often provide continued support, to create the conditions for lasting stability. NATO will be prepared and capable to contribute to stabilization and reconstruction, in close cooperation and consultation wherever possible with other relevant international actors.” (p. 20)
- “To be effective across the crisis management spectrum, we will:.. further develop doctrine and military capabilities for expeditionary operations, including counterinsurgency, stabilization and reconstruction operations.” (p. 21)
- “We are firmly committed to the development of friendly and cooperative relations with all countries of the Mediterranean, and we intend to further develop the Mediterranean Dialogue in the coming years. We attach great importance to peace and stability in the Gulf region, and we intend to strengthen our cooperation in the Istanbul Cooperation Initiative.” (pp. 30-31)

Annex B. Guiding Principles, End States and Necessary Conditions

Safe and Secure Environment – Ability of the people to conduct their daily lives without fear of systematic or large-scale violence. This end state includes the majority of conditions that NATO is prepared to support. NATO has the capability to provide training and technical support to the development of host nation armed forces as they work to separate warring parties, negotiate sustainable cease-fires, and establish disarmament, demobilization, and reintegration (DDR) programs. In addition, NATO possesses the unique ability to transport troops and

Necessary Conditions:

- *Cessation of Large-Scale Violence* is a condition in which large-scale armed conflict has come to a halt, warring parties are separated and monitored, a peace agreement or ceasefire has been implemented, and violent spoilers are managed.
- *Public Order* is a condition in which laws are enforced equitably; the lives, property, freedoms, and rights of individuals are protected; criminal and politically motivated violence has been reduced to a minimum; and criminal elements (from looters and rioters to leaders of organized crime networks) are pursued, arrested, and detained.
- *Legitimate State Monopoly Over the Means of Violence* is a condition in which major illegal armed groups have been identified, disarmed and demobilized; the defense and police forces have been vetted and retrained; and national security forces operate lawfully under a legitimate governing authority.
- *Physical Security* is a condition in which political leaders, ex-combatants, and the general population are free of fear from grave threats to physical safety; refugees and internally displaced persons can return home without fear of retributive violence; women and children are protected from undue violence; and key historical or cultural sites and critical infrastructure are protected from attack.
- *Territorial Security* is a condition in which people and goods can freely move throughout the country and across borders without fear of harm to life and limb; the country is protected from invasion; and borders are reasonably well-secured from infiltration by insurgent or terrorist elements and illicit trafficking of arms, narcotics, and humans.

humanitarian aid to areas in need of population and infrastructure protection. Finally, NATO can provide command and control assets using its Airborne Early Warning and Control System (AWACS) to assist host nations in efforts to secure its borders and manage spoilers.

Rule of Law – Ability of the people to have equal access to just laws and a trusted system of justice that holds all persons accountable, protects their human rights and ensures their safety and security. As a military alliance primarily focused on the collective defense of its member states, NATO will, admittedly, contribute less to the conditions necessary to promote the rule of law than in other sectors. Still, NATO possesses a wealth of experience in training indigenous law enforcement and national guard units resulting from its work in Kosovo, Afghanistan, and Iraq. A distinction here exists between primary security responsibilities that are not appropriate for police units, such as emergency response, explosive ordinance disposal, and the management of hazardous materials.

Necessary Conditions:

- *Just Legal Frameworks* is a condition in which laws are consistent with international human rights norms and standards; are legally certain and transparent; are drafted with procedural transparency; are equitable, and are responsive to the entire population, not just powerful elites.
- *Public Order* is a condition in which laws are enforced equitably; the lives, property, freedoms, and rights of individuals are protected; criminal and politically motivated violence has been reduced to a minimum; and criminal elements (from looters and rioters to leaders of organized crime networks) are pursued, arrested, and detained.
- *Accountability to the Law* is a condition in which the population, public officials, and perpetrators of past conflict-related crimes are held legally accountable for their actions; the judiciary is independent and free from political influence; and horizontal and vertical accountability mechanisms exist to prevent the abuse of power.
- *Access to Justice* is a condition in which people are able to seek and obtain a remedy for grievances through formal or informal institutions of justice that conform with international human rights standards, and a system exists to ensure equal and effective application of the law, procedural fairness, and transparency.
- *Culture of Lawfulness* is a condition in which the general population follows the law and seeks to access the justice system to address its grievances.

Most importantly, by providing this type of support, NATO can work to ensure host nation officials develop a respect for human rights and transparency in the enforcement of the law.

Stable Governance – Ability of the people to share, access or compete for power through nonviolent political processes and to enjoy the collective benefits and services of the state. Similar to the rule of law end state, NATO’s security focus will preclude its direct involvement in governance reform. Stable governance, however, requires the legitimate state monopoly over the means of violence, which can be achieved through security sector reform (SSR). SSR is not confined to training police units to conduct investigations and enforce laws, but includes efforts to strengthen government control, management, and oversight. In addition, NATO has the communications technologies needed to facilitate the host government’s ability to communicate with its population. Efforts to maintain transparency during the transition process will support the host government’s efforts to remain legitimate in the eyes of civilians.

Necessary Conditions:

- *Provision of Essential Services* is a condition in which the state provides basic security, the rule of law, economic governance and basic human needs services; essential services are provided without discrimination; and the state has the capacity for provision of essential services without significant assistance from the international community.
- *Stewardship of State Resources* is a condition in which national and sub-national institutions of governance are restored, funded, and staffed with accountable personnel; the security sector is reformed and brought under accountable civilian control; and state resources are protected through responsible economic management in a manner that benefits the population.
- *Political Moderation and Accountability* is a condition in which the government enables political settlement of disputes; addresses core grievances through debate, compromise, and inclusive national dialogue; and manages change arising from humanitarian, economic, security, and other challenges. A national constituting process results in separation of powers that facilitates checks and balances; the selection of leaders is determined through inclusive and participatory processes; a legislature reflects the interests of the population; and electoral processes are free and fair.
- *Civic Participation and Empowerment* is a condition in which civil society exists and is empowered, protected, and accountable; media are present, professional, and independent of government or political influence; equal access to information and freedom of expression are upheld; and political parties are able to form freely and are protected.

Sustainable Economy – Ability of the people to pursue opportunities for livelihoods within a system of economic governance bound by law. While NATO is not necessarily positioned to encourage macroeconomic stability in a legal or regulatory sense, it does have the ability to aid the host government in controlling its land and maritime borders to erode illicit economies and illegal migration networks. Moreover, NATO is poised to provide for the initial security of national resource infrastructure ahead of the development of domestic capabilities to do so. In the near term, the security of these two sectors will encourage the return of foreign and domestic private firms, promote the rehabilitation of a market economy, and provide the government with the revenue needed to expand its influence and ability to govern.

Necessary Conditions:

- *Macroeconomic Stabilization* is a condition in which monetary and fiscal policies are established to align the currency to market levels, manage inflation, and create transparent and accountable systems for public finance management. This condition requires a robust and enforceable legislative and regulatory framework to govern issues such as property rights, commerce, fiscal operations, and foreign direct investment.
- *Control over the Illicit Economy and Economic-Based Threats to Peace* is a condition in which illicit wealth no longer determines who governs, predatory actors are prevented from looting state resources, ex-combatants are reintegrated and provided jobs or benefits, and natural resource wealth is accountably managed.
- *Market Economy Sustainability* is a condition in which a market-based economy is enabled and encouraged to thrive. Infrastructure is built or rehabilitated, and the private sector and the human capital and financial sectors are nurtured and strengthened.
- *Employment Generation* is a condition in which job opportunities are created to yield quick impact to demonstrate progress and employ military-age youths, and a foundation is established for sustainable livelihoods.

Social Well-Being – Ability of the people to be free from want of basic needs and to coexist peacefully in communities with opportunities for advancement. The most significant way NATO can assist in this area is through its ability to move people and equipment over long distances in a short period of time. NATO can support at-risk populations directly by facilitating the provision of basic needs and services and the establishment of medical facilities and transitional housing for returnees.

Necessary Conditions:

- *Access to and Delivery of Basic Needs Services* is a condition in which the population has equal access to and can obtain adequate water, food, shelter, and health services to ensure survival and life with dignity. These services should be delivered in a manner that fosters reliability and sustainability.
- *Access to and Delivery of Education* is a condition in which the population has equal and continuous access to quality formal and non-formal education that provides the opportunity for advancement and promotes a peaceful society. This condition involves system-wide development and reform, and equal access to relevant, quality, and conflict-sensitive education.
- *Return and Resettlement of Refugees and Internally Displaced Persons* is a condition in which all individuals displaced from their homes by violent conflict have the option of a safe, voluntary, and dignified journey to their homes or to new resettlement communities; have recourse for property restitution or compensation; and receive reintegration and rehabilitation support to build their livelihoods and contribute to long-term development.
- *Social Reconstruction* is a condition in which the population is able to coexist peacefully through intra- and intergroup forms of reconciliation—including mechanisms that help to resolve disputes non-violently and address the legacy of past abuses—and through development of community institutions that bind society across divisions.

Annex C. Option Independent Recommendations

The United States as Flagship Nation

Information sharing often occurs when an asymmetry of power exists between the parties involved. Smaller parties in an information sharing agreement must allow those with more power a higher degree of influence and control over the process to secure their participation.⁵⁶ Any new information-sharing framework will require the United States' buy-in and resources. To ensure the success of any framework, the United States should assume the lead role.

NATO Special Operations Headquarters (NSHQ) provides a model for US leadership on joint projects. The United States played the crucial role in trans-

⁵⁶ Björn Fägersten, "For EU Eyes Only? Intelligence and European Security," European Union, Institute for Security Studies, March 4, 2016, <https://www.iss.europa.eu/content/eu-eyes-only-intelligence-and-european-security>.

forming the three-man office into a functional headquarters in 2006. US personnel staffed the most important positions in NSHQ, and the United States further provided most of the money for NSHQ's day-to-day operations. Because NSHQ's structure matched the United States' power and credibility in special operations with influence in NSHQ, the United States could shape doctrines and hold other members accountable for meeting NSHQ requirements and participating in necessary training.⁵⁷

The United States should use its experience with NSHQ as a template for establishing a successful information-sharing regime in NATO. The US intelligence community is the best resourced of any NATO member, and will bring the necessary doctrines and guidance to the table. Matching US-personnel to positions of authority within NATO's intelligence apparatus will create a greater unity of effort and a more expedient process for standing up the structure.

The drawbacks of this option manifest at the national level of member states. First, the United States government must be convinced of the necessity of the outlays for training and equipping. The other source of contention will come from other member states' governments concerns over increased sharing of intelligence among themselves. The United States can be convinced of the need for these measures by considering the investment as a force multiplier for future operations. The ability to share both operational and strategic level intelligence faster will improve alliance operations across the board. The US intelligence community will be sharing the same level of intelligence it already is releasing to NATO. The difference is that the channels will be more thoroughly understood by all participants and the likelihood of reciprocation will be greater due to other members being better trained in the disclosure processes. Pushback from member states unwillingness to increase sharing with each other can be overcome by leveraging the leading position the US has within NATO's current intelligence structure. The US produces the majority of all intelligence for the alliance and can use this as a resource to convince the other members to streamline the sharing processes already in use.

Civilian Director of Intelligence

The appointment of a NATO Assistant Secretary General for Intelligence would create a principal level position to improve intelligence operations and sharing by reducing structural inefficiencies within the alliance. Creating a principal position for intelligence, at the equivalent level of a three-star command, would provide senior level advocacy for intelligence sharing between the NATO civil and military intelligence organizations. This position would also provide a senior platform to reduce the resource waste inherent in the competition and

⁵⁷ Martin J. Ara, Thomas Brand, and Brage A. Larssen, *Help a Brother Out: A Case Study in Multinational Intelligence Sharing, NATO SOF*, Master's Thesis (Monterey, CA: Naval Postgraduate School, 2011), quote on pp. 40-41, https://calhoun.nps.edu/bitstream/handle/10945/10727/11Dec_Ara.pdf.

duplication of effort of the current split system. There are currently seven Assistant Secretaries with portfolios ranging from Public Diplomacy and Executive Management to Defense Investment and Emerging Security Challenges.⁵⁸ These issues have been deemed critical to the operation of the alliance, and the lack of effective intelligence oversight is a critical issue hindering unity of effort at both the operational and strategic levels.

A key spoiler to intelligence sharing between NATO member countries is that dissemination is performed on a national basis in accordance with national policies rather than in a unified effort under the alliance's structure.⁵⁹ Another obstruction to intelligence sharing is the split nature of intelligence providers to the alliance. The North Atlantic Council (NAC) and the Military Committee (MC) are supported by separate entities; the Intelligence Unit (IU) and the International Military Staff – Intelligence (IMS-INT), respectively. The IU collects its intelligence predominantly through member's national civilian services, on a bilateral basis, which is then presented to NATO's civilian authorities in the NAC.⁶⁰ IMS-INT is tasked with providing day-to-day strategic intelligence to all NATO Headquarter elements and Commands, and collects from both member countries' militaries and the NATO commands.⁶¹

Currently the only structural integration between these two bodies is the Intelligence Steering Board which falls under the purview of the Deputy Secretary General. Neither the Steering Board nor the Deputy Secretary General can provide the requisite leadership for alliance intelligence operations. The Deputy Secretary General is responsible for a multitude of duties, intelligence being only one, and is generally not an individual with a background in intelligence work. The Intelligence Steering Board typically only meets between six and eight times a year in response to specific issues, and as such is not designed for operational leadership.⁶² A dedicated Assistant Secretary General for Intelligence would provide a permanent senior position for an intelligence professional. This position would stand up a permanent office for integration of effort between NATO's intelligence offices, as well as endow that office with the authority to advocate for necessary structural reforms and provide a locus for strategic intelligence planning.

The creation of another large bureaucratic organization is the most significant drawback to this option. NATO is operating in an environment of fiscal austerity, and any significant expenditure will receive pushback from both within the alliance structure as well as member states. This is likely a reason for development of smaller more parochial focused intelligence billets in the form

⁵⁸ "Principal Officials," North Atlantic Treaty Organization, August 25, 2015, http://www.nato.int/cps/po/natohq/who_is_who_51639.htm.

⁵⁹ Interviews at NATO ARRC, March 14-15, 2016.

⁶⁰ Interview with Source K, US DoD official, March 16, 2016.

⁶¹ North Atlantic Treaty Organization, "International Military Staff," January 6, 2015, http://www.nato.int/cps/en/natohq/topics_64557.htm.

⁶² Interview with Source N, March 17, 2016.

of the IU and IMS-INT in the wake of the September 11th terrorist attacks. This fiscal expenditure can be mitigated by filling new positions with personnel currently serving in NATO intelligence shops, as their organizations are brought under the fold of the ASG-I's office. Another significant obstacle to NATO intelligence reform will be member states' national interests, and an extensive discourse must be enacted if the national intelligence bodies are to agree with the proposal.⁶³

Operationalizing Intelligence Staffs

During our research process, it was found that the joint intelligence staffs at headquarters of NATO maneuver elements (J2 and G2) are underprepared to operate in the complex environment in which the alliance finds itself. Operationalizing these intelligence staffs would require a number of reforms. These would include an increase in the personnel dedicated to intelligence collection and analysis, providing increased and more realistic training, integrating better real-world scenarios into the headquarters' training exercises, and allowing the integration of the staff into NATO or the framework nation's intelligence structure.

Our research found the under preparedness particularly true for the nine High Readiness Headquarters for NATO's Rapid Deployable Corps. These corps participate in the NATO Response Force (NRF) – a joint combined arms force that can be deployed at short notice to wherever needed. Each corps participates in the NRF's rotation system where it will be placed on a 12-month standby phase, and while on standby will be responsible for command of the NRF's land component.⁶⁴ These corps are central to NATO operations. The Allied Rapid Reaction Corps (ARRC), for example, has served as a headquarters for NATO led missions in Bosnia Herzegovina, Kosovo, twice in Afghanistan, and as a mentor to two Iraqi joint headquarters in 2008.⁶⁵ The mission sets NATO headquarters have been called on to perform have ranged from counter-piracy, border security and peacekeeping to multinational counterinsurgency campaigns. All of these missions require an in-depth understanding of the environment's atmospheric as well as timely intelligence concerning opposition forces. But these headquarters' intelligence staffs are not receiving the training and resources that they require when they are not on rotation as the sole NRF headquarters.

The first reason for this under resourcing is the structural and attitudinal predilection of NATO intelligence organizations to focus solely on strategic level

⁶³ Brian R. Foster, *Enhancing the Efficiency of NATO Intelligence Under an ASG-I*, Strategy Research Project (United States Army War College, March 2013), quote on pp. 27-28.

⁶⁴ North Atlantic Treaty Organization, "Rapid Deployable Corps," November 9, 2015, accessed March 28, 2016, http://www.nato.int/cps/sl/natohq/topics_50088.htm.

⁶⁵ Allied Joint Force Command, "Previous Operations," accessed March 28, 2016, <http://www.arcc.nato.int/operations/previous>.

planning.⁶⁶ This focus, while understandable at the alliance level, fails to properly prepare the analysts for the work that they will be expected to perform while in the field. Training exercises, such as Trident Jaguar, while having proven effective at developing and internalizing standard operating procedures for intelligence staffs, still do not provide the requisite skill-base for real world intelligence work that a deployed staff would be responsible for developing.⁶⁷ Another challenge facing intelligence staffs is that a number of member militaries do not field dedicated intelligence units, and as such personnel that is deployed to joint staffs often fails to possess even a rudimentary understanding of the intelligence process.⁶⁸

Cost is the primary drawback of this option. Money must be found to find, hire, equip, and ultimately train the analysts and staff for the expanded headquarters' sections. Time is also a factor that must be taken into account as this expansion process and its requisite training will not be completed overnight. Operationalization would require an increase in manpower to compensate for the greater workload that the staffs would be expected to complete. This increase in personnel would also ease the transition from dormant to operational standing by acclimating the staff to a larger and faster paced environment. The staff would gain vital experience by analyzing real world intelligence, and increase its efficiency by exercising its standard operating procedures on a consistent basis.⁶⁹ Training exercises for the entire headquarters unit would become more realistic as a result of the staff working with the current and real intelligence its intelligence section has been analyzing.⁷⁰ This operationalization would also provide an opportunity to increase the analytical bandwidth of either NATO or the participating national militaries as their personnel will be able to become subject matter experts through handling particular sets of intelligence on a daily basis.⁷¹ While expensive, this option would develop national intelligence professionals who would return to their countries after completing a deployment versed not only in their own nation's policies, but also equipped with an understanding of joint intelligence processes.

⁶⁶ Foster, *Enhancing the Efficiency of NATO Intelligence*, 3-7.

⁶⁷ Interview with Source J, March 14, 2016.

⁶⁸ Interviews with Sources E, F, G and M, March 14-15, 2016.

⁶⁹ Interview with Source B, March 15, 2016.

⁷⁰ Interview with Source J, March 14, 2016.

⁷¹ Interview with Brig. Gen. Joseph O'Sullivan, G-2 Chief at NATO ARRC, March 15, 2016.



Examining ISIS Online Recruitment through Relational Development Theory

Sarah Ponder^a and Jonathan Matusitz^b

^a *Nicholson School of Communication, University of Central Florida,*
<https://communication.ucf.edu/>

^b *Nicholson School of Communication, University of Central Florida, Partnership Center – Seminole State College of Florida,*
<https://www.seminolestate.edu/slm/university-partnership-center>

Abstract: This paper applies the theory of relational development to examine how the Islamic State of Iraq and al-Sham (ISIS) recruits new members. Relational development postulates that individuals follow relationship stages in order to reinforce their interpersonal communication or social bond. The relational development model includes five main stages, called the five stages of relationship escalation, or the “coming together” stages. These consist of initiating, experimenting, intensifying, integrating, and bonding. Overall, the authors of this analysis found that ISIS can successfully recruit many people—particularly male and female youth—thanks to stage-by-stage relational development through internet chat rooms and social network sites (SNSs) like Twitter. By the same token, the authors also believe that, should ISIS not use internet chat rooms and social network sites, and if ISIS were not following those stages of relationship escalation, their recruitment process would not be as efficient.

Keywords: caliphate, Internet, ISIS, radicalization, relational development, social media, terrorism. Twitter.

Introduction

This paper applies the theory of relational development to examine how the Islamic State of Iraq and al-Sham (ISIS) recruits new members. ISIS is a powerful Islamist terrorist organization responsible for perpetrating a high number of violent attacks on innocent civilians in regions like the Near East. ISIS believes in

establishing a caliphate (an Islamic system of world government). Relational development postulates that individuals follow relationship stages in order to reinforce their interpersonal communication or social bond.¹ The relational development model includes five main stages, called the five stages of relationship escalation, or the “coming together” stages. These consist of initiating, experimenting, intensifying, integrating, and bonding.² Initiating is the stage in which an individual makes contact with another individual. Experimenting occurs when one seeks to know more about someone and determines whether or not to continue a relationship. Intensifying occurs when individuals are more comfortable in an interpersonal dialogue and share much more personal details. Integrating occurs when people begin to identify themselves together or as a part of the same group. And bonding is a public allegiance and full-fledged commitment to a group.

Overall, the authors of this analysis found that ISIS can successfully recruit many people—particularly male and female youth—thanks to stage-by-stage relational development through internet chat rooms and social network sites (SNSs) like Twitter. By the same token, the authors also believe that, should ISIS not use internet chat rooms and social network sites (SNSs), and if ISIS were not following those stages of relationship escalation, their recruitment process would not be as efficient. This analysis begins with a detailed description of the theory of relational development (based on all five stages). Then, the authors proceed to describe ISIS and its overall recruitment methods. What comes subsequently is the heart of this analysis: the examination of ISIS recruitment through relational development. This analysis ends with a discussion that also includes suggestions for future research.

Relational Development Theory

Developed by Knapp,³ the theory of relational development explains how interactants—e.g., couples, negotiators, and so forth—follow relationship stages so as to reinforce their interpersonal communication or social bond. The theory postulates that relationships evolve into stages as a result of interpersonal dialogue. Such dialogue sheds light on the interactants’ positive or negative experiences and modifications of their intimacy or communication styles.⁴ Relational

¹ Mark L. Knapp, *Social Intercourse: From Greeting to Goodbye* (Boston, MA: Allyn and Bacon, 1978); Mark L. Knapp, *Interpersonal Communication and Human Relationships* (Boston, MA: Allyn and Bacon, 1984).

² Mark L. Knapp and John A. Daly, eds., *Handbook of Interpersonal Communication*, 3rd ed. (Thousand Oaks, CA: Sage, 2002).

³ Knapp, *Social Intercourse*; Knapp, *Interpersonal Communication and Human Relationships*.

⁴ Theodore A. Avtgis, Daniel V. West, and Traci L. Anderson, “Relationship Stages: An Inductive Analysis Identifying Cognitive, Affective, and Behavioral Dimensions of Knapp’s Relational Stages Model,” *Communication Research Reports* 15, no. 3 (1998): 280-287.

development also rests on the premise that “relationships evolve into stages as a result of interpersonal dialogue.”⁵ The relational development model includes five main stages, called the five stages of relationship escalation, or the “coming together” stages. These consist of initiating, experimenting, intensifying, integrating, and bonding.⁶ Although relationship escalation entails cycles of growing together, this would not work for relationships that are disintegrating.⁷

Initiating

When developing relationships, unacquainted people start to have intentions, hopes, needs, desires, wishes, and beliefs in mind in order to guide their actions.⁸ The first stage of relationship escalation or “coming together” is initiating: the stage in which an individual makes contact with another individual. At this stage, people acknowledge each other and start to share discourses. This stage is important because the first elements of knowledge about an individual, called “first impression,” are formed in it.⁹ The concept of first impression has an intense impact on relational development: it influences the opinion about the quality of a person, often determines the destiny of a relationship (whether or not it will last), and persists for a long time in the mind of the other interactant – hence, the better the first impression, the more positive it will be perceived. Even though the impact of the first impression can be profound, it can be created within a fraction of a second, based mostly on how a person communicates or the external and physical traits of that person, such as his or her physical appearance, body language, and attire.¹⁰

Experimenting

According to Fox, Warber, and Makstaller, *experimenting* occurs when one seeks to know more about someone and determines whether or not to continue a

⁵ Jonathan Matusitz, *Terrorism and Communication: A Critical Introduction* (Thousand Oaks, CA: Sage, 2012), quote on p. 365.

⁶ Knapp and John A. Daly, eds., *Handbook of Interpersonal Communication*.

⁷ Daniel J. Canary, Michael J. Cody, and Valerie L. Manusov, *Interpersonal Communication: A Goals Based Approach*, 4th ed. (New York: Bedford/St. Martin's, 2008).

⁸ Dorothy Miell and Steve Duck, “Strategies in Developing Friendships,” in *Friendship and Social Interaction*, ed. Valerian J. Derlega and Barbara A. Winstead (New York: Springer, 1986), 129-143.

⁹ Michael Sunnafrank and Artemio Ramirez, Jr., “At First Sight: Persistent Relational Effects of Get-Acquainted Conversations,” *Journal of Social and Personal Relationships* 21, no. 3 (2004): 361-379.

¹⁰ Christopher Y. Olivola and Alexander Todorov, “Elected in 100 milliseconds: Appearance-Based Trait Inferences and Voting,” *Journal of Nonverbal Behavior* 34, no. 2 (2010): 83-110.

relationship.¹¹ This stage commonly occurs shortly after the *initiating* phase. In the *experimenting* phase, people aim to gather information on one another by asking questions. They look for common interests through limited self-disclosure, while correcting possible mistakes made during the first impression (formed in the previous *initiating* stage). The knowledge exchanged in this stage includes personal interests.¹²

Experimenting is a probing stage in which people make a further evaluation of each other, which is what Knapp terms “trying to discover the unknown.”¹³ Welch and Rubin state that “communicators explore commonalities and generally increase breadth of topics, rarely delving into specific ones.”¹⁴ Small talk is highly representative of this stage as it gives interactants the possibility to reveal more details about each other and expand the current scope of the relationship. Knapp indicates that, at this stage, the relationship places limited demands on the interactants.¹⁵

Intensifying

Intensifying occurs when individuals are more comfortable in an interpersonal dialogue. Fox et al. found that people often disclose more information during the *intensifying* phase; relationships, then, beginning to appear.¹⁶ At this stage, the relationship status between individuals is labeled “close friends.” Interaction has more self-disclosure (e.g., revealing more personal information) and intimate verbal and nonverbal actions (use of nicknames and compliments), informal speech, asking for favors, and so forth.¹⁷ More direct expressions of commitment emerge. In a nutshell, interpersonal intimacy is finally formed: increased depth of disclosure is now happening and communication acknowledges the friendship that has developed.¹⁸

¹¹ Jesse Fox, Katie M. Warber, and Dana C. Makstaller, “The Role of Facebook in Romantic Relationship Development: An Exploration of Knapp’s Relational Stage Model,” *Journal of Social and Personal Relationships* 30, no. 6 (2013): 771-794.

¹² Paul A. Mongeau and Mary Lynn Miller Henningsen, “Stage Theories of Relationship Development: Charting the Course of Interpersonal Communication,” in *Engaging Theories in Interpersonal Communication: Multiple Perspectives*, ed. Leslie A. Baxter and Dawn O. Braithwaite (Thousand Oaks, CA: Sage, 2008), 363-375.

¹³ Knapp, *Social Intercourse*, p. 21.

¹⁴ S-A Welch and Rebecca B. Rubin, “Development of Relationship Stage Measures,” *Communication Quarterly* 50, no. 1 (2002): 24-40, quote on p. 25.

¹⁵ Knapp, *Interpersonal Communication and Human Relationships*.

¹⁶ Fox, Warber, and Makstaller, “The Role of Facebook in Romantic Relationship Development.”

¹⁷ Denise Haunani Solomon and Anita L. Vangelisti, “Relationship Development,” in *Interpersonal Communication*, ed. Charles R. Berger (Berlin: De Gruyter Mouton, 2014), 347-369.

¹⁸ Knapp, *Social Intercourse: From Greeting to Goodbye*.

Integrating

Integrating occurs when people begin to identify themselves together or as a part of the same group. At this stage, tightly-knit groups emerge. The term “coupling” can be applied here: people start appearing similar (nonverbally) and think of themselves as friends.¹⁹ They are akin in terms of attitudes, interests, and opinions. The relationship is now private and persistent: intimate information and secrets are frequently shared, and individuals exchange aspects of their social identity (e.g., in regards to friends, family, and living spaces).²⁰ People also “wear” each other’s identity through intimate tokens. For example, through pictures and pins, they have reached a higher synchronicity in behavior.²¹

Bonding

The *bonding* stage occurs when people start to identify with an individual or a group publicly. At this stage, the close relationship is represented by a formal, public commitment to the relationship or group affiliation—e.g., through a formal pledge, ceremony, or ritual—and the utmost level of empathy, trust, and intimacy.²²

Islamic State of Iraq and al-Sham (ISIS)

Occasionally called the Islamic State of Iraq and the Levant (ISIL) in the media, or simply the Islamic State, the Islamic State of Iraq and al-Sham (ISIS) is an extremist Muslim-based terrorist organization that has control of large expanses of territory in Iraq and Syria, as well as smaller areas in African countries such as Libya and Nigeria. ISIS is also active in parts of the world including Southeast Asia.²³ The roots of ISIS are based in Al Qaeda in Iraq (AQI), a terrorist group founded by Abu Musab al-Zarqawi, a Jordanian militant Islamist. In 2006, when Zarqawi was killed by U.S. and Iraqi forces, Abu Ayyoub al-Masri, an Egyptian, became the new leader, embracing the cause of what was then called the Islamic State of Iraq (ISI). In 2010, Abu-Bakr al-Baghdadi was announced as the newly proclaimed caliph – after the killing of Masri (the former leader), also by U.S. and

¹⁹ Welch and Rubin, “Development of Relationship Stage Measures.”

²⁰ Darius K.-S. Chan and Grand H.-L. Cheng, “A Comparison of Offline and Online Friendship Qualities at Different Stages of Relationship Development,” *Journal of Social and Personal Relationships* 21, no. 3 (2004): 305-320.

²¹ Richard Moniz, Jo Henry, and Joe Eshleman, *Fundamentals for the Academic Liaison* (Chicago: American Library Association, 2014).

²² Mark L. Knapp and Anita L. Vangelisti, *Interpersonal Communication and Human Relationships*, 6th ed. (Boston, MA: Pearson Education, 2008).

²³ Jay Sekulow, Jordan Sekulow, Robert W. Ash, and David French, *Rise of ISIS: A Threat We Can't Ignore* (Brentwood, TN: Howard Books, 2015); Ishaan Tharoor, “ISIS or ISIL? The Debate over What to Call Iraq’s Terror Group,” *The Washington Post*, June 18, 2014, p. A1.

Iraqi forces. In April 2013, Al-Baghdadi renamed the organization the Islamic State of Iraq and al-Sham.²⁴

ISIS vehemently believes in establishing a caliphate. A caliphate is a world-wide Islamic State, like an Islamic system of world government.²⁵ This caliphate movement seeks to (1) revive the rule of the caliph (a supreme religious and political leader in Islam); (2) restore sharia (a body of Islamic law derived from the Qur'an and the hadiths) over both the ummah (the community of faithful Muslims) and non-Muslims all over the world; and (3) ultimately spread Islamic doctrine all over.²⁶ In order to achieve the caliphate, ISIS says it has been called by Allah to carry out large-scale, coordinated attacks against both Muslims and non-Muslims. Terrorist attacks tend to involve suicide bombings, car bombs, mass executions, torture, and beheadings. ISIS terrorism is often displayed publically. This is the ultimate objective of terrorism: to intimidate audiences into supporting, or not resisting, ISIS's rapid conquest and control of the world. ISIS's capture of the city of Mosul (in northern Iraq) on June 10th, 2014 testifies to the organization's daunting military strength.²⁷ The city of Mosul came to be considered ISIS's caliphate, or the Islamic State.

ISIS Recruitment

Today, ISIS is one of the fastest-growing, most violent, and wealthiest terrorist organizations in the world.²⁸ ISIS firmly believes in the establishment of the caliphate and perpetrating jihad in the name of Allah. As Weiss and Hasan explain, "ISIS has destroyed the boundaries of contemporary nation-states and proclaimed itself the restorer of a lost Islamic empire."²⁹ ISIS relies heavily on its strategic communication campaign. ISIS leaders have proven to excel in the use of online social media for recruitment and propaganda, both of which are critical to the success and growth of the organization. They are highly skilled in grabbing the attention of the Western world: through online videos they promote horrid imagery and brutality to be seen by both the *ummah* (the community of faithful

²⁴ Zana Khasraw Gulmohamad, "The Rise and Fall of the Islamic State of Iraq and Al-Sham (Levant) ISIS," *Global Security Studies* 5, no. 2 (2014): 10-21.

²⁵ Futoshi Matsumoto, "The World Order and a New "Behemoth"," *Asia-Pacific Review* 22, no. 1 (2015): 177-190.

²⁶ Guy Rodgers, *Understanding the Threat of Radical Islam* (Broomall, PA: National Highlights, 2012).

²⁷ Stansfield, "The Islamic State, the Kurdistan Region and the Future of Iraq: Assessing UK Policy Options," *International Affairs* 90, no. 6 (2014): 1329-1350.

²⁸ Seongju Oh, Chaeyun Jung, and Taeseon Yoon, "Analysis of the Development of IS (Islamic State) in Its Relation to Conflicts within OIC (Organization of Islam Countries) by Using SPSS Statistical Program," *International Journal of Social Science and Humanity* 6, no. 10 (2016): 799-804.

²⁹ Michael Weiss and Hassan Hassan, *ISIS: Inside the Army of Terror* (New York: Regan Arts, 2015), quote on p. 8.

Muslims) and the non-Muslim world.³⁰ While many view this brutality as grotesque, it unfortunately also projects the unprecedented power that ISIS possesses.³¹

ISIS and Social Network Sites (SNSs)

There are three main narratives used by ISIS to appeal to its possible recruits. According to Gartenstein-Ross, the terrorist organization focuses mainly on the three following ideas: religious obligation, political grievances, and the success of the Islamic State.³² Regardless of gender and age, the most cited reason for joining ISIS is religious obligation or conviction. Many individuals are recruited online. Terrorist organizations also use prisons, religious institutions, and universities as recruitment grounds. Prisons in the Middle East have become much like academies for ISIS to recruit and train fighters.³³ Foreign fighters, particularly those living outside the Islamic State, are most often recruited via propaganda through online strategic messaging, social media, and chat rooms. These techniques are often used for recruiting those who will not likely come in physical contact with ISIS fighters.³⁴ According to Nissen, the main ISIS social media objectives are as follows:

- to bring attention to the caliphate message through social network sites (SNSs). SNSs give ISIS international attention
- raising financial support
- bringing together like-minded supporters
- recruiting and converting new members.³⁵

Twitter is a major communication campaign source for ISIS. Even though Twitter suspended 125,000 ISIS-related accounts in February 2016,³⁶ ISIS is always able to circumvent “filters” and create other Twitter profiles. One of ISIS’s successful SNS undertakings is a Twitter app called *The Dawn of Glad Tidings*, or just *Dawn*. The app is a real ISIS product promoted by talented SNS users. It serves to keep the world abreast on the terrorist organization’s latest exploits or

³⁰ C. Akça Ataç, “A Comparative Civilizational Reading for the Middle East and Turkey’s New Role in It,” *Global Change, Peace & Security* 28, no. 1 (2016): 99-115.

³¹ Daveed Gartenstein-Ross, “Testimony to the Committee on Homeland Security and Governmental Affairs, United States Senate,” in *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment*, S. Hrg. 114-438 (Washington, D.C.: U.S. Government Publishing Office, 2016), 12-21, <https://www.hsdl.org/?abstract&did=798565>.

³² Gartenstein-Ross, “Testimony.”

³³ Weiss and Hassan, *ISIS: Inside the Army of Terror*.

³⁴ Gartenstein-Ross, “Testimony.”

³⁵ Thomas Elkjer Nissen, “Terror.com – IS’s Social Media Warfare in Syria and Iraq,” *Contemporary Conflicts* 2, no. 2 (2014): 1-8.

³⁶ Jessica Guynn and Elizabeth Weise, “Twitter Suspends 125,000 ISIL-related Accounts,” *USA Today*, February 5, 2016, p. A1.

imminent actions.³⁷ Another well-known ISIS twitter account is called *Islamic State Media*, in which the organization brags about exterminating atheists, female drivers, Shia Muslims, the Kurds, and the Jews.

The organization sends out series of tweets to spread their messages and warnings, along with pictures. Like many individuals or groups whose goal is to increase followers, they have set up “fake” followers’ accounts. This serves to motivate real followers to join their accounts.³⁸ ISIS also employs the use of Facebook, Instagram, Skype, and YouTube. Such SNSs are typically used to engage in conversation with possible recruits. They develop an interpersonal dialogue with potential Muslim brothers and sisters. There are numerous videos online that spread ISIS’s messages, goals, and rituals such as beheadings. This terrorist organization also publishes its own publication, *Dabiq*. To be more precise, *Dabiq* is a monthly online magazine (50-60 pages) that extolls the virtues of sharia and jihad and pays tributes to the martyrs who died in holy war.³⁹ As Nissen explains, ISIS “utilizes techniques normally associated with political campaigning, e.g. by sounding out possible support through feedback on potential ideas, terms and graphics.”⁴⁰ The group “campaigns” online by spreading awareness of its cause and organization via social media, articles, videos, and websites – all useful tools put to use so as to recruit individuals to join the fight.

ISIS Recruitment of Females

The youth is particularly targeted for recruitment by ISIS for several key reasons. After all, young recruits provide clean records and cultural acclimation that benefit leaders because they draw less suspicion.⁴¹ Another benefit of using youth is that, if caught by the authorities, they may receive lighter punishment because of their young age. While male youth have served as the primary target for recruitment, there has recently been a rise in female recruitment.⁴² Females are most commonly recruited in active online chat rooms and various SNSs. This is a much more convenient platform for recruitment in comparison with recruitment methods in the 1990s, when terrorist recruiters had to rely more on face-to-face interactions.⁴³

³⁷ J.M. Berger, “How ISIS Games Twitter,” *The Atlantic*, June 16, 2014, p. A1.

³⁸ Nissen, “Terror.com – IS’s Social Media Warfare in Syria and Iraq.”

³⁹ Till F. Paasche and Michael M. Gunter, “Revisiting Western Strategies against the Islamic State in Iraq and Syria,” *The Middle East Journal* 70, no. 1 (2016): 9-29.

⁴⁰ Nissen, “Terror.com – IS’s Social Media Warfare in Syria and Iraq,” p. 3.

⁴¹ Seong Hun Yu and Omar Sultan Haque, “Vulnerabilities among Young Westerners Joining ISIS,” *The Brown University Child and Adolescent Behavior Letter* 32, no. 2 (2016): 1-6.

⁴² Thomas R. McCabe, “A Strategy for the ISIS Foreign Fighter Threat,” *Orbis* 60, no. 1 (2016): 140-153.

⁴³ Mia M. Bloom, “In Defense of Honor: Women and Terrorist Recruitment on the Internet,” *Journal of Postcolonial Cultures and Societies* 4, no. 1 (2013): 150-195.

While many females feel compelled to join ISIS for religious reasons, there are scores of women influenced by personal wants and needs. As Sherwood contends, “some young women were offered financial incentives, such as travel expenses or compensation for bearing children by ISIS.”⁴⁴ These females are also typically promised acceptance, sisterhood, and love. Men often chat with these female recruits, developing a relationship with them. Once recruited, they are expected to marry and bear children to secure the future of the organization.⁴⁵ There has been a dramatic rise in the travel of Western women, mostly European, to the Middle East. Unfortunately, many girls who are targeted and recruited are between the ages of 16 and 24, but girls as young as 13 have also been identified.⁴⁶ As Thomas Samuel puts it,

these groups attract youths by exploiting their vulnerabilities and providing them with a sense of identity, belonging and cohesiveness. Over a period of time, in a troubled environment, these youth begins to define their identity with that of the group and its struggle.⁴⁷

A Solution to Youth’s Identity Crisis

A certain number of youths today—even those living in Europe and North America—have an identity crisis: they struggle with unemployment, despair, and what they perceive as social rejection.⁴⁸ This makes them particularly ripe for ISIS recruitment. Young folks living in poverty are also a chief focus for ISIS. To these youths, ISIS seems to offer perspective, a sense of belonging and fraternity, and, of course, adventure, bravery, and martyrdom. ISIS-inspired jihad provides an unparalleled substitute for drugs and everyday crime, and an unconventional global movement with clear and straightforward rules.⁴⁹ According to Stern, since the 9/11 terrorist attacks, a significant minority of Western youth have joined the jihadist movement as a result of feelings of humiliation.⁵⁰ They feel

⁴⁴ Harriet Sherwood, Sandra Laville, Kim Willsher, Ben Knight, Maddy French, and Lauren Gambino, “Schoolgirl Jihadist: The Female Islamists Leaving Home to Join Isis Fighters,” *The Guardian*, September 29, 2014, p. A1.

⁴⁵ Bloom, “In Defense of Honor: Women and Terrorist Recruitment on the Internet.”

⁴⁶ Sherwood et al., “Schoolgirl Jihadist.”

⁴⁷ Thomas Koruth Samuel, “The Lure of Youth into Terrorism,” *SEARCCT’s Selection of Articles 2* (2011): 107-119, quote on p. 109, <http://www.searcct.gov.my/publications/our-publications?id=55>.

⁴⁸ Alex S. Wilner and Claire-Jehanne Dubouloz, “Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization,” *Global Change, Peace & Security* 22, no. 1 (2010): 33-51.

⁴⁹ Rik Coolsaet, *What Drives Europeans to Syria, and to IS? Insights from the Belgian Case* (Brussels: Royal Institute for International Relations, 2015), <http://www.egmontinstitute.be/what-drives-europeans-to-syria-and-to-is-insights-from-the-belgian-case/>.

⁵⁰ Jessica Stern, “Militant Groups: Beneath Bombast and Bombs, a Cauldron of Humiliation,” *Los Angeles Times*, June 6, 2004, p. A1.

that the West has overpowered them and purposefully humiliated them; leading them to take up arms and fight. Stern also points out that, for a holy war, jihadist groups need young people who feel humiliated and at a loss.⁵¹ Once these impressionable recruits appear, they become leaders who emerge and, in turn, take advantage of other fragile people. This is how ISIS befriends and recruits individuals so as to establish their loyalty to the group.

Examining ISIS Recruitment through Relational Development Theory

The theory of relational development is applied to the process by which ISIS recruits people around the world. More precisely, this analysis correlates five stages of relationship escalation to the efforts ISIS has made to gain support and followers. We dissect each stage of the theory and apply it to the way ISIS communicates with people around the world in an attempt to spread its propaganda and gain support. It is important to note that such ISIS recruitment model takes places not only in the Middle East but also in the Western world.⁵²

Initiating

The *initiating* phase is arguably the most important phase: the communicative aspect of recruitment has just begun. The recruiter or sympathizer makes contact with an individual or possible recruit. At this phase, people acknowledge each other and start to share discourses. Today, it has become more common to initiate discourses online through SNSs – rather than in person in a face-to-face setting. Through online chat rooms, Facebook, and Twitter, ISIS runs websites and magazines that all play a role in making a positive “first impression.”

Dabiq, the ISIS-run magazine, has been able to cast out the positive “first impression” that ISIS desired. The monthly magazine is well put together and tries to appeal to the Western youth. Indeed, *Dabiq* articles are written in perfect English, contain many beautiful, colored images, and display glorious-looking fighters on top of Toyota trucks.⁵³ Through *Dabiq* and various SNSs, ISIS uses the World Wide Web and the deep web—when the content on the World Wide Web cannot be easily found by standard search engines⁵⁴—to promote jihad, glorify the caliphate, and promise the rewards from Allah (e.g., the afterlife, with its virgins and servants, as well as the peaceful setting with waterfalls and lounging

⁵¹ Stern, “Militant Groups: Beneath Bombast and Bombs.”

⁵² Xu Zhang and Lea Hellmueller, “Transnational Media Coverage of the ISIS Threat: A Global Perspective?” *International Journal of Communication* 10 (2016): 766-785.

⁵³ Matthew Mosk, Brian Ross, and Alex Hosenball, “US Officials Ask How ISIS Got So Many Toyota Trucks,” *ABC News*, October 6, 2015, <https://abcnews.go.com/International/us-officials-isis-toyota-trucks/story?id=34266539> (April 6, 2017).

⁵⁴ Mhamed Zineddine, “Search Engines Crawling Process Optimization: A Webserver Approach,” *Internet Research* 26, no. 1 (2016): 311-331.

lions in their visuals).⁵⁵ In the *initiating* phase, this first contact can also be initiated by the inquisitive online user; here, an individual contacts a person whom he or she thinks is affiliated with ISIS. For those users who have signed up to ISIS-related SNSs, ISIS tweets include links, hashtags, and images. The same content is often tweeted by other users' twitter accounts.⁵⁶

Writing for *The Times of India*, Hafeez explains how Arif Majeed, then 23-year-old in 2014, initiated contact with an ISIS recruiter on an internet chat room.⁵⁷ As Hafeez continues, Arif Majeed "told interrogators that his indoctrination began after he visited an internet chat room. He was inspired to join the terrorist group and given the phone number of a person, whose men picked him up from Mosul in Iraq."⁵⁸ Such impressionable youth often use SNSs or chat rooms to open communication. Hence, the better the recruiter's first impression, the higher the number of possible future ISIS brothers and sisters. In order to be successful, the recruiter must exhibit charisma.

Experimenting

Experimenting is the second stage. This stage emerges after the recruiter's first impression is made and the interactants decide to pursue communication further. Once contact with a recruiter has begun, the potential recruit wants to know more about the cause. Often, many questions will be asked (from both sides) during online chats or through SNS posts. As was the case with Arif Majeed, a potential recruit may ask questions in regards to ISIS lifestyle or what it is like to train and die for Allah.⁵⁹ This stage consists mostly of small talk. In regards to the aforementioned Twitter app that ISIS created—*The Dawn of Glad Tidings* or simply *Dawn*—countless users can sign up for the app (on the internet or on their smartphones). When a user downloads the app, ISIS immediately asks some personal questions.⁶⁰ This is a reflection of the *experimenting* phase right there.

During this information-gathering phase, ISIS recruiters tend to paint a picturesque lifestyle of the jihadist cause and all that it has to offer. They tell the possible recruits anything and everything they want to hear in order to gain their attention and support. For example, a recruiter increases positivity during interpersonal dialogue by exaggerating the praise and acceptance that one will find after joining ISIS ranks (because of the commitment to Allah). They may also increase positivity by promising love, sister or brotherhood, and compensation.

⁵⁵ Harry E. Wedeck and Wade Baskin, *Dictionary of Pagan Religions* (New York: Philosophical Library, 2015).

⁵⁶ Berger, "How ISIS Games Twitter."

⁵⁷ Mateen Hafeez, "Radicalized on Net Chat Room, Given Mosul Contact: ISIS Man," *The Times of India*, November 30, 2014, p. A1.

⁵⁸ Hafeez, "Radicalized on Net Chat Room," p. A1.

⁵⁹ Hafeez, "Radicalized on Net Chat Room."

⁶⁰ Berger, "How ISIS Games Twitter."

Dabiq clearly describes how ISIS has an astronomical amount of material wealth: in addition to building five-star hotels in Mosul, the organization gives a salary and a villa with a pool to committed mujahedin. Lastly, *Dabiq* explains how ISIS offers new recruits the possibility of exerting power over others and even sadism in the name of Allah.⁶¹

During the *experimenting* phase, people evaluate whether or not they should progress with the relationship. According to Driscoll, a woman who went undercover online was contacted by an ISIS fighter whose goal was to recruit her. He repeatedly showered her with compliments and claimed that “when you get here, you’ll be treated like a princess.”⁶² By inculcating such ideas into the minds of potentially new recruits, the ISIS radicalizer can portray a paradisiacal lifestyle for successful martyrs and, as a result, can easily influence them to move into the next phase. Not only do they advertise the ideal life; they also depict the afterlife as a bliss in *Janna* (heavenly garden).⁶³

Intensifying

During the *intensifying* phase, ISIS recruiters have already solidified contact with people through SNSs or internet chat rooms. Put another way, ISIS has now developed a comfortable dialogue in which they are beginning to form what seems to be a long-lasting relationship. Skype is another common tool that is of utmost importance in this phase because the people involved are now willing to expose themselves visually; this proves that they have progressed to a phase in which they are now feeling more relaxed and are sharing more personal information such as hurtful experiences.⁶⁴ An example is Abdelaziz Kuwan, a teenager from Bahrain, who made the decision to join ISIS in 2014 after spending months interacting via Skype with “some of the brothers” in Syria.⁶⁵ What this anecdote also demonstrates is that, at this stage, interactants are no longer engaging in small talk, but are becoming more serious. ISIS feeds people with false promises during this information exchange in order to promote a positive experience. These recruiters prey on the individual’s insecurities and needs, using the disclosure of information in order to manipulate the person.

At this point, ISIS recruiters are strongly reassuring the individual to join their organization and their relationships are becoming more intimate in nature. Abdelaziz was encouraged to travel to Syria to join the fight. He managed to con-

⁶¹ Heather Saul, “ISIS Opens 262-room Luxury Hotel in Mosul,” *Independent*, May 6, 2015, p. A1.

⁶² Margarette Driscoll, “My ISIS Boyfriend: A Reporter’s Undercover Life with a Terrorist,” *New York Post*, March 7, 2015, p. A1.

⁶³ Jonathan Matusitz, *Symbolism in Terrorism: Motivation, Communication, and Behavior* (Lanham, MD: Rowman & Littlefield, 2014).

⁶⁴ Joshua R. Pederson and Rachel M. McLaren, “Managing Information Following Hurtful Experiences: How Personal Network Members Negotiate Private Information,” *Journal of Social and Personal Relationships* 33, no. 7 (2015): 961-983.

⁶⁵ Weiss and Hassan, *ISIS: Inside the Army of Terror*.

vince his mother to give his passport back.⁶⁶ In this stage, females are also prone to engaging in a “romantic type” relationship online with an ISIS member—a phenomenon called “love jihad”⁶⁷—which facilitates the advancement to the last two stages: the *integrating* and *bonding* stages. At the same time, recruiters avoid discussing the horrors and potential risks that many face after choosing to join ISIS. Most women are reeled in by the communication about acceptance, love, and praise. However, like most recruits, they are left in the dark regarding their actual rights, living arrangements, and lack of freedom they will face after traveling to Syria or Iraq.⁶⁸ The *intensifying* stage is important to the recruitment process because it enables ISIS recruiters to manipulate individuals into believing that their troubles will be gone once they have joined the organization.

After researching many articles about these ISIS recruiters, it was obvious that many ISIS recruitment methods have similar patterns of answers and shooting down of any negativity (while replacing the negative concerns with positive encouragement). ISIS recruiters use encouragement to persuade the recruit – e.g. by uttering short and simple, but convincing statements such as “Many people make this journey every day,” “It’s not the first time nations have plotted against the believers,” “Go to Sham (Syria) for it is the best of Allah’s lands on earth,” and “It is necessary to live under the caliphate.”⁶⁹ Recruiters have even encouraged curious online users to have a conversation with their loved ones to see where they stand and make a possible attempt to recruit them to come along with them. In other instances, recruiters have also managed to convince youth to disappear so as to avoid detection or arrest. Young Western women, in particular, have been at risk. This was the case with three girls who disappeared from the United Kingdom and were found to have traveled to Turkey in order to cross the Syrian border. They had been persuaded to join the cause as a result of months of online interaction with ISIS.⁷⁰

Integrating

In this context, *integrating* is the successful recruitment itself, whereby new recruits emigrate to Syria or Iraq to join ISIS. Once recruited, individuals begin to identify themselves as part of the jihadist cause. Through numerous interactions with ISIS on the ground, they begin to identify as “we” or “us” and associate with the terrorist group. In the ISIS environment, integrating implies an “us vs. them” orientation. Both verbal and physical interactions have now become much more

⁶⁶ Pederson and McLaren, “Managing Information Following Hurtful Experiences.”

⁶⁷ Kishalaya Mukhopadhyay, “Queering the Narrative: Can the Subaltern Sex Speak?” *Economic & Political Weekly* 51, no. 2 (2016): 20-23.

⁶⁸ Zainab Salbi, “Rape Survivor Who Escaped ISIS Discusses Torture She Was Subjected to,” *The New York Times*, June 23, 2015, p. A1.

⁶⁹ Tom Whitehead, “Secret Cell of British Muslim Women Encouraging Others to Join Islamic State Exposed,” *The Telegraph*, November 23, 2015, p. A1.

⁷⁰ Josh Halliday, Aisha Gani, and Vikram Dodd, “UK Police Launch Hunt for London Schoolgirls Feared to Have Fled to Syria,” *The Guardian*, February 20, 2015, p. A1.

intimate. New recruits have moved from being their own individuals to being ISIS members – a process called depluralization.⁷¹ Depluralization is a process whereby a person relinquishes his or her formal “self” so as to assume a new “self.” In essence, joining ISIS requires *integrating* a new group-affiliated “self” by adopting the entire group’s philosophy and blending in with the other members.⁷² When *integrating*, the recruiter is actively planning out the new recruits’ mission and place within an elitist Muslim brotherhood.

Bonding

The last stage of relationship escalation is *bonding*, whereby a close relationship has been formed and individuals are fully committed to fighting with ISIS and honoring the allegiance they have sworn to Abu-Bakr al-Baghdadi, the current ISIS leader.⁷³ Now, ISIS recruits are full-fledged members of the terrorist organization. An important aspect of this phase is that individuals have now identified with ISIS publicly. They upload videos of their new ISIS selves online or post tweets about their jihadist lives on SNSs.⁷⁴ Members also have symbolic cues they use to show their support such as standing with their index finger pointed upwards to show their solidarity with caliphate fighters. Essentially, this nonverbal gesture symbolizes the *bonding* between ISIS and Allah – reflecting the following message: we have been called by Allah to kill anyone until the worldwide caliphate is established.⁷⁵

In order to prove their total loyalty to ISIS, members must also be “hazed” into the terrorist group through a type of public initiation. To be more precise, they have to engage in a public action of killing the enemy – even if it means killing one’s own mother. In January 2016, a young ISIS recruit killed his own mother who was not supportive of his cause. She was accused of apostasy after her son reported her to senior ISIS members. The woman’s son, 20-year-old Ali Saqr al-Qasem, was persuaded to execute her with his own hands. After demonstrating his lethal commitment, his loyalty to ISIS was unquestionable, allowing the *bonding* stage to seal.⁷⁶ At the *bonding* stage, these full-fledged ISIS members will attempt to influence others to join them and may even become recruiters themselves. On the other hand, it is unlikely that the average ISIS member

⁷¹ Margaret Singer with Janja Lalich, *Cults in Our Midst: The Hidden Menace in Our Everyday Lives* (San Francisco: Jossey-Bass, 1995).

⁷² Barbara Franz, “Popjihadism: Why Young European Muslims Are Joining the Islamic State,” *Mediterranean Quarterly* 26, no. 2 (2015): 5-20.

⁷³ McCabe, “A Strategy for the ISIS Foreign Fighter Threat.”

⁷⁴ Diana Secara, “The Role of Social Networks in the Work of Terrorist Groups. The Case of ISIS and Al-Qaeda,” *Research and Science Today*, Supplement 3 (2015): 77-83.

⁷⁵ Orlando Crowcroft, “ISIS: What is the Story Behind the Islamic State One-fingered Salute?” *International Business Times*, June 15, 2015, p. A1.

⁷⁶ John Hall, “ISIS Militant Ali Saqr al-Qasem Publicly Executes Own Mother in Raqqa after Accusing Her of ‘Apostasy,’” *Independent*, January 8, 2016, p. A1.

will part from the cause. This final phase seals the recruitment process with the end game resulting in a new supporter and fighter for the Islamic State.

Discussion and Future Directions

What this analysis has demonstrated is that ISIS can successfully recruit many individuals around the world—particularly male and female youth—thanks to stage-by-stage relational development through internet chat rooms and social network sites (SNSs) like Twitter. By the same token, we also believe that, should ISIS not use internet chat rooms and SNSs, and if ISIS were not following those stages of relationship escalation, their recruitment process would not be as efficient. From this vantage point, the five relationship escalation stages allow us to see how relationships are formed and make it possible for us to understand the complexity of interpersonal interactions (both offline and online).

Overall, upon examining ISIS recruitment, we observed a trend of positive assurances made by terrorist recruiters in order to convince individuals to join the jihadist cause. According to Matusitz, “one method for solving a relationship crisis is to either enhance positive feelings or reduce certain negative feelings to make the other party content during the dialogue.”⁷⁷ By enhancing positivity, ISIS can make the recruit comfortable and vulnerable to manipulation. The objective of ISIS is to exterminate infidels and establish a caliphate around the world. So, in every phase of recruitment, positivity and encouragement are used as a form of persuasion. This terrorist organization has proven to excel in this process. It is important that we understand how ISIS employs these stages so that we can better help victims and put a stop to its widespread recruitment.

For future research, it may be interesting to examine two additional aspects of ISIS’s recruitment. First, with the European migrant crisis currently happening, in which over one million asylum-seekers have fled Muslim nations like Syria, Iraq, and Afghanistan as well as war-torn countries from Africa,⁷⁸ would ISIS be even more successful in its recruitment of would-be jihadists by infiltrating refugee camps? British Prime Minister David Cameron has warned us that “one in fifty Syrian refugees in Europe could be an ISIS jihadist.”⁷⁹ Under these circumstances, it would be useful to compare today’s ISIS’s recruitment through SNS with the organization’s infiltration of refugee camps. The objective would be to determine which of the two techniques is more efficient.

Second, an important question looms large: although studies and articles have confirmed that many ISIS recruits online are male and female youths, are young potential recruits all that naïve, lonely, and disaffected? It is true that many things are taken into account in order to make a good first impression –

⁷⁷ Matusitz, *Terrorism and Communication: A Critical Introduction*, quote on p. 365.

⁷⁸ Tim Arango, “Disappointed with Europe, Thousands of Iraqi Migrants Return Home,” *The New York Times*, February 4, 2016, p. A1.

⁷⁹ Cited in Alexandra Sims, “1 in 50 Syrian Refugees in Europe Could be an ISIS Jihadist, Minister Warns David Cameron,” *Independent*, September 15, 2015, p. A1.

from charismatic communication to appealing visuals and body language. Yet, it is also a known fact that a certain number of ISIS youth are highly educated individuals, with college degrees, and in-depth knowledge of science and engineering.⁸⁰ Hence, what are other factors that motivate youth to join ISIS? The answers to such questions need to be ascertained through solid research.

It is the authors' hope that this analysis of ISIS's recruitment, through the theory of relational development, has enlightened readers on how effective online social media can help a terrorist organization to be so successful at recruiting. This analysis can help others understand how easy it can be to manipulate individuals into joining a terrorist group simply through SNSs. Relational development was applied to a subject that had not been examined from such theoretical perspective before, making it a positive addition to the communication discipline at large. Both scholars and practitioners alike can now regard the ISIS recruitment process from a different angle.

About the authors

Sarah Ponder is a research assistant in the Nicholson School of Communication at the University of Central Florida. Her academic interests include terrorism studies, conflict studies, and intercultural communication.

Jonathan Matusitz, Ph.D., is an Associate Professor in the Nicholson School of Communication at the University of Central Florida. His academic interests include terrorism studies, communication & technology, and intercultural communication. Please address correspondence to Jonathan Matusitz at University of Central Florida at Seminole State College, Partnership Center (#UP 3009), 100 Weldon Blvd., Sanford, FL 32773, ☎ 407-708-2830.
E-mail: matusitz@gmail.com.

⁸⁰ Maajid Nawaz, "The Education of "Jihadi John," *The New York Times*, March 3, 2015, p. A1.



India's Counter-Terrorism Policy against Jihadist Terror: Challenges and Prospects

Vinay Kaura

Sardar Patel University of Police, Security, and Criminal Justice, Rajasthan, India

<https://www.policeuniversity.ac.in/>

Abstract: The nature of the jihadist terrorism in India is changing as radicalization and recruitment become more sophisticated. There are fears that India may become a soft target in the global jihadist plan of al-Qaeda and the ISIS, which are not only instigating violence through sleeper cells, but are also attracting educated Muslim youths through the Internet to spread their terror agenda while exploiting local grievances. To fight the rapidly changing threat of jihadist terrorism, India needs a comprehensive and innovative approach, rooted in a long-term strategic planning framework and coordinating intelligence, physical security, investigation and crisis management capabilities.

Keywords: Jihadist terrorism, Jammu & Kashmir, counterterrorism, comprehensive approach, intelligence, coordination, strategic planning.

Introduction

India has been facing several internal threats since its independence from Britain in 1947. The oldest and still unsolved violent struggle against the Indian state has been raging in the Northeast part of the country. But an unsettled sub-nationalist ethnic insurgency in India's Muslim-majority state of Jammu and Kashmir and the growing radicalization of a small but significant segment of the Muslim community in the country have emerged as biggest challenges for India's security. The nature of jihadist terrorism in India has undergone profound changes since the last two decades. Originally supported by Pakistan and confined to a specific territory in Indian-administered Kashmir, it has now become more defused with no specific area. In recent years, cities such as Mumbai, Bangalore, Hyderabad

and New Delhi have been targets of terrorist attacks. This makes facing the challenge and targeting of jihadist terrorists much more difficult than before.

Changing Nature of Jihadist Terrorism

With passage of time and the evolution of technology, the operational methodology of terrorists has evolved. Two crucial aspects need attention. First, the terrorism in Jammu & Kashmir (J&K) in the previous phase was started by disenchanted Kashmiri youths before the movement was hijacked by Pakistan as part of its low intensity war with India. In the present phase, J&K is confronted with terrorism predominantly handled by Pakistan's security establishment, either directly or indirectly through anti-India terror outfits such as Lashkar-e-Taiba, Jaish-e-Mohammad and Indian Mujahideen. The firepower of terrorists has also increased tremendously, partly due to the increased resource flow from across the border.

Second, the jihadist terrorism in India is on the verge of acquiring a global footprint, as radicalization and recruitment have become more sophisticated, thanks to social media and Internet. This marks a clear departure from the past when Jihadist terrorism was almost synonymous with the conflict in Kashmir. Most of the groups operating in Kashmir kept their activities confined to that theater except for sporadic incidents in other parts of the country. It was often held that ideologically motivated Islamist-Jihadist terror had bypassed mainland Indian Muslims and that even though there had been a separatist insurgency in the Jammu and Kashmir, Muslims in the rest of India had spurned the radical revivalist movements plaguing other Islamic countries. This is no longer the case.

It is feared that India may become a soft target in the global jihadist plan of outfits such as al-Qaeda and the ISIS, which are not only instigating violence through sleeper cells, but are also attracting educated Muslim youths through the Internet to spread their terror agenda. Though ISIS has declared its intention to expand its footprint in the Indian subcontinent,¹ it has not managed to make considerable headway in India. However, it is also an undeniable fact that a few of India's misguided Muslim youth are getting swayed by the Wahhabist propaganda. What has been most surprising is that many of the individuals arrested for involvement in some recent attacks are young men with good education and prestigious occupations, such as doctors and engineers. These men are often motivated through the Internet or through Pakistan-based terrorist networks. The majority of the homegrown terrorists are apparently self-radicalized, self-motivated and inspired by the jihadist ideology of al-Qaeda and ISIS as well as by local grievances. The groups formed to carry out the attacks are loose conglomerations, and it is still unclear whether there is an overarching commanding element directing the different cells.

¹ Husain Haqqani, "Prophecy and the Jihad in the Indian Subcontinent," *Current Trends in Islamist Ideology* 18 (May 2015): 5-17, <https://www.hudson.org/research/11310-current-trends-in-islamist-ideology-volume-18>.

To fight this fast-changing threat from the hybrid nature of jihadist terrorism, India requires a comprehensive, innovative and coordinated approach. But the central problem that aggravates India's national security policy is the absence of long-term strategic planning. Successive Indian governments have proved unable to formulate an adequate response to the challenge, which has increased the burden on India's security system, particularly its police and intelligence agencies. The internal security mechanism seems unprepared against the jihadist onslaught because of lack of political will and limited operational capacity of police and intelligence organizations.

Intelligence, physical security, coordination among agencies, investigation and crisis management are considered the most important components of counterterrorism activity. If the intelligence apparatus fails to provide early warning about an act of terrorism, the physical security machinery should be able to prevent the terrorists. And if both the intelligence and the physical security mechanisms fail, crisis management should be effective enough to cope with the consequences.² Not much data is available in the open domain about the lapses, however guarded analysis of some previous terrorist attacks indicates that intelligence, physical security, and the crisis management apparatus in India have not performed commendably. After each major terrorist attack, there are emotional demands to know how this can happen despite India's long experience in countering terrorism and insurgency in various parts of the country. In fact, India's institutional capabilities to counter terrorism have remained frozen, or have been augmented by tiny fractions of what is actually required. Even the current regime of Prime Minister Narendra Modi, which has emphasized the need for a robust security policy, has dithered on key security sector reforms. Many crucial projects relating to internal security continue to languish.

National Security Architecture

There are two styles of counterterrorist activities: a criminal justice counterterrorism, which deals with acts of terrorism within a law-enforcement framework, and a militaristic counterterrorism, which views terror as a threat to national security to be countered with armed force. India has resorted to a combination of both styles in its counterterrorism efforts.

Because of the very size of India and its heterogeneous character, the Indian Constitution has included a distribution of powers between the central government and the state governments; maintenance of law and order is a state subject. However, the federal nature of Indian polity complicates the structures

² Fred R. Schreier, "Combating Terrorism and Its Implications for Intelligence," in *Combating Terrorism and Its Implications for the Security Sector*, ed. Theodor H. Winkler, Anja H. Ebnöther, and Mats B. Hansson (Stockholm: Swedish National Defence College, 2005): 129-166, quote on p. 158; *A Case for Intelligence Reforms in India*, IDSA Task Force Report (New Delhi: Institute for Defence Studies and Analyses, 2012), p. 22, https://www.idsa.in/system/files/book/book_IntelligenceReform.pdf.

needed for counter-terrorism. Given these problems, India's performance in policing terrorism has been mixed.

Despite constitutional provisions, the Central government has raised seven Central Paramilitary Forces (CPMFs) which are regularly deployed for law and order duties along with the police forces of respective states.³ These seven CPMFs are the Central Research Police Force (CRPF), Border Security Force (BSF), Assam Rifles, Central Industrial Security Force (CISF), Indo-Tibetan Border Police (ITBP), Seema Surksha Bal (SSB), and the National Security Guard (NSG), founded in 1986 in the aftermath of Operation Blue Star. While the Indian army has about 1.2 million personnel, all seven CPMFs number more than 1.3 million. CRPF, the most important of the CPMFs, performs a wide range of duties including management of law and order, counter-insurgency and counter-terrorism all over India. Though the BSF and the ITBP are primarily meant for border security, they play a crucial role in counter-insurgency and counter-terrorism operations in three critical conflict-zones – the north-east, Maoist-affected areas, and Kashmir.

The Intelligence Bureau (IB), India's main intelligence agency, functions under the Ministry of Home Affairs and is responsible for internal security and intelligence needs. The IB is considered the nodal counter-terror agency and works closely with the State police and the central paramilitary forces on counter-terrorism intelligence. But it cannot fully execute this function because it has no legal authority to investigate an offence, arrest anyone or prosecute people in court. The Research & Analysis Wing (R&AW), India's premier external intelligence agency, operates under the Cabinet Secretariat and, thus, reports to the Prime Minister. It is generally believed that rivalries between the IB and the R&AW hamper overall intelligence effectiveness.⁴ Other intelligence agencies, such as the Central Economic Intelligence Bureau and the Directorate General of Military Intelligence also perform counter terror functions as part of their organizational mandate.

Following the Kargil incursion by Pakistan in 1999, the government of India carried out a thorough review and reform of India's intelligence apparatus in particular, and the national security system in general. Based on the recommendations of a Special Task Force, the government set up a revamped national security mechanism. The main features of the new mechanism include the creation of a National Security Council (NSC) chaired by the Prime Minister and consisting of a few cabinet members to discuss national security issues; a Strategic Policy Group (SPG) headed by the Cabinet Secretary and comprising the professional heads of the Ministries concerned with national security as well as the heads of the intelligence agencies and the armed forces to work out policy options and submit them to the NSC for consideration; a National Security Advisory Board

³ For a critical profile of India's central paramilitary forces, see K.S. Subramanian, *Political Violence and the Police in India* (New Delhi: Sage Publications, 2007), 105-124.

⁴ Prem Mahadevan, *The Politics of Counterterrorism in India: Strategic Intelligence and National Security* (New York: IB Tauris, 2012).

(NSAB) consisting of non-governmental experts to provide policy inputs to the National Security Council Secretariat (NSCS), which was set up to service the work of the NSAB, the SPG and NSC; and the creation of a National Security Advisor (NSA) to oversee the functioning of the new mechanism and to advise the Prime Minister on national security issues. The Joint Intelligence Committee (JIC), now a part of the NSCS, coordinates the intelligence inputs at the national level from all intelligence agencies and presents its independent analysis to the Cabinet Committee on Security (CCS). The Defense Intelligence Agency (DIA), started in 2002 as a nodal point to coordinate the activities of Army, Navy and Air Force Intelligence, complements the work of the R&AW.⁵ After the 26/11 Mumbai attack, India's counter-terrorism architecture has been revamped with the creation of the National Investigation Agency (NIA) to improve investigation capabilities. Deployment of the National Security Guard (NSG) has also been decentralized with four NSG hubs coming into being in different parts of India. The NSG has now matured strikingly as a terror-fighting agency. The amended Unlawful Activities Prevention Act (UAPA) has given new powers to the security agencies, including the ability to hold terror suspects for six months without charges.

Given the complexities involved in India's national security architecture, it is very important to improve coordination between various federal and state security agencies. Post-Mumbai attacks, the first step in this direction was the strengthening of the existing Multi-Agency Center (MAC), an intelligence-sharing 'fusion center' created within the IB in 2002 in the aftermath of the 1999 Kargil conflict. The national MAC coordinates across around two dozen representatives from the intelligence agencies in the home, finance and defense ministries.

The major connectivity in terms of intelligence sharing between the Center and states comes about through the state offices of the IB, and through the newly created Subsidiary Multi-Agency Centers (SMACS) as well as through the connectivity between the SMACS and state police Special Branches. It is another matter that personnel shortages have hindered their efficacy and in practice they function as little more than state-level IB offices. In a sign of the fundamental weakness of many of India's state police services, most of the intelligence inputs into the MAC come from a handful of states. Moreover, due to constitutional provisions, the intelligence sharing mechanism exists according to the goodwill of the states; if a state is not willing to cooperate with the central government, it cannot be forced to do so. Each agency guards its own turf, and coordination mostly depends on the interpersonal relationships between the officials of the agencies.⁶

⁵ Behram A. Sahukar, "Intelligence and Defence Cooperation in India," in *Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing*, ed. Musa Tuzuner (Amsterdam: IOS Press, 2010), 31-41.

⁶ For a review of India's security reforms after the Mumbai attacks, see Sarah J. Watson and C. Christine Fair, "India's Stalled Internal Security Reforms," *India Review* 12, no. 4 (2013): 280-299.

Due to this ad-hoc process and because of India's federal structure, the current national security architecture in general and the counter-terrorism structure in particular is flawed as there is no single authority from which these agencies receive unified directions.

Controversy over Anti-Terror Laws

Policing terrorism in India is fraught with numerous difficulties. The legal structure, inherited from the colonial past, has been struggling to cope with the demands placed upon it. As mentioned in the previous section, a number of police, intelligence and military organizations contribute to counter-terrorism efforts. India's Ministry of Home Affairs oversees national police, domestic intelligence and paramilitary forces. The major legislation to deal with terrorism in India is the UAPA. Some Indian states such as Maharashtra and Karnataka have their own laws which are used to prosecute suspected terrorists. The Terrorist and Disruptive Activities (Prevention) Act (TADA), the first anti-terrorism law to define and counter terrorist activities, was allowed to lapse in 1995.⁷ When there were several allegations of misuse in the application of the new anti-terror law, the Prevention of Terrorism Act (POTA), it was decided to repeal the act in 2004. This was followed by an amendment to the already existing UAPA. India's experiments with TADA, POTA and UAPA have failed to deliver the desired results. There have been allegations that the anti-terror laws are designed to shield or harass a particular community or religious denomination. The Second Administrative Reforms Commission (ARC) of India opined in its report in 2008 that "a comprehensive and effective legal framework to deal with all aspects of terrorism needs to be enacted. The law should have adequate safeguards to prevent its misuse."⁸

Failed Attempt to Create NCTC

The sweeping internal security reforms initiated after the Mumbai attacks were followed, a year later, by the announcement of central government's intention to create a National Counter Terrorism Center (NCTC) and a national computerized information-sharing network, known as the NATGRID. But the greatest failure of the post-Mumbai reforms was the NCTC, which was supposed to be established within a year of its announcement in December 2012. The central government's efforts to set up the NCTC—whose aim included preventing, containing and responding to a terrorist attack—were trapped in the political quagmire of Center-State relations and the intended launch of the NCTC had to be put on

⁷ "The Terrorist and Disruptive Activities (Prevention) Act, 1987," Act No. 28 of 1987, amended by Act 43 of 1993, available at the *South Asia Terrorism Portal*, www.satp.org/satporgtp/countries/india/document/actandordinances/tada.htm.

⁸ *Combating Terrorism: Protecting by Righteousness*, Eighth Report of the Second Administrative Reforms Commission (New Delhi: Government of India, June 2008), https://darp.gov.in/sites/default/files/combating_terrorism8.pdf.

hold. Non-Congress ruling states of Gujarat, Tamil Nadu, Odisha, Karnataka, Bihar, Tripura and West Bengal were opposed to the proposal; their main contention was that the NCTC would violate the principle of federalism. As per Indian Constitution, 'public order' and 'police' are in the State List, which is sole preserve of a state government.

The NCTC was conceived as the centerpiece of internal security reforms. It was modeled on the American institution of the same name, which functions as a center for joint operational planning and joint intelligence. India's NCTC, which was meant to subsume the MAC and whose operatives would have arrest powers throughout India, encountered a storm of criticism from State governments, who expressed strong concerns about the new agency being given the powers of arrest and searches without the prior knowledge of the state police. Similarly, the civil liberties activists saw the move as an unconstitutional expansion of government control. In the face of state opposition, plans for the NCTC were steadily watered-down: first the operational wing was eliminated, and then the NCTC as a whole was placed under the control of the Intelligence Bureau.

The states which opposed the NCTC cited two primary reasons for their opposition to it: clause 3.2 and the enabling section 43A of the UAPA, which authorized NCTC to arrest any suspect and to carry out operations without prior approval from and knowledge of the respective states; and clause 3.5, under which the NCTC would "have the power to seek information, including documents, reports, transcripts, and cyber information from any agency" in order to carry out its functions.⁹ In wanting to emulate the US model, the Home Ministry had overlooked a significant detail: the US NCTC is part of its Directorate of National Intelligence (DNI), which is manned by officials from the Pentagon, FBI, CIA and other agencies who can access its databases. The Center analyzes and collates terrorism related information to support counterterrorism operations of intelligence agencies. It is not authorized to conduct intelligence operations on its own and it has no powers to investigate or arrest.¹⁰

The Intelligence Bureau's control over NCTC also became a major bone of contention. It is commonly accepted principle in all liberal democratic countries that an intelligence agency should not possess police powers of arrest. Opposition parties expressed fear that if NCTC is made part of IB, the powers given to it under the UAPA could be misused. Presently IB is practically immune from any parliamentary oversight and its lack of parliamentary accountability would be further perpetuated by NCTC.¹¹ The gross politicization of India's intelligence

⁹ Sameer Patil, "Counter-Terrorism and Federalism," *Gateway House* (Indian Council on Global Relations, August 14, 2014), www.gatewayhouse.in/counter-terrorism-and-federalism/.

¹⁰ P.R. Chari, "National Counter Terrorism Centre for India: Understanding the Debate," *IPCS Issue Brief* 181 (New Delhi: Institute of Peace and Conflict Studies, March 2012), <https://www.jstor.org/stable/resrep09133>.

¹¹ Josy Joseph, "Locating NCTC Within Intelligence Bureau or Not: The Debate Continues," *Times of India*, July 17, 2012, <https://timesofindia.indiatimes.com/india/>

agencies has allowed the ruling parties to use these agencies to monitor the activities of the leaders of opposition parties and harass them. For instance, Bihar Chief Minister, Nitish Kumar, had opposed the proposed structure of NCTC on the ground that it was to be “created within the Intelligence Bureau which is a secret intelligence organization without any accountability to Parliament or the court”.¹² One should also not forget that there were several allegations that the NIA was used by the previous UPA government for political purposes to probe right-wing terror cases such as the 2006 Malegaon blasts and the 2007 Samjhauta Express bombings.

Second, the turf war between different intelligence agencies operating under different government ministries also caused problem for the establishment of NCTC. In fact, the Union Home Ministry committed the mistake by making the NCTC a part of the IB, rather than an independent institution. According to B. Raman, a former top official of the R&AW, “there were inadequate consultations even at the center as one could see from the opposition expressed by an increasing number of ex-R&AW officers to the move to make the NCTC a part of the IB.”¹³ Third, there have been several accusations of the alleged biases in the security agencies against the minority communities, particularly during counter terror operations.

Other internal security reforms have met with mixed success. The NATGRID was originally envisioned as a unified database that would compile a wide variety of currently available intelligence inputs. NATGRID has acquired some of the world’s most advanced data-mining software that can be used to track and potentially predict terrorist attacks. The system has faced internal resistance, however, particularly from the IB, which feels that NATGRID is encroaching on its turf.¹⁴ More than eight years after 26/11, NATGRID is still being spoken of as being in an ‘embryonic stage.’ Some of the features of NATGRID will be replicated by the Crime and Criminal Tracking Networks & System (CCTNS), which is meant to seamlessly link India’s more than 14,000 police stations to allow for better information-sharing. Several years later and despite a budget of millions of dollars, what “the government has to show for itself are a mess of reports, proposals, committees, red tape, turf battles, and the mirage of a robust security architecture.”¹⁵ After struggling with several problems, it has been decided to complete the implementation of the project by March 2017. The National Inves-

Locating-NCTC-within-Intelligence-Bureau-or-not-The-debate-continues/articleshow/15011283.cms.

¹² “NCTC Flouts ‘Sacrosanct’ Tenet: Nitish,” *The Telegraph*, May 6, 2012, available at https://www.telegraphindia.com/1120506/jsp/bihar/story_15456246.jsp.

¹³ B. Raman, “The NCTC Controversy,” *Outlook*, March 5, 2012, available at <http://www.outlookindia.com/article.aspx?280150>.

¹⁴ Sandeep Unnithan, “Anti-Terror Grid in Deep Freeze,” *India Today*, November 25, 2015, available at <https://www.indiatoday.in/magazine/nation/story/20151207-anti-terror-grid-in-deep-freeze-820885-2015-11-25>.

¹⁵ Unnithan, “Anti-terror Grid in Deep Freeze.”

tigation Agency (NIA) has also faced backlash from the states, which resist giving up their jurisdiction over policing. But the central government continues to push to make it the leading national agency.

Police incapacity

The Mumbai terrorist attack of 2008 and the Pathankot airbase attack of 2016 exposed key vulnerabilities in India's defenses against terrorism. Not only did they reflect a remarkable degree of sophistication on the part of jihadist planners, but the attacks demonstrated that the India's policing system was woefully inadequate for the task of combating suicidal assaults. Ajai Sahni, executive director of the Institute of Conflict Management, cannot be more correct when he argues that Indians "can't have first-rate counter-terrorism in a third-grade policing system." Praveen Swami, one of India's leading journalists having extensive knowledge of terrorism, echoes Sahni's argument when he observes that "Policing is the front line of a counterterrorism response; India's front line has disintegrated."¹⁶

Internal security faces added challenges with a poorly trained and understaffed police force, and insufficient modern equipment at their disposal. There is considerable variation in the size and competence of India's various State police forces. But India's low police-to-population ratio of about 180 per 100,000 is much lower of what the United Nations has recommended for peacetime policing. In Western countries, the police-to-population ratio ranges from 250 to 500 per 100,000. According to India's Bureau of Police Research & Development (BPRD), 24 % of posts in the police forces nationwide are lying vacant, with the State of Uttar Pradesh having the largest number of vacancies where only 181,000 police personnel are employed against the sanctioned strength of 363,000.¹⁷ Moreover, because of India's notorious and pervasive VIP culture, the number of police personnel actually available for the security of the common citizen is very dismal. Only one cop is available for the security of 729 Indian people, leaving police personnel overburdened and overstrained.¹⁸ Given the acute shortage in their ranks, police personnel are required to work long hours without a break and rarely get to take even their weekend off, leaving them stressed and frustrated. This has a huge bearing on their professional responsibilities, including counterterrorism duties.

¹⁶ Praveen Swami, "A Decade After 9/11, Indian Jihad Still Thrives," *The Hindu*, September 9, 2011, <https://www.thehindu.com/opinion/lead/a-decade-after-911-indian-jihad-still-thrives/article2439813.ece>.

¹⁷ PTI, "50 pc of Police Posts Vacant in UP; National Average at 24 pc," *India Today*, April 2, 2017, <https://www.indiatoday.in/pti-feed/story/50-pc-of-police-posts-vacant-in-up-national-average-at-24-pc-900731-2017-04-02>.

¹⁸ "Shortage of Police Personnel Alarming," *Deccan Herald*, February 16, 2017, available at <https://www.deccanherald.com/content/596749/shortage-police-personnel-alarming.html>.

Police in India are trained and mentally conditioned to deal with law and order problems. When faced with terrorism and insurgency, they find it extremely hard to respond effectively. To successfully prevent terrorism, the public must be willing to share with the police any vital information or suspicious activity in their locality, but even after 70 years of country's independence, the basic character and image of Indian police have not undergone any significant change. The police are held in low esteem and they are more often viewed with suspicion. Political interference in the functioning of the police, which has become a norm, leads to the abuse of authority by the police. Regrettably, many police officers deliberately allow their professional autonomy to be dominated by political pressures in their own anxiety to please the political masters. The most undesirable fallout of political interference in police functioning is the decline in its ability to respond effectively to difficult and violent situations. Ved Marwah, a former Indian Police Service officer and former governor of Manipur, Mizoram and Jharkhand, is straightforward in claiming that when state governments are reluctant or fail to deal with *violent conflicts and anti-national movements*, "instead of strengthening the state police machinery, it rushes to the Centre to hand over its responsibility at the first sign of any serious trouble. It is not surprising that in these states some sections of the police have actually joined hands with the subversive forces against the central forces."¹⁹

Corruption in the police also aggravates the challenge of fighting terrorism as there is a close relationship between crime, corruption and terrorism in the Indian context. For instance, criminal gangs such as 'D Company' have widespread networks for smuggling purposes, involving agents of corruption in the police and customs. Moreover, politicians have a leading role in manipulating the police for negative intentions or at least they turn a blind eye when police remain inactive in the face of communal disorders.

In 2006, the Supreme Court of India in a landmark judgment ordered the central and state governments to implement some crucial police reforms. From the standpoint of strengthening internal security, the most important order relates to the separation of the investigation and law and order functions of the police. Besides, the order to setup the State Security Commission is mainly directed to ensure that the state government does not exercise unnecessary influence or pressure on the police. But state governments have displayed absolute indifference to the Court order.²⁰ The reasons are not hard to find. The police are not insulated from partisan politics because the government does not allow the police to develop into an efficient and effective service. *All* governments want the police to behave "as the armed wing of their ruling party" as much of the power

¹⁹ Ved Marwah, "India's Internal Security Challenges," *Strategic Analysis* 27, no. 4, (October-December 2003): 503-515.

²⁰ "SC Anguished over States' Indifference to Police Reforms," *Zee TV News*, July 21, 2009, available at http://zeenews.india.com/news/nation/sc-anguished-over-states-indifference-to-police-reforms_549020.html.

of the executive in a post-colonial system like India is derived from the control of police.

With police reforms taking a back seat, the command and control systems of the police are also in a state of utter breakdown. The manner in which the police handled the Mumbai terror attacks in November 2008 clearly demonstrates that they are not trained for the task of confronting modern-day terrorism. The attack manifestly revealed the catastrophic weaknesses in Indian's police and intelligence apparatus. The Mumbai police did a poor job, not only due to a lack of nerve on the part of their top leaders, but also because of poor command and control. The Mumbai Police Commissioner "did not take charge of the situation and allowed all and sundry to jump into the fray and create a chaotic situation."²¹ The failure of intelligence agencies to anticipate major terror attacks including the Mumbai terror attacks of 2008 and "to apprehend most of those responsible over the years, speaks not just to weak, under-motivated, and under-equipped police forces but also to dubious intelligence capabilities."²²

India's former Prime Minister Manmohan Singh had underlined the importance of state police and intelligence agencies in the fight against terrorism, when he pointed out in September 2006, that "Unless the beat constable is brought into the vortex of our counter-terrorist strategy, our capacity to preempt future attacks would be severely limited."²³ Prime Minister Narendra Modi, at the Guwahati Conference of the Directors General of Police of states in November 2014, enunciated the concept of SMART Police – a police which should be sensitive, mobile, alert, reliable and techno-savvy.²⁴ However, there has hardly been any progress in that direction because not much has been done to either insulate the police from extraneous influences or to improve the orientation and operational capacity of the policemen themselves.

Twin Jihadist Challenges

The Pathankot airbase attack in January 2016, which exposed key vulnerabilities in India's defenses against terrorism, is the latest example of the continuance of India's weak national security decision making process, porous borders, limited law enforcement capabilities and political expediency. Seven security personnel

²¹ Ved Marwah, "The Role of India's Police in Combating Terrorism," in *Combating Terrorism*, ed. Maroof Raza (New Delhi: Viking, 2009), 80-97, quote on p. 83.

²² David Malone and Rohan Mukherjee, "Polity, Security, and Foreign Policy in Contemporary India," in *South Asia's Weak States: Understanding the Regional Insecurity Predicament*, ed. T. V. Paul (Stanford, CA: Stanford University Press, 2010), 147-169, quote on p. 160.

²³ See for example Ajit Kumar Singh, "Tuning the Indian Police," *Geopolitics* 2, no. 6 (November 2011): 54-55, quote on p. 55.

²⁴ "PM's address at the All India Conference of Directors General/Inspectors General of Police," *PMINDIA* – Official website of India's Prime Minister, November 30, 2014, www.pmindia.gov.in/en/news_updates/pms-address-at-the-all-india-conference-of-directors-generalinspectors-general-of-police-2.

were killed in the attack that lasted more than 72 hours. The attack demonstrated that the Indian policing system continues to remain woefully inadequate for the task of combating suicidal terror assaults, while confirming the widely-held perception that the country has not learnt much after the horrendous Mumbai terror attack of 2008. Similarly, the terrorist attack at an Indian army's brigade headquarters in the border town of Uri in Jammu and Kashmir in September 2016 again highlighted the threat India faces from cross-border terrorism. The attack, which claimed the lives of 19 Indian soldiers, was one of the biggest psychological and strategic blows to Indian security forces in Jammu and Kashmir. Although the Indian government carried out 'surgical strikes' against terrorist launching pads across the Line of Control (LoC) in Pakistan-administered Kashmir a few days after the attack in September 2016,²⁵ this counterattack has not been able to deter the Pakistan-based terrorists from indulging in cross-border terrorism.

Ajay Sahni has sarcastically noted that "if this is the state of protection of major national strategic assets, the preparedness—or rather, unpreparedness—across the rest of the country can only be imagined ... An examination of the security apparatus in the country, however, leads one to wonder why the attacks have been so few and relatively ineffective ... We have, moreover, been fortunate that the terrorists in this country have yet to adopt the even more devastating tactics, materials and technologies that are being used in other theatres of terrorism across the world."²⁶ The Parliamentary Standing Committee on Home Affairs, which investigated the Pathankot terror attack, has wondered why the Jaish-e-Mohammad terrorists let go a senior Punjab Police officer after way-laying his official vehicle and using it to reach the Pathankot airbase in January 2016. The multi-party committee, headed by the former Union home minister P Chidambaram, has lambasted the functioning of Punjab Police, while also asking many uncomfortable questions about the role played by the National Investigation Agency (NIA).²⁷ India's state of Punjab witnessed two terror attacks in the space of six months, first at Dinanagar in Gurdaspur district in July 2015, followed by Pathankot in January 2016.

To compound the challenge emanating from Pakistan-based jihadist outfits, there are many Indian Muslim youths who are estimated to be fighting for ISIS

²⁵ Manjeet Singh Negi, "Surgical Strikes in PoK: How Indian Para Commandos Killed 50 Terrorists, Hit 7 Camps," *India Today*, September 29, 2016, available at <http://indiatoday.intoday.in/story/uri-avenged-inside-story-indian-army-surgical-strikes-pok/1/776433.html>; Raj Kumar Arora and Vinay Kaura, "'Surgical Strikes' Beginning of a New Era in Counter-Terrorism in Kashmir?" *CPCS Occasional Paper* 10 (Jaipur: Center for Peace and Conflict Studies, October 2016).

²⁶ Ajay Sahni, "Pathankot Learnings: India Widely Exposed to Terrorism, Even in Best Protected Locations," *The Economic Times*, January 10, 2016.

²⁷ Rohan Dua, "House Panel on Pathankot Attack Puts Punjab Police SP Salwinder Singh Under Cloud", *The Times of India*, February 14, 2017, available at <http://timesofindia.indiatimes.com/india/house-panel-on-pathankot-attack-puts-punjab-police-sp-salwinder-singh-under-cloud/articleshow/57137279.cms>.

in Iraq and Syria. The IB estimated in 2016 that the Islamic States' Indian cell engaged more than 700 people in conversation and raised more than 20 identified volunteers.²⁸ During the last two years, the NIA has made several arrests of persons accused of forming ISIS modules, whose members use online social media platforms for plotting terrorist attacks.²⁹ The data suggests that people ideologically subscribing to ISIS are present across India, making it increasingly difficult for the law enforcement agencies to keep track of them. The Minister of State for Home Affairs of the government of India has informed the upper house of parliament that 75 people have been arrested for suspected links to the ISIS terror network. Out of these 75 persons, 21 were arrested from Kerala, 16 from Telangana, 9 from Karnataka, 8 from Maharashtra, 6 from Madhya Pradesh, 4 from Uttarakhand, 3 from Uttar Pradesh, 2 from Rajasthan, 4 from Tamil Nadu and one each from Jammu & Kashmir and West Bengal.³⁰ The NIA has also revealed that it had arrested 52 people for allegedly being ISIS terrorists in 2016, which also included a few converts from Hinduism and Christianity. While releasing data on the arrests, the NIA gave details of the religious affiliations of the accused; 50 percent belong to 'Ahle Hadith,' 30 percent to 'Tabligi Jamat,' and 20 percent followed Deobandi ideology. Out of 34 cases registered by the NIA in 2016, 21 were related to Jihadi terrorism.³¹

Initial investigations into the Bhopal-Ujjain passenger train blast in March 2017, which has been claimed as the first major ISIS operation in India,³² have given intelligence agencies a fresh challenge to pursue sympathizers of the global extremist group and track those highly-indoctrinated Indian Muslims that were fighting in Iraq and Syria. Saifullah, the alleged IS-inspired terrorist killed in a shootout with police on March 8, 2017 in Lucknow, had been tasked with securing arms and training facilities for a new Islamic State-linked cell in Uttar Pra-

²⁸ Praveen Swami, "For ISIS, Virtual is the Real as It Scouts for India Recruits," *The Indian Express*, March 22, 2016, available at <https://indianexpress.com/article/india/india-news-india/for-isis-virtual-is-the-real-as-it-scouts-for-india-recruits/>.

²⁹ K. K. Abdul Rahoof, "NIA Busts ISIS Terror Module in Hyderabad; 11 Suspects in Custody," *Deccan Chronicle*, June 30, 2016, <https://www.deccanchronicle.com/nation/current-affairs/300616/nia-nabs-11-isis-terrorists-in-hyderabad.html>; Shweta Desai, "Hyderabad Men's Pledge Shows Close Knowledge of Islamic State Group," *Daily News and Analysis*, December 26, 2016, www.dnaindia.com/india/report-hyderabad-mens-bayah-shows-close-knowledge-of-is-group-2286478.

³⁰ "75 Arrested for Alleged Links with ISIS: Govt," *Press Trust of India (PTI)*, March 15, 2017, http://www.ptinews.com/news/8503038_75-arrested-for-alleged-links-with-ISIS--Govt.html.

³¹ PTI, "Converted Hindus, Engineers among 52 ISIS Terrorists Held by NIA," *The Indian Express*, January 19, 2017.

³² Punya Priya Mitra, "ISIS Module Behind Blast in Bhopal-Ujjain Passenger Train in Madhya Pradesh, Police Say," *The Hindustan Times*, March 8, 2017, <https://www.hindustantimes.com/india-news/isis-module-behind-blast-in-bhopal-ujjain-passenger-train-in-madhya-pradesh-police-say/story-c0jKbjwKC0qa4xb2klfQVO.html>.

desh.³³ The NIA first came to know of Saifullah from Mudabbir Mushtaq Sheikh, a resident of the State of Maharashtra. Mudabbir is now facing trial for his role as chief of the Jund-ul-Khalifa-ul-Hind (army of the Caliph in India), an organization of Indian jihadists inspired by ISIS.³⁴

Indian agencies are reportedly worried on three accounts: first, a ‘lone actor’ attack, similar to some recent attacks in many European cities; second, presence of distinct terror cells which can be activated at short notice; and third, radicalized youth approaching other terror organizations for logistical support. Because of these factors, ISIS is being viewed as posing a serious security threat as its ideologues are not part of an organized group. By comparison, the Indian Mujahedeen (IM) was relatively easy to crack, because one arrested individual would “spill the beans” on other members. ISIS is a different phenomenon as every cell is different and is being handled by different operators abroad.³⁵ As ISIS has been routed in Iraq and Syria and their members are on the run, another worry of security agencies concerns their return to India.

Recommendations

The optimal functioning of India’s state institutions gets often compromised by poor functioning of institutional structures. The key lies in strengthening governing institutions at the state level, establishing the rule of law on a firm footing and providing a sense of dignity and security to its citizens.

- There is a need to make the National Security Council (NSC) a more professional and effective body, so that it can work in an optimal manner by anticipating national security threats and developing a coherent strategy to deal with them.
- Whilst intelligence should be the primary strategic consideration for addressing terrorism, it can only be effective if delivered in such a manner that meets the needs of its customers. In the age of jihadist terrorism, the characteristic of sound intelligence is the ability to fuse the intelligence gathered at the grassroots level with that analyzed at the national levels – what has become known in the US as ‘connecting the dots.’ The government should decide soon whether the required mechanism should be embedded in the existing agencies or in the establishment of a National Counter-Terrorism Center (NCTC) incorporating the functions being performed presently by the MAC and JIC.

³³ Praveen Swami, “Train Suspect Shot Dead Was Named Last Year by Member of IS-Inspired Cell, Police Lost Trail,” *The Indian Express*, March 9, 2017.

³⁴ Swami, “Train Suspect Shot Dead.”

³⁵ Sahil Makkar, “NIA chase, hawala and recruits: India turns into fertile ground for ISIS,” *Business Standard*, March 27, 2017, available at https://www.business-standard.com/article/current-affairs/nia-chase-hawala-and-recruits-india-turns-into-fertile-ground-for-isis-117032500782_1.html.

- The US established its Department of Homeland Security after 9/11. In India the need for the establishment of a separate Ministry of Internal Security has been felt for a long time, but this proposal continues to languish. The government should create this ministry and the NCTC should be placed under this new Ministry.
- The police are the first responders in the event of any terrorist attack. They are also the backbone of India's intelligence, investigation and anti-corruption agencies. For the security of the common citizen and to deal with the major threats confronting the country, India needs to have a reformed and restructured police force. Thus, the highest priority needs to be accorded to improving the profile of an average policeman at the grassroots level.
- Every police organization in India has deep-rooted inefficiencies built into existing processes of administration, deployment and operation. Large proportions of them are often wasted in unproductive deployments, without clear objectives within a crime-fighting or counter-terrorism framework. It is necessary to make an objective evaluation of current processes and redeploy the manpower more efficiently. Greater degree of police efficiency will also bring about changes in public perception.
- Given the fact that India is combating several active insurgencies along with countering terrorist attacks launched from inside and outside the country, it is imperative that Indian states increase the size of their police forces. An accelerated recruitment drive to fill all sanctioned posts in the police force should be the highest priority within a time-bound framework. Sanctioned strengths must also be continuously reevaluated in the context of emerging challenges.
- Most people in the security system remain oblivious to the transformations taking place in the field of policing and have little capacity to absorb and adapt to all but the most obvious technological manifestations of these transformations. For instance, India's state police forces are generally poorly trained and lack the ability to collect and analyze forensic evidence in accordance with international standards. Therefore, the training and education of police professionals must be a continuous and intensive process and must be built into the schedule of their responsibilities. Attention must be given to develop domain expertise on crime-fighting and counter-terrorism tactics.
- There are no cyber specialists or information warfare specialists, who would continue to work in their area of specialization after their limited tenures. The paramilitary and the army continue to be led by, what is often referred to as, generalist officers. Even when these officers develop a degree of specialization in the cyber domain, their next appointment often takes precedence over retaining domain expertise. Despite

having a National Cyber Security Policy since 2013 and a National Cyber Security Coordinator, the overall ecosystem of cyber security in India has not improved much. India must develop cyber security capacity among its security forces.

- The intelligence component of the state police requires greater augmentation. It should have an effective presence in each police station, particularly in the rural areas. Capacities to gather actionable and evidentiary intelligence also need to be developed, so that efficient prosecutions can be launched and convictions secured. Intelligence flows generated through the state police apparatus must interface in real time with the national databases, including MAC and CCTNS.
- India is not a wealthy country. Because of its sheer size and population, India has many pressing needs and the budgetary allocations for the internal security sector reflect India's lack of economic resources. Compared to the budgets of even much smaller developed countries, India cannot provide sufficient money for its security agencies, leading to problems of under-training and under-staffing and often counterproductive policing techniques. International assistance in the form of grants for training and equipping police forces could substantially reduce the burden of this major reform on India's budget. The United States can play a meaningful role in strengthening India's counterterrorism capabilities. One of the traditional strengths of the US law enforcement establishment has been training other countries' police and domestic intelligence agencies. India would benefit enormously from a sustained program bringing Indian police personnel to the US for training, as well as sending American trainers to Indian police academies. This training program would have the broader effect of increasing the professionalism of India's police and paramilitary forces.
- There is an urgent need for increased professionalism among state police personnel. India's Muslim community often perceives local police as biased and brutal. Focusing more on improving relations between the local police and Muslim communities can go a long way in preventing the radicalization of Muslim youth.
- If Indian Muslims, including disgruntled Kashmiri youth, are to be dissuaded from joining the so-called jihad, it is important to find more effective strategies to discredit Islamist radicals both on the battlefield and in cyberspace. The police, the paramilitary forces and the army in Kashmir must assertively employ all available social media platforms as well as all traditional propaganda tools to present an accessible, helpful, efficient and accountable image of themselves. India's security establishment would do well to put less emphasis on a heavy-handed and only tactical response to terrorism-driven insurgency in Kashmir. Given the growing importance of the insurgency's virtual dimension, it is vital

to frame a 'strategic narrative' – a compelling storyline which can explain the government's side convincingly.

Conclusion

India's response to terrorism has been largely characterized by ad-hocism, which has often led towards the creation of new agencies, meta-institutional innovations and over-centralization, an illusion of power created by technological acquisitions, and the states abdicating their law and order responsibilities. Political expediency further complicates the problem. The state governments remain preoccupied with their survival in power, which hamper their ability to look at the problem from a long-term perspective.

The internal security system is fragmented and poorly coordinated as there are a multitude of investigative and law enforcement agencies at the center and in the states. State police forces have their own counter-terrorism and intelligence units, which are often weak and work in an isolated manner. There has been an increase in the types and numbers of central paramilitary forces, but the most serious problem is of coordination of their efforts. The central and state agencies do coordinate through loosely defined mechanisms, but these are often found to be slow.

One of the major deficiencies in India's institutional approach to counter-terrorism is the gross divide between how the central and state governments view counter-terrorism. This is the reason why the proposal to create the National Counter-Terrorism Center (NCTC) has not achieved success. India cannot look for any early resolution of the problem of terrorism, either through strong anti-terror legislation or political amelioration of the issues that give rise to terrorism. Terrorism cannot entirely be countered by 'hardening' of possible targets by improving protection. Counter-terrorism activities, to be effective, must be proactive, and this intrinsically involves massive improvements in policing and intelligence – areas which have been terribly neglected. The implications of this neglect have been far-reaching. Whatever gains have been achieved in the fight against terrorism should not be allowed to be compromised or reversed because of inaction.

About the author

Vinay Kaura, PhD, is an Assistant Professor in the Department of International Affairs and Security Studies at the Sardar Patel University of Police, Security, and Criminal Justice in Rajasthan, India. He is also coordinator at the Center for Peace and Conflict Studies, Jaipur, at the Sardar Patel University of Police, Security and Criminal Justice. His research interests include India's neighborhood policy, especially on the western front, Afghanistan-Pakistan relations, counterterrorism and counter-insurgency, and conflict resolution in Kashmir.

E-mail: vinay@policeuniversity.ac.in.



Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region

Dasha Nicolson

Abstract: At the height of the influence of the ‘Islamic State’ in Syria, it involved in its ranks approximately 30,000 foreign fighters, with about a quarter of them coming from Russia (Chechnya and Dagestan) and the former Soviet Union. This article looks into the phenomenon of North Caucasian foreign terrorist fighters and its implications for security in North Caucasus, the Russian Federation and world-wide. The numbers of fighters returning from Syria to the region are not exactly known. Yet, upon returning home, the first wave of foreign fighters has managed to secure and build upon their reputations and expand their experience, skills and networks, establishing different *jamaats* and, in one instance, a ‘jihadist private military company.’ Given the opportunity, the second wave will most likely fight in the Caucasus, but if unable to return home they may be motivated to strike elsewhere.

Keywords: Russian, North Caucasus, Islamic State, foreign terrorist fighters, FTFs, antiterrorist legislation, counter-terrorist operations.

We are ashamed that we are going to Syria at a time when the Caucasus is still occupied, but young people are returning here once they’ve undergone a training course.

– BBC source, ‘close’ to Chechen boeviki

Introduction

In September 2014, the United Nations Security Council unanimously adopted resolution 2178 concerning the “acute and growing” threat posed by foreign terrorist fighters (FTFs). These individuals are defined as those “who travel to a State other than their States of residence or nationality for the purpose of the

perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict.”¹ FTFs affect the dynamic of conflict – its intractability, duration and intensity and, furthermore, pose a threat to their “States of origin, transit, destination, and neighboring zones of armed conflict in which they are active.”² Since the eruption of the civil war in Syria, and especially after June 2014 with the proclamation of the ‘caliphate,’ thousands of aspiring fighters from different regions have traveled to Iraq and Syria to join the Islamic State (IS) or other violent extremist groups.³ According to a report published by The Soufan Group in December 2015, the number of foreign fighters in Syria had reached approximately 30,000, with individuals from over 100 countries.⁴ In 2015, the top three FTF nationalities were Tunisian (6,000), Saudi Arabian (2,500), and Russian (2,300), while there were approximately 4,700 fighters from the Former Soviet Republics.⁵ In October 2015, Russian President Vladimir Putin stated that around 5,000 to 7,000 fighters from Russia and the former Soviet Union (FSU) had traveled to Syria to join IS.⁶ The majority of these fighters are from the North Caucasus (Chechnya and Dagestan), with others from Azerbaijan and Georgia as well as Central Asia – Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan. Together they share not only the ability to speak Russian, but also a heritage of grievances stemming from the Afghan-Soviet and the post-Soviet conflicts. This article attempts to look into the phenomenon of North Caucasian FTFs and its implications for security in North Caucasus, the Russian Federation and worldwide. In doing so, the motivations of North Caucasian FTFs, the groups that they fight for, and links to the domestic terrorist situation will be considered.

By 2017, the total numbers of FTFs in Syria and Iraq has fallen, both due to losses on the battlefield and to the decreased flow of foreign fighters to the conflict. For example, according to INTERPOL, in 2016 the number of FTFs deemed to be in the region amounted to 15,000.⁷ Among other factors, this reduction in mobilization of FTFs is attributed to increased control measures put in place by UN Member States, the military pressure brought to bear upon the groups and

¹ Resolution 2178 (2014), adopted by the UN Security Council at its 7272nd meeting, on September 24, 2014, S/RES/2178 (2014), [http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20\(2014\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20(2014)).

² UN SC Resolution 2178.

³ Global Coalition, *Foreign Terrorist Fighters – Trends and Dynamics, March 3, 2017*, <http://theglobalcoalition.org/en/foreign-terrorist-fighters-trends-and-dynamics>.

⁴ The Soufan Group, *Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*, December 2015, http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf.

⁵ The Soufan Group, *Foreign Fighters*.

⁶ The Soufan Group, *Foreign Fighters*.

⁷ Tanya Mehra, “Foreign Terrorist Fighters: Trends, Dynamics and Policy Responses,” *ICCT Policy Brief* (The Hague: International Center for Counter-Terrorism, December 2016), <https://icct.nl/wp-content/uploads/2016/12/ICCT-Mehra-FTF-Dec2016-1.pdf>.

IS's "financial decline." The organization's vital sources of income are tied to its territory: taxes and fees; oil; looting, confiscations and fines.⁸ Loss of territory and subsequent operation on "crisis budget" have caused the increase in desertion rates, difficulties in recruitment, and the growth of internal corruption and theft.⁹ Furthermore, as a result, the FTFs are suffering from low morale, many of them "are packing it in" and "want to defect."¹⁰ Of course, it is not only the decreased inflow of FTFs that has contributed to the fall in total numbers, but also the 'reverse flow' – FTFs returning to their home regions or moving to a third State. For example, by December 2016 approximately 30 % of European FTFs were thought to have returned to their home countries.¹¹ In view of this, the (overall) high number of North Caucasian FTFs involved in the conflict is a matter of concern. Will these FTFs return to their home regions with peaceful purposes or malicious intentions? Will they choose to stay in the conflict area and perhaps join other terrorist organizations as IS comes under increasing pressure? Or will they move to a third State, or reallocate and participate in a different conflict? Terrorism scholars Clarke and Amarasingham predict several options for transnational terrorists. The 'hardcore' FTFs of IS may stay in Syria and Iraq.¹² Some could seek to join an "underground resistance of an ISIS, 2.0," which may, with time, form a covert terrorist organization.¹³ Others may change allegiances between the groups on the ground, and eventually seek rapprochement with al-Qaeda. Other FTFs who are prevented from travelling to their countries of origin—the 'independent', the "free agents"—could form "a cohort of stateless jihadists" and travel to a third state in the name of jihad.¹⁴ Finally, the FTFs who

⁸ Stefan Heißenner, Peter R. Neumann, John Holland-McCowan, and Rajan Basra, *Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes* (London: King's College, International Center for the Study of Radicalization and Political Violence, 2017), <https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Caliphate-in-Degradation-An-Estimate-of-Islamic-States-Financial-Fortunes.pdf>.

⁹ Kairat Umarov, "Letter dated 11 January 2017 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council," S/2017/35, UN Security Council, January 13, 2017, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/000/13/pdf/N1700013.pdf>.

¹⁰ Paul Wood, "The Truth About Islamic State: It's in Crisis!" *The Spectator*, January 9, 2016, <https://www.spectator.co.uk/2016/01/the-truth-about-islamic-state-its-in-crisis/>; Martin Chulov, "Losing Ground, Fighters and Morale – Is It All Over for ISIS?" *The Guardian*, September 7, 2016, www.theguardian.com/world/2016/sep/07/losing-ground-fighter-morale-is-it-all-over-for-isis-syria-turkey.

¹¹ Mehra, "Foreign Terrorist Fighters: Trends, Dynamics and Policy Responses."

¹² Colin P. Clarke and Amarnath Amarasingham, "Where do ISIS Fighters Go When the Caliphate Falls? They Have Options," *The Atlantic Daily*, March 6, 2017, <https://www.theatlantic.com/international/archive/2017/03/isis-foreign-fighter-jihad-syria-iraq/518313/>.

¹³ Clarke and Amarasingham, "Where do ISIS Fighters Go When the Caliphate Falls?"

¹⁴ Clarke and Amarasingham, "Where do ISIS Fighters Go When the Caliphate Falls?"

return to their home countries could be either the “disillusioned,” the “disengaged but not disillusioned,” or the “operational.”¹⁵

North Caucasian FTFs are members of the much-fractured opposition to the Syrian government forces. The majority is in IS ranks, others are with al-Nusra, and the rest are part of numerous factions on the battlefield. Many of the North Caucasian FTFs have previous combat experience—for example, in Afghanistan, in Georgia, in Chechnya and Dagestan—and have reputations as fierce fighters. In fact, ‘Chechen’ fighters (and North Caucasians, generally) seem to be perceived as ‘elite fighters,’ worthy of respect.¹⁶ Such a reputation for violence seems to have been established in part by such individuals as Abu Omar al-Shishani (Tarkhan Batirashvili – now likely deceased as of 2016). Omar (Tarkhan) was from a village in the Pankisi Gorge that lies close to the Georgian-Chechen border. He was born to a Georgian father and an ethnic Chechen (Kist) mother and served for an intelligence unit of the Georgian army until he contracted tuberculosis. In 2010, he went to jail for weapons possession. His older brother, Tamaz, fought in the Chechen wars, and also subsequently joined IS. Omar became a prominent figure of the opposition, commanding powerful battalions such as the Jaysh al-Muhajirin wal-Ansar (Army of the Emigrants and Helpers) in 2013. Later on, in the year Omar al-Shishani became the northern commander for IS, leader of a Chechen and North Caucasian battalion within IS, and leader of special IS battalions.¹⁷ Generally, North Caucasian FTFs are concentrated in northern Syria – in Latakia and Idlib Provinces, Aleppo, and in the Turkish-Syrian border regions of Ras al-Ayn and Tal Abyad.¹⁸

Considering the high number of individuals involved as well as the history of conflict in the region, North Caucasian FTFs are likely to constitute a long-term security threat. It is also important to examine their motivations for fighting, the factions/organizations that they fight for, the extent of the influence of pro-jihadist propaganda and certain distinguishing characteristics (such as previous combat experience, ties to other terrorist organizations, etc.).

Motivations to Fight in Syria

Without doubt, the motivations of North Caucasian FTFs—as of those from other regions—are varied. However, one of the most important common motivations, distinguishing this group of individuals, is that the civil war in Syria provides an

¹⁵ Clarke and Amarasingham, “Where do ISIS Fighters Go When the Caliphate Falls?”

¹⁶ Joanna Paraszczuk, “IS’s Abu Waheeb Really Liked North Caucasians’ & Notes on Circassians and Shishanis,” *From Chechnya to Syria*, October 21, 2016, <http://www.chechensinsyria.com/?p=25267>.

¹⁷ “Natives from the Caucasians in the Ranks of IS (ISIS),” *Kavkazsky Uzel [Caucasian Knot]*, February 21, 2017, <http://www.kavkaz-uzel.eu/articles/251513>.

¹⁸ Emil Souleimanov and Megan Ouellette, “The Participation of North Caucasian Jihadists in the Syrian Civil War and its Security Implications,” *Rubin Center*, February 22, 2015, www.rubincenter.org/2015/02/the-participation-of-north-caucasian-jihadists-in-the-syrian-civil-war-and-its-security-implications.

alternative battleground for fighting against the Russian state.¹⁹ The conflict in North Caucasus, and especially in Chechnya, has a long history and revolves around the issue of gaining independence from the central government. This fight can be traced back to Imperial Russia and includes the two more recent bloody Russo-Chechen Wars as well as instabilities within the region. The protracted state of conflict (and official attempts at its normalization) produced and left grave societal issues and a heritage of immense grievances. These are the fuel for the North Caucasian resistance, for militants and extremists. However, insurgents or militants are left with a very limited ability to ‘carry out the fight’ in the region. For example, in Chechnya this is due to the pro-Kremlin government under former rebel Ramzan Kadyrov. The inability to ‘carry out the fight’ in the North Caucasus, in combination with Moscow’s support for the Assad regime, serve as push-factors to join the fight in Syria. As Omar Shishani openly acknowledged in an interview that was re-published by *EA Worldview* in December 2013, the ‘Caucasus Emirate’ (CE) had ‘sent in’ fighters to Syria for the purpose of training. The aim was that they would then return ‘experienced’ to fight against Russia in the North Caucasus. In other interviews, Shishani mentions the wish to “weaken one of al-Assad’s key allies” (i.e. Russia), and notes that “jihad against the Russians and their Baathist ally” was one of his primary motivations for fighting in Syria.²⁰

On a side-note, the counter-terrorist operations (CTOs) carried out by Russian governmental and Special Forces and their consequences sometimes leave individuals with no choice but to leave the region, and establish themselves elsewhere.²¹ For example, this was the case for Abdulkadyrov—“who fought here in the forest”—from Dagestan: he was hunted by local law enforcement and militants, and in order to escape from both, left to fight in Syria.²² Before the 2014 Sochi Olympics, Turkey had also become a popular destination for both jihadists

¹⁹ Dmitry Shlapentokh, “The North Caucasian Resistance and the Syrian Crisis,” *Insight* 83 (Singapore: Middle East Institute, National University of Singapore, 3 December 2012), <https://mei.nus.edu.sg/publication/insight-83-the-north-caucasian-resistance-and-the-syrian-crisis/>.

²⁰ Jack Moore, “The Ginger Jihadist of Mosul: Omar Shishani the Chechen ‘General,’” *International Business Times*, June 24, 2014, <http://www.ibtimes.co.uk/ginger-jihadist-mosul-omar-al-shishani-chechen-general-1452232>. See also Thomas Grove and Mariam Karouny, “Militants from Russia’s North Caucasus join ‘Jihad’ in Syria,” *Reuters*, March 6, 2013, <http://www.reuters.com/article/us-syria-crisis-russia-militants-idUSBRE9251BT20130306>; and Erin McClam, “Rising Star of ISIS Has Chechen Background and Fierce Reputation,” *RMSMC blog*, July 2, 2014, <https://rmsmcblog.wordpress.com/2014/07/11/more-on-omar-al-shishani-part-ii>.

²¹ Elena Milashina, “Caliphate? A Bait for Fools!” *Novaya Gazeta*, July 29, 2015 (in Russian), www.novayagazeta.ru/articles/2015/07/29/65056-171-halifat-primanka-dlyadurakov-187. Milashina investigated the town of Novosaitli in the Khasavyurt district of Dagestan. In her article, she includes descriptions of several individuals who had left to fight in Syria.

²² Milashina, “Caliphate? A Bait for Fools!”

transiting to Syria and the peaceful conservative Muslim families.²³ Also, in 2016 ‘thousands of Chechens’ travelled to Germany through Poland, in order to claim asylum.²⁴ In June 2016, the number of Russians claiming asylum in Germany amounted to 1,835, reportedly 90 % of them were Chechen; and from the 6,100 who applied in Poland – 94 % were from North Caucasus.²⁵ According to head of the Brandenburg central registration office for foreigners, Frank Nürnberger, a similar surge had occurred in 2013, with a decline in 2014, and an increase in 2016.²⁶

Of course, another prominent motivational factor is religion. Just as during the Chechen/Dagestani/Ingush resistance when religion served as a force to attract foreign fighters to Chechnya, so has religion been used as a unifying force by North Caucasians fighting in Syria. Many young men had been drawn to ‘join the Syrian jihad’²⁷ and convinced that it is their duty to take up arms. For one, they regard the Alawite (heterodox sect of Shi’i Islam) Assad regime as ‘not truly Muslim’ and ‘infidel.’²⁸ Second, the regime is perceived as ‘Russia’s key ally’ in the Middle East. So, it is not only an opportunity for jihad, but also a duty of Russian-speaking Muslims to join their oppressed brothers in Syria.²⁹ Most of North Caucasian FTFs are salafist. Others exhibit ‘Sunni solidarity’ in response to images and propaganda of Sunni Muslims injured/tortured/killed by the ‘infidel’ Alawi regime.³⁰ Thus, the battleground in Syria presents North Caucasian FTFs with the chance to fight both the Russian government and its interests, and to fight the enemies of Islam worldwide.³¹

Furthermore, by participating in the Syrian civil war, inexperienced FTFs may obtain combat experience and establish connections – and engage in domestic insurgency or terrorist activities upon their return home. In addition, participa-

²³ International Crisis Group, “The North Caucasus Insurgency & Syria: An Exported Jihad?” *Europe Report* no. 238, March 16, 2016, <https://www.crisisgroup.org/europe-central-asia/caucasus/north-caucasus/north-caucasus-insurgency-and-syria-exported-jihad>.

²⁴ Alix Culbertson, “Thousands of Chechens Slipping Through Unmanned Border in Latest German Migrant Crisis,” *Express*, August 24, 2016, <http://www.express.co.uk/news/world/703337/Chechen-migrants-unmanned-German-border-Poland>.

²⁵ Janosch Delcker, “Germany’s New Problem Border: Poland,” *Politico*, August 24, 2016, <http://www.politico.eu/article/police-officials-concerned-about-migrants-crossing-german-polish-border-terrorism-migration>.

²⁶ Delcker, “Germany’s New Problem Border: Poland.”

²⁷ Emil A. Souleimanov, “Globalizing Jihad? North Caucasians in the Syrian Civil War,” *Middle East Policy* 21, no. 3 (Fall 2014), <http://www.mepc.org/globalizing-jihad-north-caucasians-syrian-civil-war> (21 August 2017).

²⁸ Shlapentokh, “The North Caucasian Resistance and the Syrian Crisis.”

²⁹ Souleimanov and Ouellette, “The Participation of North Caucasian Jihadists in the Syrian Civil War and its Security Implications.”

³⁰ Souleimanov and Ouellette, “The Participation of North Caucasian Jihadists in the Syrian Civil War and its Security Implications.”

³¹ Souleimanov, “Globalizing Jihad? North Caucasians in the Syrian Civil War.”

tion in the conflict may offer an opportunity for identity reconstruction – by stepping out from a life of poverty and unemployment, where “one has nothing left,” to fighting for “a brotherhood in arms” and for “a noble” cause.³²

The battle ground in Syria demonstrates the rise of a ‘jihadist international,’ as Mark Galeotti refers to the phenomenon, with fighters willing to travel from one conflict zone to another in the name of violent jihad, regardless of whether they have any personal connection to the conflict or not.³³ First, this can be seen through the presence of numerous factions comprised of North Caucasians and individuals from Central Asia in Syria and Iraq (independent or al-Nusra affiliated). Second, in the case of some North Caucasian FTFs, this can be seen through the change of alliance among the different armed groups operating in the region, primarily fueled by the motivation to fight in the opposition to the al-Assad regime in order to fight Russia. One example is Omar Shishani, who eventually ended up in IS ranks. Third, some of the prominent individuals have a history of participation in previous conflicts. The phenomenon, however, is not new – during the Chechen Wars, foreign warlords (Saudi-born Ibn Khattab, Abu Omar al-Saif, among them) established their commands in the North Caucasus. The term, ‘*jihadist international*’ then, can be used as a classification of FTFs, denoting those that are potentially more dangerous for global civil society because of higher commitment, greater (potential/future) experience, and the continued readiness to fight regardless of a personal connection to a given conflict.

Some scholars, for example Ratelle, argue that North Caucasian fighters can be divided into two waves: those that travelled to Syria in 2011-2013 because they could not fight in their home region, and those who traveled to Syria in 2014-2017 because they ‘openly decided’ not to fight in the North Caucasus and “to join an international jihadist front.”³⁴ The contestation between Imarat Kavkaz (Caucasus Emirate) and the Islamic State can, to some extent, explain this dynamic.

Imarat Kavkaz vs Islamic State

Imarat Kavkaz (IK, also known as the Caucasus Emirate, or CE) is a self-proclaimed separatist group which aspires to establish its own Islamic State within the North Caucasus.³⁵ It was established in 2007, during the period of the Second Chechen War, by warlord Doku Umarov. He proclaimed himself to be the ‘Emir of the *mu-*

³² Souleimanov and Ouellette, “The Participation of North Caucasian Jihadists in the Syrian Civil War and its Security Implications.”

³³ Mark Galeotti, “Chechen ‘Jihadist International’ Emerges in Syria,” *Russia Beyond the Headlines*, April 15, 2013, https://rbth.com/opinion/2013/04/15/chechen_jihadist_international_emerges_in_syria_25025.html.

³⁴ Jean-François Ratelle, “North Caucasian Foreign Fighters in Syria and Iraq: Assessing the Threat of Returnees to the Russian Federation,” *Caucasus Survey* 4, no. 3 (2016): 218-238.

³⁵ “Imarat Kavkaz,” *Kavkazsky Uzel [Caucasian Knot]*, December 27, 2016, www.kavkaz-uzel.eu/articles/158730.

jahideen of the Caucasus,' the 'leader of jihad' and the 'only legitimate power in all the territories, where *mujahideen* are present,' uniting the militant *jamaats*.³⁶ As of the moment of its formation, the Emirate consisted of six Vilayats (territorial administrative formations): Dagestan, Nokhchicho (Ichkeria), Galgaiche (Ingushetia), Iriston (North Ossetia), Nogai Steppe (Stavropol Territory) and the united valayat of Kabarda, Balkaria, and Karachay. Furthermore, the Caucasus Emirate had an official representative office abroad—the Vekalat—headed by an authorized representative of the *mujahideen* and the Caucasus Emirate.³⁷ However, in 2010, under the Omra³⁸ # 20 Doku Umarov abolished the Vekalat. Furthermore, by 2010, CE was recognized as a terrorist organization both by Russia and the US.

At the same time, already in 2010 the organization had started to suffer from internal fragmentation. By the end 2014, with the death of Doku Umarov (officially announced by the Federal Security Bureau (FSB) in 2014) and the subsequent hassle surrounding the appointment of successive leadership and later their elimination, the Caucasus Emirate headquarters moved several times. In fact, the whole organization had become even more fragmented and, perhaps, even entered a state of decline. Some experts (Roschin, for example) point to the change in terrorist tactics of the CE – notably more suicide bombings, carried out by young men and women, as an indicator of the declining state of affairs of the organization. In Autumn 2014, Zailanabidov (the leader of a militant group operating in the Khasavyurt district in Dagestan) took an oath to Abu Bakr al-Baghdadi (leader of IS).³⁹ His example was followed by several other militant leaders, who called upon their 'brothers' to do the same. Importantly, a pledge of allegiance to al-Baghdadi in this context requires the individual to renounce their oath to the CE. These actions further aggravated the fragmentation between North Caucasian militants. Presently in 2017, CE is hardly functional, as most of the leaders of its remaining units in Russia have been neutralized.

Throughout the development of the conflict in Syria, starting from 2011 and 2012, the factions led by North Caucasian FTFs in Syria got caught up in the struggle for control over the Syrian opposition between al-Qaeda and IS. In fact, the factions that had appeared in Syria in the first two years of the conflict were very much linked to the Caucasus Emirate. The first North Caucasian *jamaat* in Northern Aleppo was under the command of a veteran Chechen fighter known as Khamzat (the first Imarat Kavkaz emir in Syria). This was "effectively an outpost of IK," according to Joanna Paraszczuk.⁴⁰ Generally, the Caucasus Emirate rested its loyalties with al-Qaeda – at least, in the early stages of its operations. CE

³⁶ "Imarat Kavkaz," *Kavkaz Uzel*.

³⁷ "Imarat Kavkaz," *Kavkazsky Uzel*.

³⁸ Directive/Order.

³⁹ "Imarat Kavkaz," *Kavkazsky Uzel*.

⁴⁰ Joanna Paraszczuk, "1st Imarat Kavkaz Amir in Syria Fought Alongside Gelyaev in Chechnya, Died Fighting Alongside Ahrar," *From Chechnya to Syria*, July 21, 2016, <http://www.chechensinsyria.com/?p=25171>.

differs from IS not only ideologically, structurally, in terms of recruitment and the extent of violence it uses, but also in the manner of operation. It works through what Orkhan Dzemat, a regional journalist, refers to as “night-time government” – a parallel government with a clear military structure, “ruling over people oppressed by the weight of the world.” IS, however, adopted a “day-time” approach, calling on entire families to join and start a new life.⁴¹

Prior to 2015, the leaders of CE would denounce those militants who took an oath to al-Baghdadi, and some of those would later re-instate their loyalties to the Caucasus Emirate. For CE, the absence of charismatic leaders, increased fragmentation within itself, the lack of finances and difficulties in recruitment, combined with the impact of CTOs on behalf of the Russian government, have possibly made the alternative Islamist narrative more appealing, making space for IS presence and power.

Interestingly, CE technically had a ‘velayat’ in Syria, known as Imarat Kavkaz v Shame. On 8 July, 2015, Salakhuddin Shishani and a group of fighters loyal to CE pledged *bay’ah* to the new CE emir – Abu Usman Gimrinski (Suleimanov). Abu Usman was killed in August 2015 as a result of a CTO carried out by Russian governmental forces. In December 2015, Salakhuddin was removed as the emir of Imarat Kavkaz v Shame. The organization had later in 2016 engaged in battles in the southern Aleppo countryside alongside Junud al-Aqsa⁴² and al-Nusra. However, it seemed that the majority of the fighters were, in fact, Syrian.⁴³

On 23 June 2015, IS declared the formation of a new vilayat in Russia’s North Caucasus. This declaration followed a string of formal pledges of allegiance of thousands of militants in the region, echoing those of 2014, thus signifying the decline of Imarat Kavkaz and highlighting the need to assess the extent of ISIS influence in the region. As a result of effective IS propaganda targeting Russia and its neighboring countries, by 2017 Russian had become the third most spoken language in IS, after English and Arabic. There is even an IS magazine, published in Russian – *Istok*, and a media platform called *Furat Media*.

For Whom Do the North Caucasians Fight?

The first North Caucasians in Syria became active around 2012, most of them forming the North Caucasian *jamaat* (groups). According to some sources there were around 15-17 fighters, and among them such figures as Omar al-Shishani,

⁴¹ As quoted in Anna Borschevskaya, “The Islamic State Comes to Russia,” *Journal of International Security Affairs* (Fall/Winter 2015): 27-32, available at <https://www.washingtoninstitute.org/policy-analysis/view/the-islamic-state-comes-to-russia>.

⁴² “Jund al-Aqsa,” in Jihad Intel’s “Database: Identifiers of Designated Islamic Terrorist Organizations,” Middle East Forum, <http://jihadintel.meforum.org/group/123/jund-al-aqsa> (21 August 2017).

⁴³ Joanna Paraszczuk, “Arabic-Speaking Katiba Guraba Fighting Under Auspices of IK v Shame in South Aleppo,” *From Chechnya to Syria*, March 10, 2016, <http://www.chechensinsyria.com/?p=25028>.

Salakhuddin al-Shishani, and Sayfullakh Shishani.⁴⁴ Omar al-Shishani and Sayfullakh had left to form a new, relatively small group called Katiba Muhajireen, which in 2013 would merge with two others (the Arab Kata'ib Khattab and Jaysh Muhammad) to form Jaish al-Muhajireen wal-Ansar. Khamzat, however, stepped out of CE, and later went to fight alongside Ahrar al-Sham⁴⁵ in Aleppo.

Throughout the development of the conflict in Syria, the number of fighters from the North Caucasus, the rest of Russia and the Commonwealth of Independent States (CIS), rose to around 5,000-7,000. The probable motivations of these FTFs have been mentioned – one of the most important being the wish to fight the Russian State and fight against the al-Assad regime. Yet, who do they fight for? Generally speaking, the fighters can be classified as IS-allied and as al-Nusra (i.e. al-Qaeda) allied. However, the dynamic is complicated, as throughout the conflict factions have switched alliances due to within-faction dynamics, developments within CE, and the changing relationship between IS and al-Nusra.

Jaish al-Muhajireen wal-Ansar (JMA, The Army of Emigrants and Helpers)

One of the most prominent jihadi groups with originally large North Caucasian membership is *Jaish al-Muhajireen wal-Ansar (JMA, The Army of Emigrants and Helpers)*. As mentioned above, it was formed as a result of a merger between several other factions, and it was Chechen-led, with about a third of the fighters coming from the North Caucasus. The group played an important role in the civil war. It was involved in capturing strategic infrastructure in the north, and is known for its military prowess, high-profile leadership, and affiliation with al-Qaeda. Omar al-Shishani was the first leader of the group and maintained ties with CE since the group needed 'authority in Syria,' while Omar needed men. The majority of men arriving in Syria from North Caucasus were under oath to Umarov, and Omar Shishani told them that he was also under oath to the CE leader. According to some sources, he had tried to preserve JMA autonomy from either IS or al-Nusra.⁴⁶ Yet, in March 2013 he pledged *bay'ah* (allegiance) to IS leader al-Baghdadi, along with some of his men. This caused a split inside JMA – many CE loyalists perceived it as 'treason,' while at the same time Omar accused Sayfullakh of theft and *takfir*, ousting him from JMA.⁴⁷ The majority of Russian-speaking fighters faced a dilemma: either to continue fighting independently, under oath to CE, or to swear *bay'ah* to the IS leader.

⁴⁴ Paraszczuk, "1st Imarat Kavkaz Amir In Syria Fought Alongside Gelyaev In Chechnya, Died Fighting Alongside Ahrar."

⁴⁵ "Ahrar al-Sham," in *Mapping Militant Organizations*, updated August 5, 2017, <http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/523>.

⁴⁶ Joanna Paraszczuk, "Umar Shishani's Biographer Distances Him from Imarat Kavkaz Bayah," *From Chechnya to Syria*, August 1, 2016, www.chechensinsyria.com/?p=25200.

⁴⁷ Joanna Paraszczuk, "Khalid Shishani on Why Sayfullakh Shishani & Umar Shishani Fell Out," *From Chechnya to Syria*, August 23, 2016, www.chechensinsyria.com/?p=25233.

Later, Omar would leave JMA and defect to IS in November 2013, taking many fighters with him. He would become a high-profile commander of a northern battalion with a large Russian-speaking membership. Likewise, when Sayfullakh was ousted, many North Caucasian fighters followed him to join Junud al-Sham.⁴⁸ JMA in 2014 would join the Ansar al-Din coalition, and later pledge allegiance to al-Nusra. Salakhuddin Shishani was the emir of JMA and reportedly attempted to maintain neutrality between the IS and al-Nusra, and even attempted to facilitate a truce. In June 2015, Salakhuddin Shishani (also the emir of Imarat Kavkaz v Shame) was ousted from JMA, and together with FTFs loyal to him and to CE left to establish the Imarat Kavkaz v Shame.⁴⁹ The same year, some of the Russian Speakers from JMA joined Katiba Sayfullah (an Uzbek-led group, part of al-Nusra) to form Liwa al-Muhajireen, although there is not much information about the group.⁵⁰ Muslim al-Shishani, yet another influential FTF from Georgia's Pankisi Gorge, was the leader of Junud al-Sham, who tried to maintain the faction's independence. However, in 2016 Junud al-Sham dissolved, and Muslim and the majority of North Caucasian fighters joined Ajnad al-Kavkaz, supposedly also independent from the Caucasus Emirate.⁵¹ Salakhuddin Shishani and his followers formed in 2016 a new group, Jaysh al-USrah.⁵² As of 2017, JMA is part of Hayat Tahrir al-Sham—the very recently rebranded al-Nusra—which claims to have no ties to al-Qaeda.⁵³

⁴⁸ "Jund al-Sham – Syria," Terrorism Research & Analysis Consortium (TRAC), <https://www.trackingterrorism.org/group/jund-al-sham-syria> (21 August 2017).

⁴⁹ Joanna Paraszczuk, "Salakhuddin Shishani Swears *Bay'ah* to New CE Emir," *From Chechnya to Syria*, July 9, 2015, <http://www.chechensinsyria.com/?p=23921>.

⁵⁰ Joanna Paraszczuk, "'Umar from the Caucasus' is Emir of Nusra's Liwa al-Muhajireen Wal Ansar," *From Chechnya to Syria*, March 12, 2016, www.chechensinsyria.com/?p=25032.

⁵¹ Joanna Paraszczuk, "Interview & Letter from Anjad al-Kavkaz Amir Abdul Hakim Shishani," *From Chechnya to Syria*, February 24, 2017, www.chechensinsyria.com/?p=25309#more-25309; and Joanna Paraszczuk, "Anjad al-Kavkaz Don't Have Bay'ha to Caucasus Emirate," *From Chechnya to Syria*, May 22, 2015, available at <http://www.chechensinsyria.com/?p=23771>.

⁵² Joanna Paraszczuk, "Salakhuddin Shishani is Emir of Jaish al-USrah, Khayrullah Shishani Is His Deputy," *From Chechnya To Syria*, February 16, 2016, available at <http://www.chechensinsyria.com/?p=24678>.

⁵³ Hayat Tahrir al Sham (HTS) formed following a merger between Jabhat Fateh al-Sham (al-Nusra), Ansar al-Din Front, Jayish al-Sunnah, Liwa al-Haqq, Nour al-Din al-Zinki Movement on 28 January 2017. In his message from 9 February 2017, HTS leader Abu Jabir insisted that the organization "is an independent entity and not an extension of previous organizations or factions." This is seen as an attempt to further distance the organization from al-Qaeda. See BBC Monitoring, "Tahrir al-Sham: Al-Qaeda's Latest Incarnation in Syria," *BBC News*, February 28, 2017, <https://www.bbc.com/news/world-middle-east-38934206>; Thomas Joscelyn, "Hay'at Tahrir al Sham Leader Calls for 'Unity' in Syrian Insurgency," *FDD's Long War Journal*, February 10, 2017, <https://www.longwarjournal.org/archives/2017/02/hayat-tahrir-al-sham-leader-calls-for-unity-in-syrian-insurgency.php>.

The majority of North Caucasian FTFs reside with IS (especially in view of the effective IS propaganda) and the second largest number – with al-Nusra (now Hayat Tahrir al-Sham). Both organizations have North Caucasians in some of the leadership positions. Those that are loyal to IS often criticize the others (al-Nusra and Imarat Kavkaz-allied) for their ‘alleged indecisiveness and nationalism,’ while the latter disapprove of IS and their excessive use of violence against civilians.

Regardless of whether the FTFs from the North Caucasus joined the ranks of IS, al-Nusra (now Hayat Tahrir al Sham) or other factions, the reputation of being fierce fighters follows them – they tend to take on a higher death toll than local fighters and are often considered as ‘elite.’ In addition, many North Caucasians are known for plunging into the front lines with no intent of returning alive.⁵⁴ The degradation of the Caucasus Emirate influenced the dispersion of North Caucasian FTFs on the Syrian battleground. Especially after 2014, many FTFs joined IS. The CE decline also allowed for the emergence of IS in North Caucasus. While it may be used just as a substitute ‘brand’ by the local militants, IS still has a network for present and future use. Furthermore, the numerous ‘independent’ and al-Nusra affiliated factions harbor individuals who have been involved in the Syrian conflict for a long time. They have gained experience and connections and are fueled by the motivation to fight the Russian government. Many of them can be expected to pose a threat in the future – either in the Caucasus or in other conflict areas.

North Caucasian leaders such as Omar al- Shishani had frequently been used as the ‘face’ for IS propaganda in Russian in order to attract more fighters. Furthermore, according to other (non-IS) jihadists, IS propaganda had proven to be extremely effective in attracting youth from the Caucasus region and by 2014 the number had almost doubled. The Europol report also references an article from the Russian daily *Novaya Gazeta*, in which the author postulates that the FSB actually facilitates the travel of extremists from Chechnya and Dagestan to Syria in order to reduce violence within the Russian Caucasus region. Moreover, there seems to be a propaganda war between IS and non-IS affiliated Russian speaking pro-jihadists (e.g. between IS and al-Nusra), which IS appears to be winning. In a letter written via the Kavkaz Center’s Telegram account, Khalid Shishani wrote that the North Caucasian youth is generally oblivious to the true nature of the “pseudo-caliphate (IS),” and “explanations on Al-Insad website... and about scholars of jihad such as Abu Qatada Al-Filistini.”⁵⁵ He further proposed to step up their own propaganda efforts through the use of various social media accounts with an expectation of receiving constant bans, because “in Chechnya the majority of youth are supporters of IS” and this is the fault of the various emirs,

⁵⁴ Rao Komar, Christian Borys, and Eric Woods, “The Blackwater of Jihad,” *Foreign Policy*, February 10, 2017, <http://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military-contractor-syria-russia-malhama-tactical/>.

⁵⁵ Joanna Paraszczuk, “Khalid Shishani: IS is Winning the Propaganda War in Chechnya,” *From Chechnya to Syria*, April 18, 2016, <http://www.chechensinsyria.com/?p=25071>.

himself included.⁵⁶ The members of non-IS affiliated factions, such as Abdul Hakim Shishani and Muslim Shishani gave interviews to different websites, such as Nohchicho, for example.⁵⁷

The means by which pro-jihadist propaganda spreads have improved throughout the evolution of the conflict in Syria. Media platforms have become more ‘professional’ and have adapted according to the needs of their target audience. A large portion of the material is in Russian, which allows for reaching a very broad audience of Russian-speaking individuals worldwide. Despite the ongoing pro-IS and non-IS propaganda war, the former has been extremely effective to date. As a result, many young North Caucasians become easily radicalized and recruited. Many of them continue to seek a way into IS to the battle ground in Syria, while others carry out attacks in North Caucasus (mostly Dagestan and Chechnya). Of course, al-Nusra and other factions also gain new recruits; however, the majority of North Caucasian FTFs still rests with IS. Furthermore, the existing channels of propaganda aid in establishing networks between jihadists that can be used in the future.

Security Implications of North Caucasian FTFs

Presently, the rate of incoming FTFs into Syria has decreased. This is a result of increased border controls and high casualties among militant groups, among other reasons. Those that have travelled to Syria and Iraq at the beginning of the conflict, for the large part could not return to the North Caucasus to fight against the Russian government. Typically, these were fighters with combat experience who were known to authorities. These fighters paved the way—for themselves and for the fighters in the years to come—by establishing either their own ‘independent’ factions like Abdul Hakim Shishani and Muslim Shishani, factions affiliated to CE, or those that would later split and be shaped by the IS – al-Nusra rivalry.

Regardless of which faction they may have chosen to join, these fighters may pose a large security threat not only to Russia, but to neighboring countries, or to future conflict zones. The new combat experience gained and/or refined, training received, established networks and reputation add to their ‘danger value’ – and therefore their ability to mobilize new recruits. Furthermore, the fact that the Syrian battleground had seen the emergence of Malhama Tactical is dangerous in that it may set a future trend. Due to the fact that the majority of North Caucasian FTFs are guided by the wish to fight the Russian government, they may be seen as ‘jihadist international’s,’ willing to travel to other regions in the future because of the inability to fight in the North Caucasus. Some of the ‘independent’ factions have a stronger political agenda, which may pose a

⁵⁶ Paraszczuk, “Khalid Shishani: IS is Winning the Propaganda War in Chechnya.”

⁵⁷ IA Nohchicho, “Abdul-Hakim ash-Shishani: We Are Supporting the Action of 23 February,” Address by Abdul-Hakim ash-Shishani sent to the media (in Russian), <http://nohchicho.com/tribune/abdulhakim-about-23-february/>.

greater danger for the Caucasus and increase their desire to return. In sum, the influence of the war in Syria and specifically the ideological reach of the Islamic State in the North Caucasus is a growing concern, despite the heavy security presence in the region.

Instabilities in North Caucasus

In the fight against insurgency, terrorism and the militants in North Caucasus, there are at least three types of players: the siloviki (police/law enforcement), the boeviki, also sometimes known as 'lesniye' ('from the woods,' because of their place of hiding), and the 'peregovorshik' (the negotiator between law enforcement and the militants). The latter is a peacemaker of sort, who 'brings people out of the woods' and negotiates certain deals between the police and militants. According to Milashina, journalist of *Novaya Gazeta*, this is how Russian authorities know who left Russia to fight in Syria and, furthermore, they "are not worried about those who leave, they are worried about those who may return."⁵⁸

It is difficult to find official updated statistics concerning the numbers of returning fighters from Syria or the number of terrorist plots or attacks committed by fighters/insurgents affiliated with IS. The number of fighters who returned to the North Caucasus in 2015, according to some estimates, was around 15-20 % (or as many as 889 individuals).⁵⁹ Likewise, not a lot of concrete information about counter-terrorist measures, operations and progress exists in the public domain. In 2015, according to statements of the FSB, 30 terrorist attacks had been successfully averted and 770 'bandits'⁶⁰ and their accomplices were put on trial. In 2016, the number of averted attacks amounted to 42. The individuals on trial include those who have been involved in crimes of terroristic nature, among them financing, recruiting new members, and leaving the country with the aim to fight abroad.

The website 'Kavkazsky Uzel' provides a chronology of events in the North Caucasus. According to its information, the intensity of fighting between siloviki (law enforcement, Rosgvardia) and the boeviki (militants/insurgents) had grown.

⁵⁸ For a summary of the article by Elena Milashina in *Novaya Gazeta* in English, see Paul Goble, "Novaya Gazeta – FSB Helps Islamists from Russia Go to Syria, Only Worried When They Come Back," *The Interpreter*, July 31, 2015, www.interpretermag.com/novaya-gazeta-fsb-helps-islamists-from-russia-go-to-syria-only-worried-when-they-come-back/.

⁵⁹ In 2015, the Director of FSB Alexander Bortnikov stated that 889 fighters had returned to Russia from Syria and Iraq. See Maksim Solopov, "Russia's Special Services Calculated Hundreds of Fighters Coming Back from Syria and Iraq," *RBK* (in Russian), December 25, 2015, <https://www.rbc.ru/politics/25/12/2015/567bfd9a7947a3b3bc7387>.

⁶⁰ 'Bandit' has a broader meaning and is a general term to refer to a criminal connected to criminal 'band' or organization. In this case it has been used to denote terrorists, or those individuals involved in terrorist activity.

In 2016, there were 84 armed clashes, 23 explosions, seven terrorist attacks, and a total of 287 casualties.⁶¹ By contrast, in 2015, there were 87 armed clashes, 11 explosions, six terrorist attacks, and a total of 258 casualties.⁶² The efficacy of attacks carried out by the boeviki had also grown. In 2015, on average, for every 10 siloviki, the boeviki would lose 35 men, while in 2016, for every 10 siloviki, the boeviki would lose 17 men. This tendency had remained until the present (April 2017). The escalating situation in Chechnya, the failures of the Rosgvardia and the returning fighters from Syria have contributed to sustaining this tendency. As a result of clashes and CTOs in 2016, 162 boeviki were killed (including 22 leaders of the 'bandit underground'⁶³), and four wounded. These numbers had decreased throughout the past three years, with 174 in 2015, and 249 in 2014. So far in 2017, 17 militants have been killed in Chechnya, and eight in Dagestan.⁶⁴ The casualties for law enforcement officers amount to 97 (32 killed and 65 wounded) in 2016; which is nearly double the number in 2015 (49). Since 2015, in Chechnya alone there have been at least 10 cases of assaults on the siloviki (three in 2017, four in 2016, and three in 2015).

Attacks also took place in Ingushetia, Kabardino-Balkaria and Dagestan. Furthermore, IS is increasingly claiming responsibility for assaults in the region. In August 2016, IS had released a video calling for jihad in Russia; however, Kadyrov, the head of the Chechen Republic, did not take it seriously, stating that IS boeviki have neither the required power nor the capabilities. Nevertheless, already back in 2015 IS took responsibility for the first attacks in the North Caucasus; the assault on the Russian army barracks in South Dagestan and a shooting in Derbent provide examples. Some of the boeviki involved in these attacks were fighters who had returned from Syria.⁶⁵ In 2016, there were another five IS-linked attacks in Dagestan and one in Chechnya. Finally, in 2017 (as of April), IS has been linked to at least four attacks, including an assault on a Rosgvardiya checkpoint at the end of March, and two clashes with jihadists in Chechnya. The

⁶¹ "Statistics of Casualties in North Caucasus for 7 years," *Kavkazsky Uzel [Caucasian Knot]*, http://www.kavkaz-uzel.eu/articles/statistika_jertv_2010_2016/ (21 August 2017); "North Caucasus: On the Background of Growing Violence in Chechnya, the Fighters' Activities Became Much More Effective," *Kavkazsky Uzel [Caucasian Knot]*, April 6, 2017, <http://www.kavkaz-uzel.eu/articles/300522/>.

⁶² "Statistics of Casualties in North Caucasus for 7 years"; "North Caucasus: On the Background of Growing Violence in Chechnya, the Fighters' Activities Became Much More Effective."

⁶³ 'Bandit underground' is used to describe the various networks and organizations of insurgents/militants, considered to be tied to terrorist activity.

⁶⁴ "Infographics: Statistics of the Casualties in North Caucasus in the First Quarter of 2017 Based on *Caucasian Knot's* Data," *Kavkazsky Uzel [Caucasian Knot]*, April 17, 2017, <http://www.kavkaz-uzel.eu/articles/301176/>.

⁶⁵ "NAC: Two Militant Leaders and a Fighter Returning from Syria Have Been Neutralized in Dagestan," *RIA Dagestan*, November 29, 2015 (in Russian), www.riadagestan.ru/news/incidents/nak_v_dagestane_neytralizovany_dva_bandglavarya_i_boevik_vern_uvshiyasa_iz_sirii/.

attack that took place in March could be tied to a video released on Youtube a few days earlier entitled the “Council of the military *jamaat* Ichkeria,” which allegedly depicts some of the returning fighters who were part of JMA.

The recent terrorist attack in St. Petersburg on 3 April 2017 (an explosion in the city’s underground between two central stops which killed 16 and left around 102 injured) was the first one of such scale since 2013. The suspected suicide bomber is said to have been an ethnic Uzbek born in Kyrgyzstan. He had obtained Russian citizenship in 2011 and had been living and working in St. Petersburg. According to RBC, in December 2016 he was deported from Turkey.⁶⁶ On 25 April 2017, the SITE Intelligence Group stated that Katiba al-Imam Shamil, an al-Qaeda linked group in Syria, claimed responsibility for the attack.⁶⁷ Some experts had also suggested that the perpetrator may have been tied to one of the leaders of CE in Kabardino-Balkaria, who according to the National Antiterrorist Committee (NAC) had been eliminated during a CTO in St. Petersburg earlier in August 2016, together with four other prominent members.

A few points, however, should be kept in mind. The attacks for which IS has claimed responsibility are not necessarily carried out by fighters returning from Syria or Iraq. IS has spread to the North Caucasus and many young people (influenced by IS propaganda, as well as the conditions in the region) become radicalized without having been abroad to fight. The word ‘boeviki’—militant/insurgent—provides no distinction between the type or affiliation of the militant (Caucasus Emirate, Islamic State, or any other), and is used synonymously to mean ‘terrorist.’ CE now barely exists, due to the CTOs carried out in 2016 by government forces, and IS has stepped in to fill the void. At least one attack in Chechnya can be tied to fighters who came back from Syria, and who used to be part of JMA. Another attack in Dagestan is tied to a fighter returning from Syria. Furthermore, many returning fighters have already joined the ‘bandit underground,’ even though the numbers are unclear.

Dealing with FTFs: Collective Responsibility

Within the past three years, Russia’s legislation on countering terrorism⁶⁸ and ensuring public security have been supplemented with new legislation, including

⁶⁶ Igor Zalubovin, “The Terrorist’s Ghost: Chasing Akbar Dzhililov Who Blew Up the Underground,” *Snob*, April 12, 2017 (in Russian), <https://snob.ru/selected/entry/123174>.

⁶⁷ Artem Filipenok and Anjelika Basisini, “A Group Connected to Al-Qaeda Claimed Responsibility for the Terrorist Act in the Underground,” *RBK*, April 25, 2017 (in Russian), <https://www.rbc.ru/society/25/04/2017/58ff6c359a7947167d4fdcd4>; and SITE Intelligence Group, “Alleged AQ-Linked Group Claims St. Petersburg Metro Bombing,” 25, 2017, <https://news.siteintelgroup.com/Jihadist-News/alleged-aq-linked-group-claims-st-petersburg-metro-bombing.html>.

⁶⁸ The relevant laws are listed on the website of the National Antiterrorist Committee, <http://nac.gov.ru/zakonodatelstvo/zakony.html>.

those known as the ‘Yarovaya Laws.’⁶⁹ These have acted to broaden the spectrum of crimes understood as terroristic. They have introduced new clauses such as establishing criminal responsibility for failure to inform of a crime of a terrorist nature, on committing an act of international terrorism, and on monitoring electronic messages. Moreover, they defined new auxiliary measures: regulations for telecommunications and internet provider companies on storing data, and a ban on missionary and extremist activity, among others. Some of these laws are the subject of debate concerning limitations of human rights, and possible unconstitutionality.⁷⁰ However, they are a direct response to the issue of Russian fighters in Syria and the domestic terrorist situation. The maximum penalty that one can get is incarceration for life. The North Caucasus, however, is understood to live according to slightly different laws.

Precisely how the local North Caucasian authorities deal with fighters returning to the region is shrouded in secrecy and so is not entirely clear. Legally, regional approaches draw upon Russian counter-terrorism legislation (the Federal Criminal Laws of the Russian Federation and other anti-terrorist laws⁷¹) and security services conduct regular CTOs. Of particular interest, however, are the concept of collective responsibility and other measures aimed at the general public.

The principle of collective responsibility in modern times is regarded negatively, since it presupposes holding responsible a group of innocent individuals not affiliated with the crime. It is presently employed in Chechnya for control over the population and, by extension, its repression. As reported by Kavkazsky Uzel, in 2016 through this method (in combination with Kadyrov’s active visits to different states in the Middle East, financing of mosques and schools), the influence of the Chechen government is increasingly felt among Chechen diasporas within and outside the borders of Russia. According to human rights defenders Sokiryanskaya, Orlov, Lokshina and Gannushkina, Chechen refugees do not forget that they still have ‘pressurable’ relatives back in Chechnya, who sometimes serve as a reason to return back to their homeland.

According to Orlov, presently Kadyrov is pushing to legislate the principle of collective responsibility on a federal level – and on various local talk shows one

⁶⁹ Valeria Zenovina, “The President of the Russian Federation Signed the Set of Anti-terrorist ‘Yarovaya Laws,’” *Garant.ru*, July 7, 2016 (in Russian), www.garant.ru/news/782190/.

⁷⁰ “Stipulations of the Antiterrorist Legislation, Constraining Citizen’s Rights,” *Monitoring New Russian Laws and Their Implementation in the Field of Civil Rights* (in Russian), <http://monitoring.mhg.ru/zakon15>.

⁷¹ Section 208, p. 2 of the Criminal Law of the Russian Federation is very commonly applied to those who have returned from Syria. It refers to incarceration for “participation in an armed entity/formation on the territory of a foreign state with aims contradictory to the interests of the Russian Federation” (translated from Russian). Section 205, on the other hand, pertains to terrorism. The Yarovaya Laws have caused mass public discontent and have drawn the attention of Amnesty International for alleged violations of human rights.

would now hear that the principle is a norm (although ‘only a couple of years ago it was considered barbaric’). In Chechnya, the main motivations for invoking the principle of collective responsibility, however, are counter-terrorism, countering extremism and radicalism, the fight against insurgency and militants (the so-called ‘boeviki’). Russian criminal law does not support collective responsibility. One of the anti-terrorist ‘Yarovaya Laws,’⁷² as of 20 July 2016, increases criminal responsibility for crimes of terroristic character (beginning at the age of 14), including non-information about an action (completed or in progress) of terroristic character.⁷³ The maximum penalty for withholding information is imprisonment for one year, and it is not applicable to spouses and close relatives; however, they can be held financially responsible for any damage inflicted in a terrorist attack.⁷⁴ Nevertheless, the Russian government typically “turns a blind eye” to Kadyrov’s collective responsibility in Chechnya and the rest of the North Caucasus. According to Kadyrov, militants responsible for criminal activity will have their families ousted from the republic, and their houses demolished “to the fundament.”⁷⁵

Collective responsibility is not only the preferred official strategy, it is seemingly supported by ordinary citizens as well (out of fear of the authorities or otherwise). In December 2016 and January 2017, in response to attacks in Dagestan and Chechnya, governmental forces had carried out mass ‘reid’ detentions and questionings of relatives and friends of eliminated militants. Around 200 people were reportedly detained, including minors. According to Maaz Bilalov, all of the relatives of militants involved in the attacks in December had been fired from their jobs, and their pensions and social subsidies had not been paid. After the January attacks on Chechen police/Rosgvardiya, some of the relatives of militants endured public penance, sometimes through the use of local media (TV

⁷² Not all have been presently implemented – some have entered into force on 20 July 2016, while others are to be implemented in 2018.

⁷³ These include obtaining education with the aim of carrying out terrorist activity, involvement in a terrorist network, involvement in a terrorist organization, an act of international terrorism, and several others. For more information see Federal Law N375-FZ of July 6, 2016; <http://www.garant.ru/hotlaw/federal/782193/> (in Russian).

⁷⁴ Peter Roudik, “Russia: Collective Responsibility for Acts of Terrorism,” *Global Legal Monitor*, December 24, 2014, <http://www.loc.gov/law/foreign-news/article/russia-collective-responsibility-for-acts-of-terrorism/>.

⁷⁵ This statement was made in December 2014, condemning actions of militants who had attacked local police, killing 14 and leaving others injured. After the claim was made, according to information from human rights center ‘Memorial,’ in December 2014 around nine houses were burnt down and their inhabitants were ousted from Chechnya. For further information see Elena Milashina, “The Threat to Shoot Someone in the Forehead Is Not Illegal?” *Novaya Gazeta*, December 13, 2014, <https://www.novayagazeta.ru/articles/2014/12/13/62349-ugroza-pustit-pulyu-v-lob-ne-yavlyayetsya-chem-to-nezakonnym>.

channels, for example), and were forced to leave their homes in Chechnya.⁷⁶ Moreover, the relatives of the deceased police officers have called for blood feuds. According to the custom, the relatives of a killed individual are obliged to take revenge on the killer or his relatives. Historically, among the peoples of North Caucasus blood feuds had served to regulate public relations, protect family honor and fortune.⁷⁷ There was no ‘expiration date’ for a blood feud, it should be announced through a ‘mediator,’ and it targets the perpetrator or his close male relatives. This tradition is not new, yet it had been (semi-) contained through the efforts of Kadyrov himself. Reportedly, in response to threat of blood feuds, all the males of the Baharchiev family have left Chechnya.⁷⁸

On January 8, 2017, a protest against IS and its leader al-Baghdadi was held in Grozny, Chechnya and it gathered approximately 2,000 people, mostly ordinary citizens. Among the speakers were mothers of militants that had joined or were planning to join IS. They publicly asked for forgiveness for their sons’ crimes. Parental responsibility had also been discussed – people agreed that parents should harshen methods and improve upon the upbringing of their children. Another speaker involved in the protest was the returning fighter Said Mazhaev. He turned himself in to the authorities upon his return from Syria through Turkey in 2014, and had his initial sentence pardoned as a result of a deal with the authorities – evidently according to which he was to engage in counter-narratives and various forms of anti-IS propaganda work with the youth of the republic.⁷⁹ Thus, Said Mazhaev had frequently appeared at mosques, schools, and universities, in interviews in newspapers and on television channels, and elaborated on the dangers of IS (he had actually fought for JMA, and left Syria before Omar Shishani officially joined IS). Reportedly, Mazhaev actually managed to convince some individuals not to join IS, yet his younger brother was among those involved in the attack in Grozny in December 2016.⁸⁰ The protest against IS ended with the burning of al-Baghdadi’s portraits. Other public events that serve as a platform for ‘discussing’ strategies like collective responsibility are town meetings, frequently held after an attack or clash had occurred.

The aim of such protests is to invoke fear in the population through the realization that there will be consequences for involvement in terrorist activities, including for relatives. The principle of collective responsibility is not new and has

⁷⁶ Kazbek Chanturiya, “Collective Responsibility in Chechnya; An Ineffective Method of Influence,” *OC Media*, January 19, 2017, <http://oc-media.org/collective-responsibility-in-chechnya-an-ineffective-method-of-influence/>.

⁷⁷ “Blood Feuds – How They Kill Today in the Caucasus,” *Kavkazsky Uzel [Caucasian Knot]*, December 26, 2017 (in Russian), <http://www.kavkaz-uzel.eu/articles/296137/>.

⁷⁸ “Villagers Reported on the Eviction out of Chechnya of the Relatives of a Suspected Fighter,” *Kavkazsky Uzel [Caucasian Knot]*, December 26, 2017 (in Russian), <http://www.kavkaz-uzel.eu/articles/296137/>.

⁷⁹ Chanturiya, “Collective Responsibility in Chechnya; An Ineffective Method of Influence.”

⁸⁰ Chanturiya, “Collective Responsibility in Chechnya.”

historically been used by local authorities and Russian special services in their fight against insurgency in the North Caucasus. Strong pressure is usually exerted onto all male relatives, “up to second cousins,” on the paternal side. This frequently involves disappearances, questioning, beatings and torture. It sometimes also involves the use of relatives as human shields in order to persuade a militant to ‘come out of the forest,’ or cross over to the side of the government. Despite the fact that collective responsibility is an ineffective strategy in terms of addressing the root causes of underlying social problems (in fact, it fuels them), it is deemed successful by the Chechen authorities.

Concluding Remarks

The approaches to countering terrorism and extremism in the North Caucasus feed into the already existing social instability, grievances and discontent with authorities in the region. The Russian government should develop softer approaches to counter-terrorism. As a result of years of CTOs and counter-terrorist strategies (including ‘collective responsibility’) the Caucasus Emirate has practically dissolved and presently seems to be hardly functional. However, this is also due to the increasing influence of IS in the region. IS propaganda successfully targets the North Caucasian (and by extension, Russian) youth, agitating them to walk the path of jihad in Russia or outside of its borders. The number of FTFs from Russia and other CIS states, even though presently decreasing, is high (5,000-7,000) and, according to some reports, Russian Security Forces may have contributed to the outflow of fighters in the past. Even though the numbers of fighters returning from Syria to the region are not exactly known, they could be around 15-20 %. Those that have returned are either being prosecuted or incarcerated, have joined underground networks, or their whereabouts are unknown.

The number of IS-affiliated attacks in the North Caucasus has grown, and some of the recent attacks in the region are linked to ex-fighters of JMA and other returnees from Syria. The remaining fighters in Syria and Iraq, and those who still seek to join them on the battleground, pose a threat not only to Russia, but to neighboring countries. Their motivations to fight include fighting the Russian government wherever that is possible. With the current developments of the conflict in Syria, and the deteriorating situation and repression in Chechnya and neighboring republics, those motivations only grow stronger. The first wave of FTFs can be seen as potentially more dangerous, for they have managed to secure and build upon their reputations and expand their experience, skills and networks. They are the ones that have established themselves on the battleground through forming different *jamaats*, and in one instance a ‘jihadist private military company.’ The second wave of fighters from the North Caucasus was mostly influenced by IS propaganda, which remains influential in the region despite set-backs for the organization in Syria and Iraq. Regardless of their affiliation, North Caucasian FTFs pose a long-term threat to global security. Given the opportunity, they will most likely fight in the Caucasus, but if unable to return home they may be motivated to strike elsewhere instead.



The Prospects of Azerbaijan to Enhance Military Interoperability with NATO

Elman Nasirov and Khayal Iskandarov

Institute of Political Studies of the Academy of Public Administration under the President of Azerbaijan

Abstract: After the end of the Cold War, NATO recognized the importance of extending far beyond its traditional borders in order to maintain peace and stability throughout Europe. The incorporation of new members into the Alliance came to the fore. In the light of this approach, cooperation with partner nations became an important area for discussion. Ensuring that partner forces could work together effectively was one of the main objectives and this, in turn, highlighted the term ‘interoperability’ once again. Thus, the evolution of interoperability between NATO and partner nations after the demise of Cold War is considered in this essay, its importance is underscored, the levels of interoperability are introduced and the feasibility of Azerbaijan’s engagement in these levels is analyzed in this article. Different tools and mechanisms that the Alliance has launched over the last decades are scrutinized and useful recommendations are considered for Azerbaijan to enhance its military interoperability with NATO. From this perspective of interoperability, different successful models have been outlined as examples for Azerbaijan to follow.

Keywords: interoperability, NATO, security, cooperation, training, exercise.

Introduction

Having adopted a New Strategic Concept in 1991, NATO began to focus on the development of multinational force projection in order to adapt to the post-Cold War era and expand its capabilities for crisis management operations. In pursuit of future strategic goals NATO had to broaden and deepen cooperation with the

countries beyond its traditional borders. Thus, the Alliance was in urgent need of partners that would be able to keep abreast of NATO requirements. This approach in turn required members, as well as partner forces, to work together for out-of-area operations. The first initiative, designed to encourage these nations to work together, was the Partnership for Peace (PfP) program which was launched in 1994. The ultimate goal of this program was, and still is, to support partners in their efforts to reform their national defense structures and to assist them in developing their national capabilities. If the partner nations that signed the framework of this program wanted their militaries to operate together, they would have to follow procedures mainly determined in Brussels by NATO Allies.

This initiative proved to be a very successful tool. The fledgling Republic of Azerbaijan was among those countries who joined the program with an expectation to integrate into the Alliance eventually. Shortly afterwards, the Alliance embarked upon the Partnership Planning and Review Process with the aim of promoting the development of the forces and capabilities of the partners that were best able to cooperate alongside NATO Allies in crisis response operations and other activities to maintain security and stability. It provided a structured approach for enhancing interoperability and the capabilities of partner forces that could be made available to the Alliance for multinational training, exercises and operations.¹ This strategy continued over the ensuing years and the Alliance initiated new programs and mechanisms (such as the Operational Capabilities Concept (OCC), the Membership Action Plan (MAP), and the Individual Partnership Action Plans (IPAP)) for closer and deeper cooperation with its partners. The objective of NATO's partnerships, as stated in all three post-Cold War Strategic Concepts, is to safeguard security together. In the current Strategic Concept (2010), the three core tasks of NATO are collective defense, crisis management and cooperative security. Out of these, cooperative security is very much about partnerships. Thus, cooperative security is a broad task consisting of numerous elements. Fundamentally, it consists of three components: strengthening partnerships, contributing to arms control, non-proliferation and disarmament, and assisting potential new countries to prepare for NATO membership. An important sub-element of both strengthening partnerships and preparing new countries for potential membership is interoperability.² In short, with the new NATO missions and engagement in operational theatres there has been a dramatic shift from a single nation fighting on its own, to coalitions where multinational units, down to the level of platoons, are working together.

¹ Partnership for Peace Planning and Review Process, NATO Topics, last updated November 5, 2014, https://www.nato.int/cps/en/natohq/topics_68277.htm.

² Stephen J. Maranian, "NATO interoperability: Sustaining Trust and Capacity within the Alliance," *Research Paper* 115 (Rome: Research Division, NATO Defense College, June 2015), https://www.files.ethz.ch/isn/192707/rp_115.pdf.

A strategy for Keeping Interoperability on Track

The world is currently involved in a much more complicated security environment than it was decades ago. Thus, as an epicenter of global security NATO needs to become attuned to the challenges its member and partner nations are encountering. The implementation of the Alliance's grand strategy requires the continuous improvement of military effectiveness. In this regard interoperability is a *sine qua non* for the success of any operation/mission in coalition warfare. At the 2012 Chicago Summit, the Alliance embarked upon some new programs like Smart Defense (SD) and the Connected Forces Initiative (CFI). The rationale for launching these programs was, once again, the search for greater interoperability and coherence.³ The following declaration which was adopted in the Summit emphasized the importance of interoperability: "The Alliance's recent operational experiences also show that the ability of NATO forces to act together seamlessly and rapidly is critical to success. We will, therefore, ensure that the Alliance's forces remain well connected through expanded education, training and exercises."⁴ At this juncture, it is important to stress the various impacts that the lack of interoperability can have. First, it can endanger the successful implementation of operational missions. Second, it can have a major negative impact on resources and the logistical footprint, as it makes it difficult, or even impossible, to share spare parts, ammunition and fuel, and therefore, affects the efficiency of the force, in general. In certain areas, non-interoperability can have a dramatic impact, such as blue-on-blue fire or the unnecessary loss of life. It proves that enhancing interoperability increases the effectiveness of NATO operations and saves lives and resources.⁵ It is therefore in everyone's interest to cooperate and invest in order to achieve the highest level of interoperability and cooperation. In the Chicago Summit declaration, four of five references to interoperability dealt with extra-Alliance partnerships: Georgia, Ukraine, Mediterranean Dialogue nations and a general reference to partners attending the summit.⁶ This attitude, in turn, stimulated NATO's 'open door' and enlargement policy. In April 2013, when General Phil Breedlove took over U.S. European Command (EUCOM) he was asked, at his confirmation hearing, about the most im-

³ *What is Transformation? An Introduction to Allied Command Transformation*, with foreword by Lieutenant General Phil Jones, Chief of Staff (Norfolk, Allied Command Transformation, January 2015), http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2015/NATO_Introduction_AlliedCommand_Transformation_Jan2015.pdf.

⁴ Marcel-Petru Ivtu and Florian Ianoşiu Hangan, "Interoperability between NATO and Partner States in the post-ISAF Period. Present and Perspectives," *Romanian Military Thinking* 11, no. 4 (October-December 2015): 116-124, http://smap.mapn.ro/gmr/Engleza/Arhiva_pdf/2015/revista_4.pdf.

⁵ Florian Ciocan, "Perspectives on Interoperability Integration within NATO Defense Planning Process," *Journal of Defense Resources Management* 2, no. 2 (2011), 53-66, http://www.jodrm.eu/issues/volume2_issue2/06_ciocan.pdf.

⁶ Maranian, "NATO interoperability."

portant lessons learned from 10 years of NATO operations in Afghanistan. Leading his list was the increased ability of U.S. and allied troops to literally fight and operate side by side: "First of all, NATO in general, and some of the partners, has become much more interoperable." General Breedlove went on to say that the risk of losing this interoperability was one of his key concerns in thinking about how the North Atlantic Alliance moves forward beyond Afghanistan.⁷

At the 2014 Wales Summit, the Alliance updated the concept for its NATO Response Force (NRF) which was created at the 2002 Prague Summit. But, it was after Russia occupied the Crimea in early 2014, when its significance really came to the fore. This Response Force is a technologically advanced, flexible, deployable, interoperable and sustainable force that includes land, sea, and air elements that will be available wherever it is needed. It is intended to serve as a vehicle for the transformation of allied nations' and partners' military structure and capabilities.⁸ A consideration of the last three declarations issued by the heads of NATO state and government shows that interoperability is mentioned sixteen times. The Wales Summit⁹ declaration gave it much more prominence than both Chicago¹⁰ and Warsaw¹¹ declarations, where it was mentioned only five and 13 times respectively. Therefore, it can be said that the 2014 Wales Summit established a basis for the enhancement of interoperability between NATO and partner nations by initiating invaluable programs and mechanisms.

By 2014, when NATO anticipated completing its operations in Afghanistan, allied militaries had been deployed together in combat and post conflict land, maritime, and air operations for more than 20 years.¹² In order to implement this strategy, all stakeholders need to think and act coherently. It is about gaining and retaining a competitive advantage, a process which involves filling gaps and, in particular, those gaps which the changing environment threatens to create in the future. Recent destabilizing events around the globe, and within the Euro-Atlantic region, have reinforced NATO's assessments of a future security envi-

⁷ John R. Deni, "Whose Responsibility is Interoperability?" *Small Wars Journal*, June 26, 2013, <http://smallwarsjournal.com/jrnl/art/whose-responsibility-is-interoperability>.

⁸ Juha Pyykönen, "Partners of NATO: How similar are Finland and Sweden within NATO cooperation?" *FIIA Report* 48 (Helsinki: Finnish Institute of International Affairs, 2016), <https://www.fii.fi/en/publication/nordic-partners-of-nato>.

⁹ Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, *NATO e-Library, Official Texts*, September 5, 2014, www.nato.int/cps/en/natohq/official_texts_112964.htm.

¹⁰ Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, last updated August 1, 2012, www.nato.int/cps/en/natohq/official_texts_87593.htm.

¹¹ Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, last updated March 29, 2017, www.nato.int/cps/en/natohq/official_texts_133169.htm.

¹² Charles Barry, "Building Future Transatlantic Interoperability Around a Robust NATO Response Force," *Transatlantic Current* 7 (Washington, D.C.: National Defense University, Institute for National Strategic Studies, October 2012), quote on p. 1.

ronment as being volatile, complex and uncertain. The political relevance of the Alliance and the military effectiveness of its forces will continue to be challenged by a combination of this highly dynamic, interconnected and ambiguous operating environment, together with a period of lasting fiscal austerity.¹³ In this regard, the constant improvement of military structures and capabilities of the Azerbaijan Republic has the utmost importance, because it entails enhancing its military effectiveness and interoperability with Allied forces.

The NATO Glossary of terms and definitions defines interoperability as “the ability of the forces of two or more nations to train, exercise, and operate effectively together in the execution of assigned missions and tasks.”¹⁴ NATO’s interoperability policy defines the term as the ability to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives. Specifically, it enables forces, units or systems to operate together and allows them to share common doctrines and procedures, as well as each other’s infrastructure and bases, and to be able to communicate with one another. Interoperability reduces duplication, enables the pooling of resources, and produces synergies among the 28 Allies, and, whenever possible, with partner countries.¹⁵ Therefore, interoperability occurs at various levels – strategic, operational, and tactical as well as technological. Because of these different levels and multiple dimensions, interoperability can be examined from the broadest available definition: “The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together.”¹⁶

At a strategic level, interoperability is one of the essential factors contributing to the creation of a coalition of forces, thereby demonstrating a desire by the coalition members to act together against common threats as long as is necessary. At this level, interoperability focuses on harmonizing the global visions of the members’ strategies, doctrines and force structures. At operational and tactical levels, interoperability refers mainly to how interoperable issues, that have been agreed at political and strategic levels, work together to support allied and partner states or members of a coalition in conducting crisis management, creating the environment to achieve the set of objectives, and winning the war. At the operational and tactical levels, interoperability depends on synchronization among allied and partner forces. In general, the benefits of achieving interoperability at operational and tactical levels are represented by the interchange of

¹³ “What is Transformation?” p. 3.

¹⁴ Ivut and Hangan, “Interoperability between NATO and partner states.”

¹⁵ “Partnership Interoperability Initiative,” *NATO Topics*, last updated June 7, 2017, https://www.nato.int/cps/en/natohq/topics_132726.htm.

¹⁶ “A Broad Definition of Interoperability,” Chapter 2 in Myron Hura, Gary W. McLeod, Eric V. Larson, James Schneider, Dan Gonzales, Daniel M. Norton, Jody Jacobs, Kevin M. O’Connell, William Little, Richard Mesic, and Lewis Jamison, *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: RAND Corporation, 2000), 7-15, www.rand.org/pubs/monograph_reports/MR1235.html.

the coalition forces and units/subunits.¹⁷ At the technological level, the benefits of interoperability come, primarily, from their impacts at the operational and tactical levels in terms of enhancing fungibility and flexibility. This level focuses on “communications and computers but also involves the technical capabilities of systems and the resulting mission compatibility or incompatibility between the systems (hardware and software) and the data of coalition partners.”¹⁸ Thus, it may be deduced that the qualities of interoperability at all levels are deployability, flexibility, sustainability, mobility, and survivability. This description makes interoperability one of the main requirements for effective operations.

In order to shed light on all levels of interoperability one can envisage an example of the way in which an air campaign could be conducted (as depicted in Figure 1). In this example the strategic level reviews the airspace policy and establishes airspace structures. The campaign level addresses operational planning and execution, as well as force planning according to NATO doctrines. The main element at this level is the political willingness to cooperate. Interoperability at the operational level occurs when strategic and tactical interoperability come together to manage crisis situations. The allocation of airspace takes place at the tactical level. Airspace structures determined at this level are disseminated to interested airspace stakeholders. The technological level focuses on the technical capabilities of the systems and data of coalition partners to respond in similar way to a particular situation.

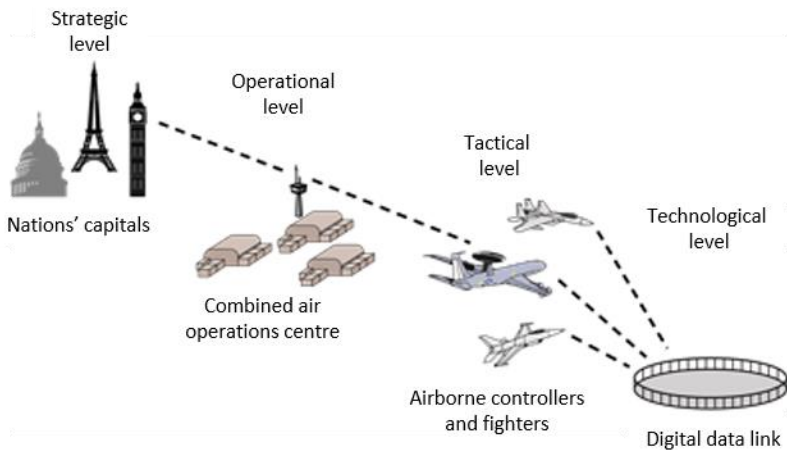


Figure 1: Interoperability at four levels – Case of air campaign.¹⁹

¹⁷ Ivut and Hangan, “Interoperability between NATO and Partner States.”

¹⁸ “A Broad Definition of Interoperability,” p. 13.

¹⁹ “A Broad Definition of Interoperability,” p. 9.

Achieving interoperability is a constant necessity at all levels. In NATO member states it is achieved by implementing agreed standards. As for the relations with partner states, achieving a high level of interoperability is a crucial factor considering the joint participation in NATO-led operations/missions.²⁰ While NATO members are engaged at every level, partner nations are not involved at the strategic level. Parenthetically, the Alliance develops partnerships at different levels and it is up to the partner nation to choose the level at which it wishes to engage in order to strengthen and extend their peace and stability. Since Azerbaijan has not articulated a desire for full membership, a concrete way to achieve interoperability from a military perspective is to benefit from the tools and mechanisms regarding education and training that the Alliance has launched over the past years. In fact, these tools are a valuable means by which to improve interoperability and capabilities at all levels. Having capitalized on these opportunities, military forces of some partner nations (e.g. Austria, Finland and Sweden) have reached a high level of interoperability as a result of years of participation in joint training and exercises at the first three levels. Interoperability is not necessarily a political decision, it is more often a technical one. Therefore, there would appear to be no hindrances to the Azerbaijan Armed Forces being fully interoperable with NATO.

Interoperability does not, necessarily, mean that allied or partner states should have or should purchase common military equipment. It is as much, or more, about human teamwork than it is about compatible machines and processes. What is especially important is the ability to use the existing equipment by sharing facilities, and so being capable of interacting, connecting, communicating and exchanging information and services with similar equipment from another states inventory.²¹ Here, it is necessary to mention that the Azerbaijan Armed Forces have made giant strides by utilizing NATO's Partnership Staff Element (PSE) concept and its Defense Education Enhancement Program (DEEP). The PSE concept creates possibilities for Azerbaijan to deploy its officers within various NATO headquarters and commands to gain experience and knowledge by working side-by-side with Allies in the same headquarters and offices. Azerbaijan utilizes this instrument effectively and has sent more than 20 officers to various PSE posts since 2002, making it one of the biggest partner staff contributors among the PfP countries.²² After completing their missions, these officers are appointed to various leading positions where they may contribute to the enhancement of the relations between NATO and Azerbaijan. Having identified the needs in the military domain, Azerbaijan has begun to utilize widely the NATO expert advice available through the DEEP Program in order to upgrade its mili-

²⁰ Ivut and Hangan, "Interoperability between NATO and Partner States."

²¹ Ivut and Hangan, "Interoperability between NATO and Partner States."

²² *Azerbaijan – NATO partnership* (Brussels: Mission of Azerbaijan to NATO, 2014), http://nato-pfp.mfa.gov.az/files/file/broch_AZE-OTAN_LR.pdf.

tary education system with the purpose of becoming intellectually interoperable with the Alliance.

Given the above-mentioned aspects it can be deduced that interoperability encompasses the following areas²³:

1. the ability of forces from different nations to work effectively together
2. the effectiveness of the combined military organizational structure
3. the degree of similarity of technical capabilities of the forces from different nations.

According to an action plan approved by NATO Defense ministers, interoperability has three dimensions²⁴:

1. technical (hardware and systems)
2. procedural (doctrine and procedures)
3. human (language, terminology and training).

On the other hand, the mechanisms that support the achievement of interoperability are: the effective implementation of allied agreed standards (STANAGs), doctrine and tactics; joint training; the participation in NATO/multinational exercises; the application of NATO policy related to lessons learned; and the conduct of demonstrations and tests. According to the NATO Strategic Concept 2010, partnerships with third countries “can make a concrete contribution to enhancing international security, to defending the values on which the Alliance is based, to NATO’s operations and to preparing interested nations for membership of NATO.”²⁵

Interoperability in coalition warfare is at the core of U.S. defense policy and military doctrine. The January 2012 Defense Strategic Guidance, the most recent top-level Department of Defense (DOD) strategy document, emphasizes sixty times the importance of allies and partners in its brief eight pages. The latest version of the military’s capstone doctrinal publication refers to interoperability 87 times in just 200 pages.²⁶

At the 2012 NATO Summit in Chicago, NATO committed itself to further strengthening and deepening its partnerships. This was reaffirmed at the 2014 Wales Summit when it launched the Partnership Interoperability Initiative (PII) to maintain and deepen the interoperability that has been developed with partners during NATO-led operations and missions over the last decades. Once again, the PII underlined the importance of interoperability for all its partnerships and proposed new means to deepen cooperation with those partners that wished to be interoperable with NATO. As NATO’s Deputy Secretary Gen-

²³ “A Broad Definition of Interoperability.”

²⁴ “Interoperability: Connecting NATO Forces,” *NATO Topics*, last updated June 6, 2017, https://www.nato.int/cps/ic/natohq/topics_84112.htm.

²⁵ Ivut and Hangan, “Interoperability between NATO and Partner States.”

²⁶ Barry, “Building Future Transatlantic Interoperability.”

eral Alexander Vershbow emphasized: “This is the first standing consultative forum dedicated to interoperability, and by far the greatest opportunity for cooperation and dialogue for those who wish to be an enhanced opportunity partner.”²⁷ Included in the PII is the “Interoperability Platform” of 25 selected partners and the tailor-made “Enhanced Opportunities” for deeper cooperation with five specific partners (Australia, Finland, Georgia, Jordan and Sweden).²⁸ This initiative provides increased capacity to cooperate with partners to counter security threats by:

1. interrelating all existing interoperability mechanisms and programs
2. supporting partners that wish to become interoperable
3. providing partners that significantly contribute to the Alliance with increased opportunities, and
4. developing, maintaining, diversifying and increasing a pool of forces and capabilities belonging to partner states, which are certified and ready to contribute to future NATO operations or to the NRF.²⁹

The second initiative, which was endorsed at the Wales Summit to reinforce the Alliance’s commitment to the core task of cooperative security, is the Defense and related security Capacity Building (DCB) Initiative. It focuses on helping partners to provide their own security by strengthening their defense and related security capacity.³⁰ In this regard the Partnership for Peace Planning and Review Process, the Operation Capabilities Concept and the Military Training and Exercise Partnership are the main tools by which to promote the interoperability and capabilities of the forces of partner nations. The Alliance has recently developed an Individually Tailored Roadmap Capstone Concept that should simplify existing partnership programs and improve cooperation by increasing shared situational awareness and trust. Pilot projects that include cyber-defense aspects have been launched with Finland, Georgia and Jordan. Another model of how NATO and coalition partners have worked together to improve interoperability and information sharing in operations, exercises and training events is NATO’s Federated Mission Networking. This framework includes policy, processes, procedures, standards and physical components such as static and deployed networks, services and supporting infrastructures. Partners will be engaged also in the areas of early warning, prevention, and analysis of cyber threats.³¹

²⁷ “Partnership Interoperability Initiative.”

²⁸ “Partnership Interoperability Initiative.”

²⁹ Ivut and Hangan, “Interoperability between NATO and Partner States.”

³⁰ “Partnership Tools,” *NATO Topics*, last updated June 24, 2016, www.nato.int/cps/en/natohq/topics_80925.htm.

³¹ Piret Pernik and Tomas Jermalavičius, “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” in *Forward Resilience: Protecting Society in an Interconnected World*, ed. Daniel S. Hamilton (Washington, D.C.: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins

NATO militaries have achieved a high level of interoperability through decades of joint planning, training and exercises. Member countries have put this interoperability into practice and developed it further during joint operations and missions. These operations have also enabled partner countries to improve their interoperability with the Alliance.³² The International Security Assistance Force is the best example of this, both in terms of the benefits arising from achieving a high level of interoperability between NATO and partner states and the need to maintain the achieved level.³³ If maintaining, and even developing, the achieved level of interoperability with partner nations is a priority for NATO, then Azerbaijan's aspiration of much deeper cooperation with the Alliance is a realistic goal.

Conclusion

In order to be interoperable with NATO forces, a state is required to have qualified military capabilities. Azerbaijan has been developing its military capabilities since it achieved independence from the USSR. Azerbaijan is an enthusiastic partner of NATO. However, there is still a lot of work to be done in order to enhance its military interoperability with NATO. Azerbaijan needs to go beyond achieving minimum interoperability and reach a higher stage of integration. Taking into account all of the four levels of interoperability introduced in this article, Azerbaijan is, arguably, actively engaged in the first three levels (technological, tactical and operational levels). In order to achieve all of these goals Azerbaijan will need to enhance its national capabilities for crisis response operations in order to be a capable, willing and reliable partner in a crisis. Thus, more demanding exercises and training are welcomed by Azerbaijan, as multinational exercises verify interoperability in an effective manner. The bottom line is that the more a partner invests in cooperation, the more it benefits from it. PARP remains one of the most effective mechanisms for Azerbaijan in the field of defense and force planning. The Operational Capabilities Concept has to be utilized widely to ensure the required level of armed forces interoperability.

In order to increase interoperability with Western forces, Azerbaijan may benefit from NATO through obtaining advice in areas such as defense institution building, cyber defense, logistics, and standardization. NATO, in turn, could develop more robust assistance and engagement programs for Azerbaijan considering its vulnerability and susceptibility to neighboring aggression. DEEP is an invaluable tool to develop educational institutions in the defense sector and to make Azerbaijani military personnel intellectually interoperable with NATO's.

As a part of the "Interoperability Platform" Azerbaijan has recognized the importance of working together with NATO and may benefit from a more tailor-

University, 2016), 99-112, <https://archive.transatlanticrelations.org/publication/forward-resilience-protecting-society-interconnected-world/>.

³² "Interoperability: Connecting NATO Forces."

³³ Ivut and Hangan, "Interoperability between NATO and Partner States."

made relationship, such as “Enhanced Opportunities” to maintain an optimal level of interoperability. In this way, the Alliance may create additional tailored programs based on the individual needs of Azerbaijan. In addition to the above programs, Azerbaijan could ask for a defense and related security capacity building package in order to strengthen its defense and related security through education and training. The NATO Response Force is the central platform for sustaining interoperability and Azerbaijan could easily benefit from the Connected Forces Initiative concept for the enhanced training of its troops and, with the use of modern technology, to facilitate interoperability and integration of the required capabilities. Also, by deploying the minimum level required by the OCC evaluators for potential operations, Azerbaijan could join NRF exercises with other designated forces since it is the most visible instrument for the certification of interoperability capabilities between NATO and Azerbaijan. Finally, it is important to stress that foreign language training is a prerequisite for the whole gamut of interoperability-related activities. The primary focus is, of course, on English as the language of the NATO integrated military structure. Thus, the Foreign Language and Partnership Center functions under the aegis of the War College, with the purpose of imparting training in different foreign languages to the personnel of the Armed Forces. By enabling Azerbaijani military personnel to communicate in English at a reasonable level of proficiency (STANAG levels 2-3), they are provided with an opportunity to learn NATO tactics in the military domain.

About the authors

Prof. **Elman Nasirov** is Doctor in political sciences and Director of the Institute of Political Studies of the Academy of Public Administration under the President of Azerbaijan. He serves also as member of parliament of the Republic of Azerbaijan.

Khayal Iskandarov is Chief of the editorial section of the War College of the Armed Forces, Republic of Azerbaijan. He holds a Master degree in military sciences and is currently pursuing a PhD degree in military sciences and national security. *E-mail:* xayal1333@gmail.com.